OAC Boletín de septiembre de 2023

(Reúne el período Junio, Julio y Agosto)

"Un Estado, puede lograr poco por la diplomacia a menos que tenga la fuerza y voluntad de respaldar sus exigencias por la fuerza."

Samuel P. Huntington (El soldado y el Estado pag77

"***A lo largo de todo el curso de la historia, la guerra, siempre está cambiando***"

Andres Beaufre-

Tabla de Contenidos

El Observatorio Argentino del Ciberespacio (OAC), es un micro-sitio de la Facultad Militar Conjunta de las Fuerzas Armadas, editado y publicado por el Instituto de Ciberdefensa de las Fuerzas Armadas

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

Esta publicación mensual se encuentra inserta en el Nodo Territorial de Defensa y Seguridad de la Red Nacional de Nodos Territoriales (NT) de Vigilancia Tecnológica e Inteligencia Estratégica (VTeIE) del Ministerio de Ciencia, Tecnología e Innovación 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 ambiente operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo.

ESTRATEGIA

Fortalezas y debilidades de la inteligencia Artificial China

Estados Unidos se enfrenta a un "momento del Proyecto Manhattan" en inteligencia artificial (IA).

A medida que sus científicos desarrollan capacidades militares, los adversarios ven su poder y buscan mantenerse al día. "En términos de impacto, la inteligencia artificial será similar al armamento nuclear", dijo Alexandr Wang, director ejecutivo de ScaleAI, un desarrollador de software.

Occidente enfrenta cuatro riesgos principales frente a China:

(1) La inversión es la principal ventaja de China;

(2) La desinformación y la influencia en los procesos democráticos;

(3) Procesos de adquisición lentos

(4) Los datos abiertos de Occidente

https://www.afcea.org/signal-media/ai-chinas-strengths-and-weaknesses?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIlVg1&_zl=9iS89

Estrategias de Seguridad en la Cadena de suministros

El ataque cibernético de 2021 que cerró el Oleoducto Colonial durante días, movió a los funcionarios de Energía de la Agencia de Logística de Defensa a buscar nuevas formas de llevar combustible a los clientes de la costa este y subrayó la necesidad de resiliencia en la cadena de suministro.

Una nueva estrategia que está redactando la Agencia Logística de la Defensa (DLA), se convertirá en la hoja de ruta de la agencia para abordar tales vulnerabilidades y proteger la seguridad de la cadena de suministro del Departamento de Defensa que sirve a las tropas y socios federales en todo el mundo.

Las medidas de protección se están desarrollando en cuatro áreas:

(1) Sistemas y datos de DLA;

(2) Proveedores con información como información no clasificada controlada, datos de control de exportaciones y otros datos de DLA;

(3) Operaciones críticas de proveedores;(4) Proveedores y sistemas críticos para brindar soporte no incluidos en otras categoría

https://www.defense-aerospace.com/upcoming-strategy-to-outline-defense-logistic-agencys-supply-chain-security/

El metaverso en el mundo militar

Es un panorama cambiante que requerirá cada vez más una respuesta conectada y multidominio, con activos desde los confines del espacio hasta las profundidades del océano en red para garantizar la superioridad y la preparación para las misiones en un mundo dominado por volúmenes crecientes de datos.

Aquellos que sean capaces de aprovechar, interpretar y utilizar con éxito esos datos en el campo de batalla tendrán una ventaja crítica.

El Proyecto OdySSEy está en el centro de esta colaboración. Reúne a expertos en simulación, supercomputación, análisis de datos y realidad virtual y aumentada para crear un entorno sintético único, que permita que las fuerzas aéreas, terrestres, marítimas, espaciales y cibernéticas se conecten y entrenen juntas.

https://www.defensenews.com/native/BAE/2023/09/01/welcome-to-the-military-meta-verse/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch

Estimación Anual del Entorno de Seguridad Estratégica

La *Estimación Anual del Entorno de Seguridad Estratégica* sirve como guía para académicos y profesionales de la comunidad de defensa sobre los desafíos y oportunidades actuales en el entorno estratégico. La publicación de este año describe cuestiones estratégicas clave en los cuatro grandes temas: Desafíos y oportunidades regionales, Desafíos nacionales, Desafíos institucionales y Dominios que impactan la ventaja estratégica de EE.UU. Estos temas representan una amplia gama de temas que afectan la seguridad nacional y proporcionan una evaluación global del entorno estratégico para ayudar a centrar a la comunidad de defensa en la investigación y la publicación.

La competencia estratégica con la República Popular China y las implicaciones de la invasión rusa de Ucrania siguen siendo desafíos dominantes para los intereses de seguridad nacional de Estados Unidos en todo el mundo. Sin embargo, el entorno de seguridad en evolución también presenta amenazas nuevas y no convencionales, como ataques cibernéticos, terrorismo, delitos transnacionales y las implicaciones de los rápidos avances tecnológicos en campos como la inteligencia artificial. Al mismo tiempo, Estados Unidos enfrenta desafíos internos e institucionales en forma de déficits de reclutamiento y retención en la fuerza exclusivamente voluntaria, la perspectiva de una logística cuestionada en operaciones de combate a gran escala, y la salud de la Base Industrial de Defensa de EE.UU. Además, los panoramas de seguridad en rápida evolución en la región ártica y el dominio espacial plantean desafíos potenciales únicos para la ventaja estratégica del Ejército.

https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1958&context=monographs

La Ciberdefensa y las Relaciones Internacionales

Una investigación realizada por Military Times y The Texas Tribune descubrió que los líderes de la Guardia Nacional de Texas disolvieron el ala de inteligencia de la Operación Lone Star después de que denunciantes informaron sobre la vigilancia de WhatsApp, que apuntaba a grupos de inmigrantes para rastrearlos a través de México, porque creían que violaba reglas de larga data contra el estado al ejecutar operaciones de espionaje. Durante el mismo período, según un informe de incidente interno, otro equipo de la dirección de inteligencia supuestamente envió inteligencia clasificada del FBI a sus colegas de la Guardia de Texas en una aparente violación de las leyes federales de secreto.

https://www.c4isrnet.com/news/your-army/2023/08/29/texas-guardsmen-spied-on-migrants-via-whatsapp-mishandled-secret-docs/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-cyber

India aprueba la legislación de protección de datos en el Parlamento. Los críticos temen la violación de la privacidad

Los legisladores indios aprobaron el miércoles una legislación de protección de datos que "busca regular mejor a las grandes empresas de tecnología y penalizar a las empresas por violaciones de datos", mientras varios grupos expresaron su preocupación por los derechos de privacidad de los ciudadanos.

La legislación limitará la transferencia transfronteriza de datos y proporcionará un marco para establecer una autoridad de protección de datos para garantizar el cumplimiento

de las empresas tecnológicas, dijo el ministro de Tecnología de la Información y Telecomunicaciones, Ashwini Vaishnaw.

https://apnews.com/article/india-data-privacy-law-modi-parliament-0776af2d9cf873917e986b31e1e21078

CIBERDEFENSA

La IA en la Ciberdefensa sería más potente que las operaciones ofensivas

Los funcionarios del Comando Cibernético del Ejército de EE.UU. consideran que la inteligencia artificial (IA) generativa ofrecen mayores beneficios a los ciberdefensores que a los adversarios.

https://www.afcea.org/signal-media/cyber-edge/ai-may-benefit-cyber-defense-more-offense?_zs=pIlVg1&_zl=2iS89#:~:text=Artificial%20intelligence%20(AI)%20capabilities%20offer,positive%E2%80%9D%20effects%20for%20the%20command.

Big Data e Inteligencia Artificial en las redes militares

Al reducir la cantidad de redes y expandir las capacidades de big data, el Ejército de EE. UU. está mejorando la ciberseguridad y sentando las bases para el uso de inteligencia artificial (IA) en la red.

En los últimos años, el servicio ha duplicado la cantidad de terminales de red que aportan datos de registro casi en tiempo real a la plataforma de big data conocida como Gabriel Nimbus (el Ejército cree que marcará la diferencia en la guerra contra adversarios tecnológicamente avanzados es una red invisible que une a cada soldado, comandante y arma en el campo), que se basa en la plataforma de big data de la Agencia de Sistemas de Información de Defensa, un sistema de código abierto que admite la infraestructura de ingesta, correlación y visualización de datos. La arquitectura común de la plataforma de big data se puede instalar en cientos de servidores en algunas horas y permite compartir datos, visualizaciones y análisis cibernéticos con los socios de la misión.
https://www.afcea.org/signal-media/cyber-edge/big-data-enables-artificial-intelligence-army-networks?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIlVg1&_zl=1iS89

https://www.nationaldefensemagazine.org/articles/2022/7/1/army-continues-build-up-of-integrated-tactical-network

Acerca del Plan de Datos del Ejército de EE.UU.:

El Plan de Datos del Ejército establece el marco para utilizar mejor los datos institucionales del Ejército para aumentar la velocidad de toma de decisiones en todos los niveles. El plan de datos proporciona orientación sobre la implementación de estándares comunes en toda la empresa para facilitar la interoperabilidad entre los socios conjuntos, de coalición y de misión.

https://www.army.mil/standto/archive/2019/11/22/
https://www.arcyber.army.mil/Organization/Inspector-General/

La Ciberdefensa y las Relaciones Internacionales

Actualmente todo tiene su versión ciber: ciberespacio, la ciberdefensa ciberespionaje, ciberincidente, ciberataque, , ciberguerra, ciberarma, cibercrimen, ciberdelincuencia, ciberseguridad; entre muchos otros. ¿Pero qué implican estos fenómenos en las Relaciones Internacionales?

En primer lugar, hay que tener en cuenta que el ciberespacio está en todos lados y en ninguno al mismo tiempo, logrando configurarse como tierra de todos y de nadie. Si bien los individuos, los Estados, las empresas y los organismos no estatales, entre otros, estamos entrometidos en la red de información que se forma con internet, al mismo tiempo estamos dentro de un "común global". Es decir, un espacio que escapa al control o la jurisdicción de algún Estado en particular (Bartolomé, 2022, 3), siguiendo la naturaleza anárquica del sistema internacional.

https://www.escenariomundial.com/2023/08/01/las-relaciones-internacionales-a-nivel-cibernetico/

Escalando la frontera de defensa: la visión de DISA para un futuro digital seguro y ágil

La red de información del Departamento de Defensa es la tercera más grande del mundo", dijo el teniente general Robert Skinner, director de DISA y comandante del Cuartel General de la Fuerza Conjunta, Red de Información del Departamento de Defensa (DoDIN).

https://www.afcea.org/signal-media/scaling-defense-frontier-disas-vision-secure-and-agile-digital-future?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=vBgDh1&_zl=QhsB9

Se despliegan nuevas variantes de campañas de phishing

Tomarían objetivos a organizaciones de telecomunicaciones, gobierno, defensa, petróleo y servicios financieros. Su *modus operandi* suele involucrar el uso de tácticas de *spear-phishing*, utilizando señuelos persuasivos que culminan en la implantación de diversas puertas traseras.

https://www.afcea.org/signal-media/scaling-defense-frontier-disas-vision-secure-and-agile-digital-future?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=vBgDh1&_zl=QhsB9

CIBERGUERRA

Ucrania: Las primeras lecciones cibernéticas

A medida que Rusia avanzaba hacia Kiev, el país montó una evacuación digital masiva mientras mantenía servicios digitales vitales para minimizar la inminente crisis humanitaria.

Dos tareas encabezaron la agenda: reubicar servidores vitales y almacenamiento de datos y mover algunos recursos de información fuera del país.

Pocos sabían que la guerra comenzó más de un mes antes de que el primer tanque ruso cruzara la frontera. De hecho, la guerra cibernética comenzó 41 días antes del 24 de febrero, la fecha en que comenzó la guerra cinética.

"Los ataques cibernéticos, que comenzaron el 14 de enero, fueron tan severos, fueron continuos, junto con ataques [distribuidos de denegación de servicio] y con una serie de ataques disruptivos", dijo Victor Zhora, director de transformación digital del Servicio Estatal de Comunicación Especial y Protección de la Información de Ucrania.

https://www.afcea.org/signal-media/cyber-edge/ukraine-first-cyber-lessons?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=vBgDh1&_zl=EhsB9

CERT Ucraniano comparte información sobre las tácticas de exfiltración rápida

Gamaredon, el grupo de cibercriminales respaldado por el estado ruso, ha captado la atención recientemente debido a la velocidad con la que ejecutan sus ataques, logrando extraer datos en menos de una hora después de comprometer un sistema.

También conocido como *Aqua Blizzard, Armageddon, Shuckworm o UAC-0010, Gamaredon*, se estima que este grupo ha infectado miles de sistemas gubernamentales. Se sabe además que este grupo está estrechamente vinculado a la oficina principal del SBU en la República Autónoma de Crimea, la cual fue anexada por Rusia en 2014.

https://unaaldia.hispasec.com/2023/07/cert-ucraniano-comparte-informacion-sobre-las-tacticas-de-exfiltracion-rapida-empleadas-por-gamaredon.html

Las capacidades rusas asociada a la guerra en el ciberespacio. Caso OpsPsic

El artículo describe la estructura general de los destacamentos de operaciones psicológicas del Ejército de la Federación de Rusia. Debido al alcance insuficiente de la información verificable, algunos datos citados en el texto pueden carecer de precisión o estar desactualizados. La Federación de Rusia posee poderosas fuerzas para operaciones psicológicas (PsO). Incluyen varios componentes: (1) Fuerzas PsO y medios de formaciones militares; (2) Fuerzas PsO y medios de servicios especiales; (3) Agencias gubernamentales civiles involucradas en operaciones de información; (4) agencias civiles no gubernamentales (controladas por el gobierno) involucradas en la administración de operaciones de información y (5) organizaciones religiosas dedicadas a la administración de operaciones de información.

https://mil.in.ua/en/articles/russian-army-psyops-units/

La ciberguerra, nuevos desafíos en nuevas modalidades

La Inteligencia Artificial (IA) transformará el escenario con armas autónomas que responderán a decisiones de sistemas informáticos creados especialmente para plataformas militares. Los juegos de guerra (*war-game simulations*) se realizan con algoritmos secretos. Paul Scharre, vicepresidente Ejecutivo y Director de Estudios del CNAS (Center for a New American Security), en su nuevo libro *Four Battlegrounds: Power in the Age of Artificial Intelligence*, plantea cómo la IA está cambiando el poder global. Muchas cosas cambiarán en el concepto de libertad y seguridad con el advenimiento de la Inteligencia Artificial.

https://dplnews.com/la-ciberguerra-nuevos-desafios-en-nuevas-modalidades-ciberseguridad-cibercrimen-ciberterrorismo-dark-web/
https://dplnews.com/ciberseguridad-guerras-del-futuro-han-comenzado/

La National Geoespacial-Intelligence Agency (NGA), logra avances significativos en el proyecto MAVEN basado en AI

El Proyecto Maven, que se estableció en 2017 y tiene como objetivo acelerar el uso de la IA en el ejército, fue transferido tanto a la Agencia Geoespacial Nacional (NGA) como a la Oficina Principal Digital y de IA del Pentágono el año pasado y está preparado para convertirse en un programa oficial de registro en el año fiscal 2024.

Apenas unos meses después de hacerse cargo de partes del proyecto de inteligencia artificial del Pentágono del mencionado proyecto, el director de la (NGA) dijo que la agencia ha logrado "avances significativos", mientras se prepara para convertirse en un programa de registro a principios del próximo año fiscal. año.

"…, hemos logrado avances importantes", expresó el vicealmirante Frank Whitworth en la conferencia GEOINT 2023. "Trabajamos en estrecha colaboración con los comandos para integrar la IA en los flujos de trabajo, ello permitió acelerar la velocidad de toma de decisiones. Esto beneficia el conocimiento del dominio marítimo, la gestión de objetivos y nuestra capacidad para buscar y detectar automáticamente objetos de interés".

https://breakingdefense.com/2023/05/nga-making-significant-advances-months-into-ai-focused-project-maven-takeover/

De ChatGPT a HackGPT: enfrentando la amenaza de ciberseguridad de la IA generativa

Durante los últimos años, los ciberdelincuentes han estado utilizando la inteligencia artificial para piratear sistemas corporativos e interrumpir las operaciones comerciales. Pero las nuevas y poderosas herramientas de inteligencia artificial generativa, como ChatGPT, presentan a los líderes empresariales un nuevo conjunto de desafíos.

From ChatGPT to HackGPT: Meeting the Cybersecurity Threat of Generative AI (mit.edu)

Cómo IBM y AWS se asocian para abordar los desafíos de ciberseguridad y sostenibilidad

Un video que presenta una conversación con Mark Fitch, socio cliente de IBM para AWS en el Reino Unido, en el mismo se comparte información única sobre cómo la asociación está navegando en los entornos de la IA y la computación en la nube, impulsando una infraestructura de TI sostenible, reforzando las medidas de ciberseguridad y aprovechando el potencial de la IA generativa. Permite una comprensión de esta alianza está impulsando

el cambio, preparando a las empresas para los desafíos futuros y dando forma a nuestro futuro digital.

https://www.youtube.com/watch?v=XQ5Y7cDmhyk&t=1s

La IA maliciosa llega a la Dark Web

Nefastos actores no estatales ya están aprovechando la IA para ampliar sus actividades maliciosas. Así como los usuarios legítimos han pasado de explorar ChatGPT a crear herramientas similares, lo mismo ha sucedido en el sombrío mundo del cibercrimen.

https://www.homelandsecuritynewswire.com/dr20230823-malicious-ai-arrives-on-the-dark-web

Las bandas internacionales de ransomware

En realidad, no pasa una semana sin que se produzcan ataques que afecten a gobiernos, escuelas, hospitales, empresas y organizaciones benéficas de todo el mundo. Estos ataques tienen importantes costos financieros y sociales. Hoy en día se reconoce ampliamente que el ransomware constituye una gran amenaza y un desafío para la sociedad moderna, y se espera que los delincuentes sigan adaptando sus estrategias y causando daños generalizados durante muchos años más.

https://www.homelandsecuritynewswire.com/dr20230829-international-ransomware-gangs-are-evolving-their-techniques-the-next-generation-of-hackers-will-target-weaknesses-in

CIBERCONFIANZA

Confianza cero puede garantizar el futuro de la ciberseguridad

Frente al aumento en el volumen y complejidad de los ciberataques, y los entornos híbridos de trabajo, una estrategia de confianza cero permite asegurar mejor a las organizaciones.
https://www.computerweekly.com/es/noticias/252526243/Confianza-cero-puede-garantizar-el-futuro-de-la-ciberseguridad

3 estrategias para mejorar habilidades en el futuro ciberespacio

Con el auge de las tecnologías de IA, metaverso y web3 (como VR, blockchain y NFT), está claro que los tipos de habilidades que necesitan las organizaciones están evolucionando. El problema es una enorme escasez global de habilidades en torno a las tecnologías futuras.

https://www.forbes.com/sites/bernardmarr/2023/07/17/3-strategies-to-overcome-the-future-skills-shortage/?sh=73dc0b942b75

El futuro del metaverso, según su inventor

En una discusión reciente, como parte de Global Collaboration Village, el Foro Económico Mundial recibió a Neal Stephenson para escuchar sus perspectivas sobre el potencial de interacción en este medio virtual inmersivo, quien se apresuró a señalar la importancia de fomentar un enfoque abierto y colaborativo para desarrollar el metaverso. Agregó "Podemos y debemos adoptar un enfoque abierto y responsable para desarrollar el metaverso. Aquí hay una tecnología, como tantas otras innovaciones sorprendentes de las últimas décadas en el espacio de Internet, que realmente puede enriquecer miles de millones de vidas y conectar a personas de todo el mundo". mundo."

Cerrando el foro Stephenson dijo que: "La responsabilidad es de todos nosotros para crear algo que realmente aporte valor a las vidas humanas. El metaverso puede remodelar los negocios, la educación y la vida social. Sin embargo, se debe trabajar mucho para que trascender la mera novedad para convertirse en una parte real de nuestra experiencia humana colectiva".

https://www.weforum.org/agenda/2023/05/how-does-one-of-the-founders-of-the-metaverse-envision-its-future/?utm_source=sfmc&utm_medium=email&utm_campaign=2804519_WeeklyAgenda2June2023&utm_term=&emailType=Agenda%20Weekly

El FBI en una operación internacional derrota a una de las familias de malware más activas

En una operación policial conjunta denominada «Operación *Duck Hunt*» (Operación «Caza de Patos» en español) coordinada por el FBI, se ha logrado derrocar a la famosa familia de *malware* de Windows conocida como *QakBot* quien ha dejado su huella en más de 700,000 dispositivos alrededor del mundo, orquestando operaciones relativas a fraudes financieros y a la ejecución de *ransomware*.

https://www.msn.com/es-es/noticias/tecnologia/as%C3%AD-ha-ca%C3%ADdo-qakbot-la-mayor-botnet-de-la-historia-controlaba-700000-pcs-en-todo-el-mundo-y-caus%C3%B3-cientos-de-millones-en-p%C3%A9rdidas/ar-AA1g0ujw

https://techcrunch.com/2023/09/01/fbi-qakbot-takedown-operation-duck-hunt/

https://unaaldia.hispasec.com/2023/08/el-fbi-en-una-operacion-internacional-consigue-derrocar-a-qakbot-una-de-las-familias-de-malware-mas-activas.html

TECNOLOGÍA

Libro tecnologías de operación 2023

El libro contiene información desde la perspectiva del empleo de tecnologías en operaciones espaciales, con capítulos acerca de: (1) Lecciones aprendidas de Ucrania, EE. UU. se reinventa con Fuerzas Especiales, para una lucha con China; (2) El operador especial del mañana más 007 y menos Iroman; (3) ¿Cómo las fuerzas de operaciones

especiales deben enfrentar los desafíos de una nueva era?; (4) El futuro paralas operaciones especiales es una Inteligencia Artificial autónoma colaborativa y portátil; (5) El presupuesto de Operaciones especiales debe aumentar un 20% en I+D

El acceso a este libro requiere que Ud. ingrese datos personales

https://www.defenseone.com/assets/special-operations-technology-2023/portal/

Inteligencia Artificial y Defensa

Un análisis a cerca de la Inteligencia Artificial, sus ramas y categorizaciones, con una mirada de cómo puede impactar su empleo en las fuerzas armadas, y algunos aspectos a tener en cuenta para su segura implementación

https://www.pucara.org/post/el-impacto-de-la-inteligencia-artificial-en-la-defensa

La computación en la nube

La computación en la nube ha permitido la transformación empresarial y ha marcado el comienzo de un crecimiento económico masivo. Ha revolucionado marcos informáticos completos, pero no sin expandir exponencialmente la superficie de ataque y redefinir las líneas de frente de las amenazas existentes y emergentes. Apesar de la carrera hacia la nube, el progreso hacia la madurez de la seguridad en la nube ha sido lento... pero no es demasiado tarde.

https://www.c4isrnet.com/opinion/2023/09/01/cloud-computings-balancing-act-are-we-in-a-mushroom-cloud-moment/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-cyber

Ropa Inteligente, para el espionaje

El gobierno federal de los EE.UU. ha desembolsado al menos 22 millones de dólares en un esfuerzo por desarrollar ropa "inteligente" que espíe a quien la usa y su entorno. Al igual que en proyectos anteriores de lanzamiento a la luna financiados por agencias militares y de inteligencia, la inspiración puede haber venido de la ciencia ficción y las superpotencias, pero las aplicaciones básicas están a la altura del gobierno: vigilancia y recopilación de datos.

https://theintercept.com/2023/09/02/smart-epants-wearable-technology/

Modelos Matemático para la gestión de la incertidumbre

La gestión de la incertidumbre de riesgos de seguridad es un campo que se ocupa de evaluar y mitigar las acciones de posibles amenazas que pueden afectar a la integridad de activos tangibles e intangibles: personas, bienes o información, entre otros. Es un tema complejo que requiere el uso de modelos matemáticos adecuados. Estos permiten cuantificar y evaluar los posibles escenarios de amenaza, vulnerabilidad e impacto, así como las medidas de mitigación y respuesta. Se aplican en diversos ámbitos, como la seguridad industrial, la ciberseguridad, la seguridad vial o la seguridad nacional.

http://alfredoyuncoza.blogspot.com/2023/08/modelos-matematicos-para-la-gestion-de.html

CIBERFORENSIA

Informes CISA

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EEUU, estos boletines proporcionan un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad (NVD) del Instituto Nacional de Estándares y Tecnología (NIST).

Semana del 5 de junio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-163
Semana del 12 de junio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-171
Semana del 19 de junio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-177
Semana del 26 de junio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-184
Semana del 3 de julio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-191
Semana del 10 de julio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-198
Semana del 17 de julio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-205
Semana del 24 de julio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-212
Semana del 31 de julio de 2023	https://www.cisa.gov/news-events/bulletins/sb23-219
Semana del 7 de agosto de 2023	https://www.cisa.gov/news-events/bulletins/sb23-226
Semana del 14 de agosto de 2023	https://www.cisa.gov/news-events/bulletins/sb23-233
Semana del 21 de agosto de 2023	https://www.cisa.gov/news-events/bulletins/sb23-240
Semana del 28 de agosto de 2023	https://www.cisa.gov/news-events/bulletins/sb23-249

A tener en cuenta:

1. Mozilla ha publicado actualizaciones de seguridad para abordar las vulnerabilidades de
    a. Firefox 116 https://www.mozilla.org/en-US/security/advisories/mfsa2023-29/ ,
    b. Firefox ESR 115.1 https://www.mozilla.org/en-US/security/advisories/mfsa2023-31/
    c. Firefox ESR 102.14. https://www.mozilla.org/en-US/security/advisories/mfsa2023-30/

    Un atacante podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado.

Archivos maliciosos de Word en PDF

Expertos en ciberseguridad del equipo de JPCERT/CC han alertado sobre una ingeniosa técnica de elusión de antivirus que implica la inserción de un archivo malicioso de *Microsoft Word* en un archivo *PDF*, este desarrollo en medio de un aumento en las campañas de ingeniería social supone una creciente preocupación por los expertos, que advierten sobre nuevas técnicas para evadir las protecciones en los sistemas.

1. https://unaaldia.hispasec.com/2023/09/maldoc-en-pdf-y-otras-tecnicas-de-ingenieria-social.html

RESUMEN DE NOTICIAS

Créase la Mesa Interministerial sobre Inteligencia Artificial

Créase la Mesa Interministerial sobre Inteligencia Artificial en la órbita de la JEFATURA DE GABINETE DE MINISTROS, como ámbito transversal para abordar el avance y aplicación de la Inteligencia Artificial en diversos sectores de la economía y de la sociedad, de conformidad con un marco ético, de desarrollo sostenible y de transformación digital, y con la finalidad de diseñar una estrategia integral al respecto para ser aplicada por el PODER EJECUTIVO NACIONAL.

La citada será presidida por la JEFATURA DE GABINETE DE MINISTROS y será coordinada por esta conjuntamente con la SECRETARÍA DE ASUNTOS ESTRATÉGICOS de la PRESIDENCIA DE LA NACIÓN, quienes adoptarán las medidas necesarias para su funcionamiento.

Estará integrada por las siguientes jurisdicciones: la JEFATURA DE GABINETE DE MINISTROS, el MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN, el MINISTERIO DE DEFENSA, el MINISTERIO DE ECONOMÍA, el MINISTERIO DE RELACIONES EXTERIORES, COMERCIO INTERNACIONAL Y CULTO, el MINISTERIO DE SALUD, el MINISTERIO DE SEGURIDAD, el MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL y la SECRETARÍA DE ASUNTOS ESTRATÉGICOS de la PRESIDENCIA DE LA NACIÓN.

https://www.boletinoficial.gob.ar/detalleAviso/primera/293710/20230908