XXXVI CONGRESO ANUAL
NUEVO ORDEN INTERNACIONAL Y REESTRUCTURACIÓN DEL PODER: CRISIS, FRAGMENTACIÓN Y DESAFÍOS

UNIVERSIDAD ANÁHUAC MAYAB

MÉRIDA, YUCATÁN

Desafíos contemporáneos en el escenario internacional: reflexiones sobre la crisis sistémica post-pandemia, el conflicto entre Rusia y Ucrania y la ciberseguridad

- **La agenda de ciberseguridad en las Relaciones Internacionales**

Lic. Noradilda Calderón Lara

19 de octubre de 2023

UNAM POSGRADO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
Τό ζῳον πολιτικόν
FACULTAD DE CIENCIAS POLITICAS Y SOCIALES

AMEI
Asociación Mexicana de Estudios Internacionales, A. C.

EL ECONOMISTA

Departamento de Estado de Estados Unidos crea una Oficina de Ciberespacio y Política Digital

kies propias y de terceros para realizar el análisis de la navegación de los usuarios y mejorar nuestros servicios. Si continúa navegando, consideramos que acepta su us

byte 20 años

ACTUALIDAD · CIO/CISO EN 20 LÍNEAS · MUJERES TIC · CIBERSEGURIDAD · A FONDO · COMPARATIVA · TENDENCIAS

Inicio › Ciberseguridad › La invasión rusa de Ucrania dispara hasta un 24% los ciberataques

La invasión rusa de Ucrania dispara hasta un 24% los ciberataques

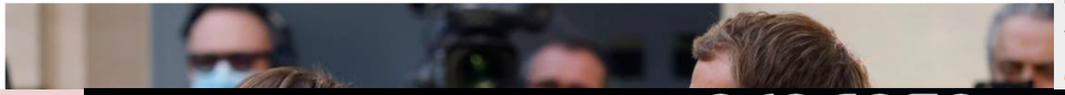
The Washington Post
La democracia muere en la oscuridad

EL UNIVERSAL MXM VIDEOS PODCAST NEWSLETTERS

Término de búsqueda SUSCRÍBETE SALA PL

EU se unirá a una asociación internacional de ciberseguridad

La vicepresidenta de Estados Unidos, Kamala Harris, anunció el apoyo de su país al "Llamamien París por la confianza y la seguridad en el ciberespacio"



veintitres

TENDENCIAS 05-10-2023 17:12 Hs.

Kiev reivindica los ciberataques con aeropuertos rusos

Todas las noticias sobre ataques cibernéticos y hackers

Por Redacción Veintitrés

Israel intensifica la vigilancia de los palestinos con un programa de reconocimiento facial en Cisjordania

Por Elizabeth Dwoskin

8 de noviembre de 2021 a las 2:00 am EST

EUROPA · EE UU · MÉXICO · AMÉRICA LATINA · ORIENTE PRÓXIMO · ASIA · ÁFRICA · FOTOS · OPINIÓ

proceso

Nacional · Revista Proceso · Economía · Internacional · Opinión · Ciencia y Tecnología · Cultura · Dep

sin límites es conocer las perspectivas de todos los ciudadanos US$ 1 primer mes SUSCRÍBETE

SEDENA

"Hackeo" a la Sedena y desidia en ciberseguridad

No sólo se trata de una institución que procura la seguridad nacional, como la Sedena, sino de la indolencia que ha tenido México en materia de ciberseguridad en

UCRANIA >

Ucrania denuncia un ciberataque a gran escala contra el sistema informático del Gobierno

Kiev dice que “es pronto” para señalar un culpable pero que Rusia ya fue origen de acciones similares. Mientras, Moscú asegura que se le ha “acabado la paciencia” para esperar compromisos de EE.UU. y la OTAN

Ciberespacio

"Es el entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos usando redes informáticas". (Manual de Tallín, 2017)

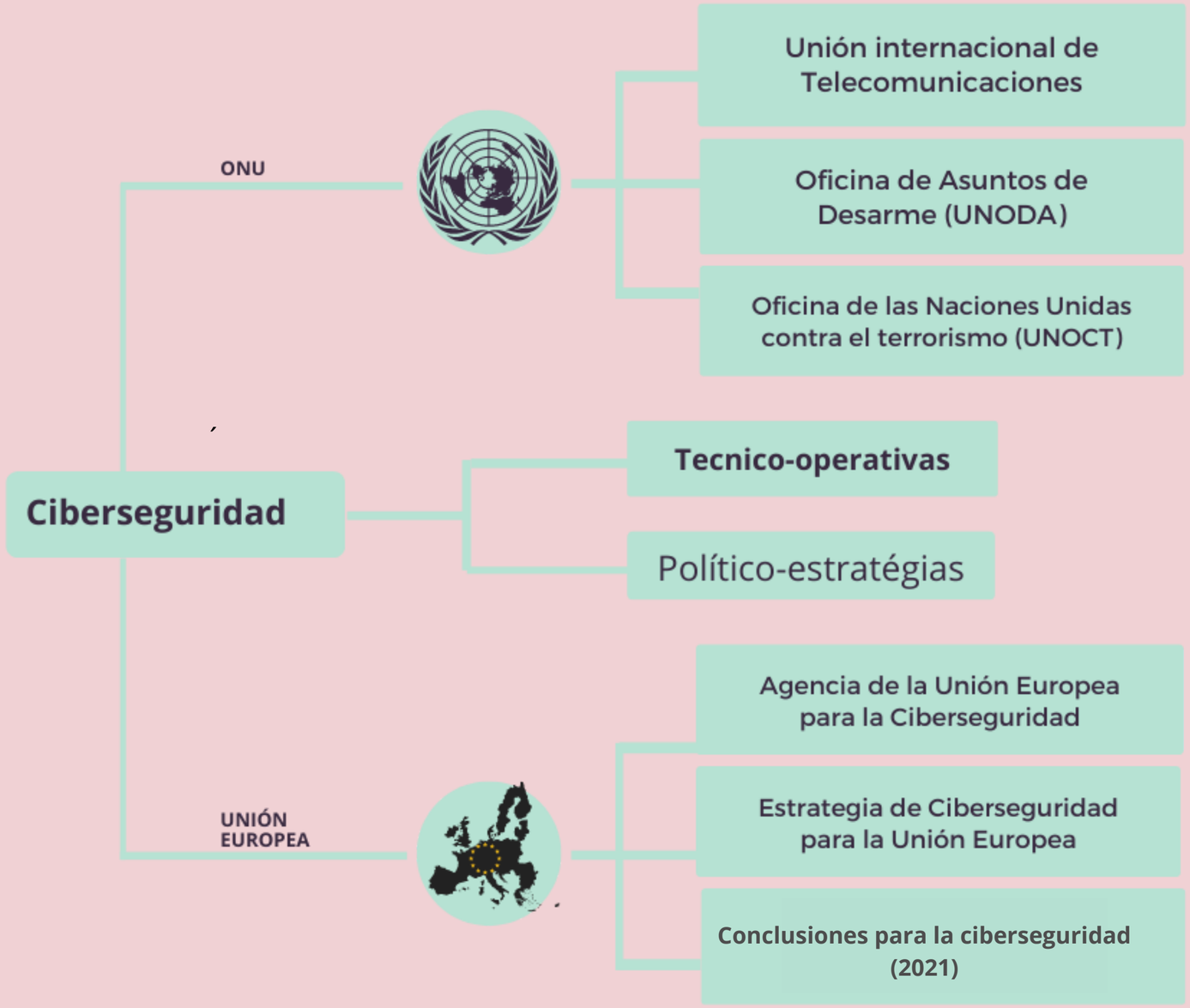
La voz ciberespacio está ligada al término *kibernetes*. Así eran llamados los marinos que se encargaban de conducir los barcos en la antigua Grecia.

En 1948 el matemático estadounidense N. Wiener, definió el término cibernética como: *the scientific study of control and communication in the animal and the machine*.

La primera mención del término ciberespacio, se remonta a 1984 en la obra *Neuromante* del escritor norteamericano Willian Gibson.

De manera que la vigencia del *kybernetike* (arte de navegar) no dista mucho de sus orígenes, “ahora se navega en un mar de información, en el que también, si no tenemos cuidado, podemos naufragar”. (2022, Ortega Morán)

"La ciberseguridad es el conjunto de herramientas **políticas**, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los **activos** de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los **sistemas** de comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad" (UIT, 2010)



Ciberdefensa

"La ciberdefensa incluye tres categorías complementarias: proactiva, activa y regenerativa. Las actividades 'proactivas' fortalecen el entorno cibernético y mantienen la máxima eficiencia para la infraestructura cibernética y las funciones de la misión. Las actividades 'activas' detienen o limitan el daño del adversario cibernético en tiempo cibernético relevante. Las actividades 'regenerativas' restauran la eficacia o la eficiencia de la misión después de un ciberataque exitoso."
(Herring y Willet, 2014)

"Capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia" (JID, 2020)

"El término ciberdefensa, que se orienta a las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; sin soslayar que en los nuevos escenarios que plantea el ciberespacio, puede incidir en el momento de trazar rutas estratégicas plausibles para el cumplimiento de las diversas misiones militares de ciberdefensa"
(Virilio, citado en Borbúa, V., Herrera, R., & Reyes, R., 2017)

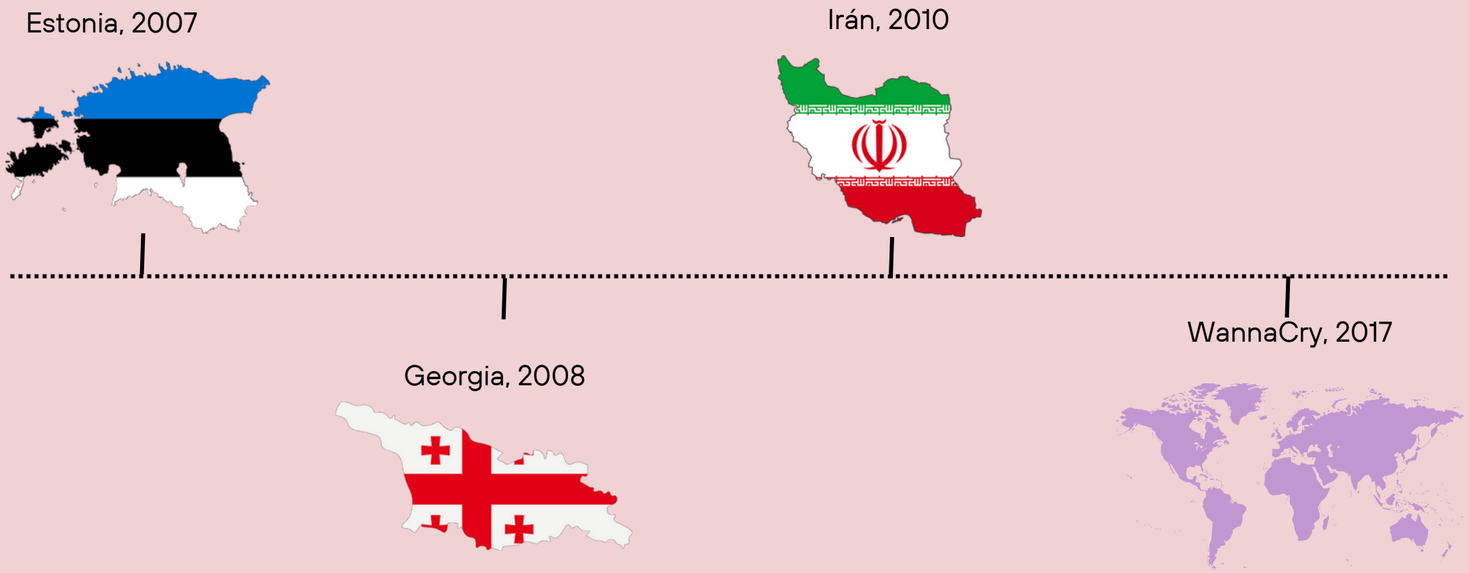
Ciberataque

Un **ciberataque** es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización. Usualmente, el atacante busca algún tipo de beneficio con la interrupción de la red de la víctima. (Cisco, 2021)

1.Ciberataques a infraestructuras informáticas.

a) Ciberataques con intención de tomar el control de otros dispositivos o sistemas informáticos.
b) Ciberataques con intención de obtener información confidencial.

2. Ciberataques a infraestructuras físicas.



CONVENIO DE BUDAPEST

Convenio del Consejo de Europa sobre Ciberdelincuencia

2001

2004

UE

Agencia Europea de Seguridad de las Redes y de la Información, (ENISA)

OCS

Reglas de conducta en el Área de Segruidad de la Información

2015

2016

OTAN

El ciberespacio como cuarta dimensión de operaciones militares junto con la tierra, mar y aire.

UE

Brújula Estratégica

2022

2022

OTAN

Concepto Estratégico

Gracias por su atención

noradilda@politicas.unam.mx