GOBIERNO DE MÉXICO | MARINA | SEDENA

Glosario de Términos SEDENA-MARINA en materia de Seguridad en el Ciberespacio

JUNIO 2021

Unidad de Ciberseguridad (UNICIBER) del Estado Mayor General de la Armada

Centro de Operaciones del Ciberespacio (C.O.C) del Estado Mayor de la Defensa Nacional

Glosario de Términos SEDENA-MARINA en materia de Seguridad en el Ciberespacio

La primera versión del Glosario de Términos Homologados Técnicamente en Materia de Seguridad en el Ciberespacio SEDENA-SEMAR fue publicado en 2013 al interior de las Fuerzas Armadas Mexicanas, la cual incluyó nueve términos generales; con la presente actualización, sigue vigente el propósito de contar con un listado de aquellos comúnmente empleados al abordar el tema de la "Seguridad en el Ciberespacio".

En este sentido, en esta nueva versión, catalogada como de uso público, se han actualizado los términos anteriores y se han agregado nuevos, algunos relacionados con las capacidades nacionales que el Estado mexicano ha logrado desarrollar, con la visión de alcanzar la Seguridad en el Ciberespacio, como son: Seguridad de la Información, Ciberseguridad y ahora la Ciberdefensa.

El presente documento pretende ser de consulta para las investigaciones académicas, los trabajos conjuntos con las instancias de Seguridad Nacional, y todo organismo público o privado que lo requiera para impulsar la legislación, la cooperación, la innovación, investigación y desarrollo tecnológico, para continuar generando las capacidades del Estado mexicano en favor de la seguridad de la sociedad mexicana en el Ciberespacio, en cumplimiento de las atribuciones y misiones de la SEDENA y MARINA en materia de Seguridad Nacional.

Es importante mencionar que el "Glosario de Términos SEDENA-MARINA en Materia de Seguridad en el Ciberespacio" está sujeto a un proceso de mejora continua a través del C.O.C. del Estado Mayor de la Defensa Nacional y la UNICIBER del Estado Mayor General de la Armada.

A

Acción en el Ciberespacio: esfuerzos que se realizan mediante el empleo de las Tecnologías de la Información y Comunicaciones (TIC) para defender y/o atacar activos de información en o a través del Ciberespacio.

Acción Defensiva en el Ciberespacio (Ciberdefensiva): acción pasiva de las Fuerzas Armadas en o a través del Ciberespacio con el objetivo de neutralizar o mitigar los efectos de Ciberataques, manteniendo la capacidad operativa propia.

Acción Ofensiva en el Ciberespacio (Ciberofensiva): acción activa de las Fuerzas Armadas en o a través del Ciberespacio con el objetivo de limitar o destruir la capacidad operativa de un adversario.

Activo(s) de Información: persona o tecnología que conoce o contiene información, y que, por su importancia, deben ser protegidos para mantener su confidencialidad, integridad y disponibilidad, incluyendo los activos de TIC.

Activo(s) de Tecnologías de la Información y Comunicaciones (Activo de TIC): programas de cómputo, bienes informáticos, soluciones o servicios tecnológicos, las redes, sistemas o aplicativos, sus componentes y bases de datos, archivos electrónicos y la información contenida en éstos, pudiendo o no formar parte de una Infraestructura Esencial o Crítica de Información.

Amenaza Persistente Avanzada (APT): tipo de Ciberataque con el propósito de acceder a una red o sistema, infiltrándose de manera anónima, sigilosa y desapercibida para tomar el control y perpetuarse de los activos de TIC hasta obtener ventaja estratégica en un periodo de tiempo prolongado mediante el empleo de técnicas, tácticas y procedimientos (TTPs). También se denomina con estas siglas a algunos grupos organizados de expertos asociados o no a un Estado-Nación.

Análisis de Ciberriesgo: procedimiento para estimar riesgos de Seguridad en el Ciberespacio derivados de la manifestación de amenazas; primero se determina el nivel de vulnerabilidad del activo y posteriormente se evalúan los riesgos que se le asocian, para finalmente calcular el impacto e implementar medidas y controles que reduzcan los efectos a un nivel aceptable.

Áreas de Conocimiento del Ciberespacio: son los conocimientos profesionales y técnicos relacionados a la electrónica, informática, Seguridad Informática, cómputo, desarrollo de sistemas y equipos de TIC, comunicaciones, espectro electromagnético y análisis de información.

Avatar (Ciberpersona): representación o identidad virtual de una persona, grupo o entidad para navegar e interactuar en el Ciberespacio sin dar a conocer su identidad real en el mundo físico.

C

Campo de Adiestramiento en el Ciberespacio: zona aislada del Ciberespacio para el desarrollo de capacidades de una fuerza de Seguridad en el Ciberespacio y/o fuerza de Ciberdefensa, favoreciendo la simulación de Ciberoperaciones dentro de un ambiente controlado.

Capacidades de Seguridad en el Ciberespacio: capacidades basadas en los recursos humanos, materiales, tecnológicos y financieros que se destinan, para proporcionar Seguridad en el Ciberespacio; entendidas como Seguridad de la Información, Ciberinteligencia, Ciberseguridad y Ciberdefensa en su respectivo ámbito de atribuciones y competencias.

Caza de Ciberamenazas: proceso operativo, dinámico y proactivo de Ciberdefensa y Ciberseguridad, orientado a la detección y contención de Ciberamenazas que evaden las medidas y controles de seguridad tecnológicos tradicionales.

Ciberamenaza: fuente potencial externa o interna, con capacidad de provocar un efecto adverso en o a través del Ciberespacio.

Ciberarma: programa de cómputo, bien informático, sistema o aplicativo y sus componentes, específicamente diseñados para causar un daño o efecto perjudicial a un activo de información o de TIC, pudiendo tener consecuencias físicas en los ámbitos o entornos operacionales convencionales.

Ciberataque: acción ofensiva o maliciosa, externa o interna, con la intención de causar un efecto adverso en o a través del Ciberespacio.

Cibercrisis: evento inesperado donde las capacidades de Seguridad en el Ciberespacio de una organización se ven rebasadas o han fracasado por una(s) Ciberamenaza(s) de forma temporal o permanente.

Ciberdefensa: capacidad de un Estado-Nación traducida en acciones, recursos y mecanismos en materia de Seguridad y Defensa nacionales en el Ciberespacio, para prevenir, identificar y neutralizar Ciberamenazas o Ciberataques, incluidos los que atentan contra instalaciones estratégicas de un país.

Ciberespacio: entorno o ámbito intangible de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones, en el que se comunican e interactúan las entidades públicas, privadas y la sociedad en general, coadyuvando al desarrollo nacional y garantizando el ejercicio de los derechos y libertades como en el mundo físico. Para las Fuerzas Armadas, se considera el quinto entorno operacional para proporcionar Seguridad y Defensa.

Ciberespionaje: es el acceso ilícito a las TIC en o a través del Ciberespacio, para recabar información sensible del campo político, económico, social, militar o diplomático.

Ciberguerra: es una nueva clasificación de la guerra, donde el Ciberespacio es empleado como entorno de operaciones para la conducción de acciones hostiles.

Ciberidentidad: individuos u organizaciones con registro público, que mantiene direcciones de Internet conforme a la normatividad, haciendo referencia a nombres de organizaciones o entidades en el mundo físico.

Ciberinteligencia: actividad de la inteligencia que hace uso del Ciberespacio, para obtener información de valor de todo tipo de amenazas que atentan contra las organizaciones o que impactan en la Seguridad Nacional del Estado-Nación. Para las Fuerzas Armadas, esta actividad apoya a los entornos o ámbitos de tierra, mar, aire, espacio ultraterrestre y Ciberespacio.

Ciberresiliencia: capacidad de un sistema, organización o Estado-Nación, en o a través del Ciberespacio para seguir operando, pese a estar sometido a un Ciberincidente o Ciberataque; incluye la capacidad de recuperarse en el menor tiempo posible para la continuidad de operaciones.

Ciberriesgo: probabilidad de que una Ciberamenaza aproveche y explote una vulnerabilidad, y cuyo resultado provoque un impacto negativo a una organización o a la Seguridad Nacional.

Ciberseguridad: capacidad de un Estado-Nación y de todos los sectores de la sociedad para generar y aplicar políticas públicas, legislación, normas, procedimientos y controles tecnológicos para la protección de Infraestructuras de Información Esenciales e Infraestructuras Críticas de Información.

Ciberterrorismo: empleo del Ciberespacio como fin o medio para generar terror o pánico generalizado, con la finalidad de influir en las decisiones o imponer ideologías contra la sociedad y/o las instituciones de un Estado-Nación.

Ciberterreno Clave: conjunto de elementos de cualquiera de las capas del Ciberespacio (humana, Ciberhumana, cognitiva, lógica, TIC y geográfica) que facilitan las actividades, operaciones o funciones esenciales para la misión y cuya destrucción, interrupción o captura generaría una ventaja operativa para el adversario.

Ciberusurpador: individuos u organizaciones que se registran y mantienen direcciones de Internet parecidas o que hacen referencia a nombres de organizaciones o entidades en el mundo real en o a través del Ciberespacio.

CSIRT Ciberdefensa: centros técnicos operativos con capacidades nacionales para planear, conducir y ejecutar actividades de Seguridad en el Ciberespacio, para la protección de la Infraestructura Crítica de Información de las Fuerzas Armadas y las correspondientes a las Instalaciones Estratégicas del país que les sean asignadas, en coadyuvancia con el esfuerzo nacional para el mantenimiento de la integridad, estabilidad y permanencia del Estado-Nación.

D

Delitos Cibernéticos (Ciberdelitos): acciones ilícitas que se encuentran tipificadas en la legislación nacional y/o internacional vigentes, perpetradas en o través del Ciberespacio utilizando las Tecnologías de la Información y las Comunicaciones como medio o fin.

E

Equipo de Misión Nacional en el Ciberespacio: un equipo técnico conformado por personal de las instancias de Seguridad Nacional; pudiendo incorporarse personal de organismos públicos y privados, para coadyuvar en el esfuerzo nacional en el cumplimiento de misiones de Seguridad en el Ciberespacio.

Equipos de Misión de Fuerzas Armadas en el Ciberespacio: equipos tácticos-técnicos conformados por personal de las Fuerzas Armadas, para realizar acciones defensivas u ofensivas en el cumplimiento de misiones de Seguridad en el Ciberespacio.

F

Fuerza Laboral del Ciberespacio: son los profesionales y técnicos de las instituciones y organismos del sector defensa, público y privado, que se desempeñan en las áreas de conocimiento del Ciberespacio.

Fuerza de Seguridad en el Ciberespacio: es el personal de las instancias de Seguridad Nacional; así como de organismos públicos y privados, especializados en Seguridad de la Información, Ciberseguridad y/o Ciberdefensa en sus respectivos ámbitos de competencia.

Fuerza de Ciberdefensa: es la fuerza de Seguridad en el Ciberespacio de las Fuerzas Armadas, para realizar acciones defensivas u ofensivas en el cumplimiento de las misiones en materia de Seguridad Nacional.

H

Hacktivismo o activismo digital: fenómeno que se genera en o a través del Ciberespacio para expresar ideas que promueven actividades de desobediencia civil, propaganda o proselitismo político, social o ideológico.

I

Incidente de Ciberseguridad (Ciberincidente): interrupción, acceso no autorizado o cualquier falla que provoque afectación a los activos de información de las Infraestructuras Críticas de Información e Infraestructuras de Información Esenciales, pudiendo concretarse o no en una acción de Ciberdelito o de Ciberataque.

Infraestructura(s) Crítica(s) de Información (ICI): infraestructuras de Información Esenciales consideradas estratégicas por estar relacionadas con la provisión de bienes y de prestación de servicios públicos esenciales y cuya afectación pudiera comprometer la Seguridad Pública o la Seguridad Nacional en términos de las leyes en la materia.

Infraestructura(s) de Información Esencial(es) (IIE): las redes, servicios, equipos e instalaciones asociados o vinculados con activos de TIC y de Tecnologías de Operación (TO), cuya afectación, interrupción o destrucción, tendría un impacto en el individuo u organismos públicos o privados.

Inteligencia de Ciberamenazas: proceso de la Ciberinteligencia que analiza Ciberincidentes, Ciberamenazas y/o Ciberataques que atentan contra los activos de información de una organización o que impactan en la Seguridad Nacional del Estado-Nación, en el que se obtienen indicadores de compromiso y atribución para poder contrarrestarlos.

O

Operaciones en el Ciberespacio (Ciberoperaciones): actividades que realiza el Estado-Nación en o a través del Ciberespacio, para proporcionar Seguridad a la sociedad. Para las Fuerzas Armadas son consideradas como operaciones militares en el Ciberespacio en el cumplimiento de las misiones encomendadas.

P

Panorama Operacional del Ciberespacio: es la situación estratégica, operacional y táctica actual y futura del entorno o ámbito del Ciberespacio, mediante el cual se apoya la toma de decisiones en el planeamiento, conducción y ejecución de las Ciberoperaciones.

S

Seguridad de la Información: capacidad de las instituciones y organismos públicos o privados de preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de riesgos, así como su autenticidad, auditabilidad, trazabilidad, protección a la duplicación, no repudio y legalidad.

Seguridad en el Ciberespacio: es la condición que busca toda sociedad en o a través del Ciberespacio, alcanzada mediante acciones de Seguridad de la Información, Ciberseguridad y Ciberdefensa como capacidades de un Estado-Nación.

Sistema de Armas para el Ciberespacio: sistema que integra funciones de mando y control, Ciberarmas y apoyos técnicos necesarios para proporcionar capacidades de Ciberdefensa de un Estado-Nación.

T

Tecnologías de Operación (TO): son las TIC que generan o detectan un cambio a través del control y/o monitoreo de procesos y eventos en las Infraestructuras Críticas de Información o Infraestructuras de Información Esenciales.

V

Vulnerabilidad en el Ciberespacio: falla, ausencia o debilidad en el diseño, implementación u operación de un activo de información o de las TIC, pudiendo ser explotada por una Ciberamenaza, con lo cual se materializan los riesgos.

El presente Glosario de Términos fue desarrollado por el personal Especialista del Centro de Operaciones del Ciberespacio del E.M.D.N. (C.O.C. E.M.D.N.) y Unidad de Ciberseguridad del E.M.G.A. (UNICIBER E.M.G.A.), definidos como:

Centro de Operaciones del Ciberespacio del E.M.D.N. (C.O.C. E.M.D.N.): es el CSIRT del Estado Mayor de la Secretaría de la Defensa Nacional. Tiene como misión: "Planear, coordinar, dirigir y ejecutar los esfuerzos del Ejército y Fuerza Aérea Mexicanos, para identificar las amenazas provenientes del Ciberespacio y mitigar sus efectos, así como prevenir y responder a incidentes que atenten contra la información e infraestructura crítica soportada en las Tecnologías de la Información y Comunicaciones de la Secretaría de la Defensa Nacional".

Unidad de Ciberseguridad del E.M.G.A. (UNICIBER E.M.G.A.): es el CSIRT del Estado Mayor General de la Armada de México. Tiene como misión: "Planear, conducir y ejecutar actividades de Seguridad de la Información, Ciberseguridad y Ciberdefensa, para la protección de la Infraestructura Crítica Institucional, y coadyuvar en el esfuerzo nacional para el mantenimiento de la integridad, estabilidad y permanencia del Estado Mexicano".

Ciudad de México, junio de 2021

Vo. Bo.

Secretaría de Marina
Estado Mayor General de la Armada
Unidad de Ciberseguridad

Contralmirante C.G. D.E.M.
Jefe de la UNICIBER E.M.G.A.
Jesús Arrellano Rodarte

Vo. Bo.

Secretaría de la Defensa Nacional
Estado Mayor de la Defensa Nacional
Centro de Operaciones del Ciberespacio

Gral. Brigadier I.C.E. D.E.M.
Director del C.O.C. E.M.D.N.
Francisco Javier Villa Vargas

REFERENCIAS:

- Diccionario de términos, UNAM CERT, disponible en: https://www.seguridad.unam.mx/diccionario/a, México, consultado en enero de 2021.
- Estándar ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity, Organización Internacional de Normalización (ISO). EE.UU., 2012.
- Estrategia Conjunta de Ciberdefensa SEDENA -SEMAR. Secretaría de la Defensa Nacional – Secretaría de Marina, México, 2019.
- Estrategia Nacional de Ciberseguridad, Gobierno de México, disponible en: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad, 2017.
- Framework for Improving Critical Infrastructure Cybersecurity, Instituto Nacional de Estándares y Tecnología, 2014.
- Glosario de Términos de Ciberseguridad, Instituto Nacional de Ciberseguridad de España (INCIBE), disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf , España 2107.
- Glosario de términos en Ciberseguridad, Centro Especializado en Respuesta Tecnológica de la Policía Federal (ahora Guardia Nacional). https://www.gob.mx/policiafederal/articulos/glosario-de-terminos-en-ciberseguridad?idiom=es Consultado en enero, 2021.
- Términos homologados técnicamente en Materia de Seguridad en el Ciberespacio SEDENA-SEMAR, 2013.
- Guía de Ciberdefensa, Orientaciones para el diseño, planeamiento, implantación y desarrollo de una Ciberdefensa Militar. Junta Interamericana de Defensa (JID). https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf, consultado en enero de 2021.
- Guía de Seguridad (CCN-STIC-401), Glosario y Abreviaturas. Centro Criptológico Nacional, España, 2015.
- Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI). Secretaría de la Función Pública. D.O.F. 23 de julio de 2018.
- Manual de Operaciones Militares, Secretaría de la Defensa Nacional, México, 2017.
- Manual de Tallin 2.0, Sobre el Derecho Internacional Aplicable a las Ciberoperaciones, Segunda Edición, Cambridge University Press, EE.UU., 2017.
- Términos homologados técnicamente en materia de Seguridad en el Ciberespacio SEDENA-SEMAR. Secretaría de la Defensa Nacional-Secretaría de Marina, 2013.