SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

MARINA
SECRETARÍA DE MARINA

"GLOSARIO DE TÉRMINOS SEDENA-SEMAR EN MATERIA DE CIBERSEGURIDAD Y CIBERDEFENSA"

Centro de Operaciones del Ciberespacio del Estado Mayor Conjunto de la Defensa Nacional.

Coordinadora General del Ciberespacio del Estado Mayor General de la Armada.

JULIO DE 2024

"GLOSARIO DE TÉRMINOS SEDENA-SEMAR EN MATERIA DE CIBERSEGURIDAD Y CIBERDEFENSA"

A

Acción en el Ciberespacio: Cualquier actividad, operación o medida defensiva u ofensiva tomada con el empleo de las Tecnologías de la Información y Comunicaciones para prevenir, detectar, mitigar, neutralizar o responder ante amenazas y ataques que puedan poner en peligro la seguridad e integridad de la infraestructura en el Ciberespacio.

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 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.

Ámbito (Dominio o entorno) de operaciones: Entorno (aire, mar, tierra, espacio y Ciberespacio) de interés e influencia en el que se llevan a cabo actividades, funciones y operaciones militares.

Amenaza Persistente Avanzada (APT): Tipo de Ciberamenaza 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. También se denomina con estas siglas a algunos grupos organizados de personas expertas asociadas o no a un Estado-Nación.

C

Campo de Adiestramiento en el Ciberespacio: Zona aislada del Ciberespacio para el adiestramiento 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.

Ciberactivismo (Hacktivismo o activismo digital): Uso del Ciberespacio para desarrollar actividades de desobediencia civil, propaganda o proselitismo para promover un cambio político o social.

Ciberamenaza: Fuente potencial externa o interna, que posee la capacidad de causar intencionadamente un efecto adverso en activos de información o de TIC, a través del Ciberespacio, comprometiendo su confidencialidad, integridad o disponibilidad.

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.

Ciberdefensiva (Acción Defensiva en el Ciberespacio): 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.

Cibercrisis: Situación en la que las capacidades de Ciberseguridad de una organización se ven rebasadas o han fracasado por un Ciberincidente 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 que atentan contra instalaciones estratégicas de un país, incluidas las Infraestructuras Críticas de Información.

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

Ciberespacio: Entorno o ámbito intangible de naturaleza virtual, soportado por las Tecnologías de la Información y Comunicaciones (TIC), 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: Actividades realizadas en el Ciberespacio, para recabar información sensible de los campos del poder nacional.

Ciberfuerza: Es la Fuerza de Seguridad en el Ciberespacio de las Fuerzas Armadas, para realizar Ciberoperaciones en el cumplimiento de las misiones en materia de Seguridad Nacional.

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

Ciberidentidad: Personas 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.

Ciberincidente (Incidente de Ciberseguridad): 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.

Ciberinteligencia: Disciplina de la inteligencia que utiliza el Ciberespacio como medio para adquirir, analizar y utilizar información valiosa relacionada con amenazas que pueden afectar a organizaciones o tener un impacto en la Seguridad Nacional. Este proceso involucra la recopilación y análisis de datos y la identificación de amenazas, con el propósito de apoyar al Estado-Nación, incluyendo las Fuerzas Armadas, en todos los ámbitos operacionales (tierra, mar, aire, espacio y Ciberespacio).

Ciberofensiva (Acción Ofensiva en el Ciberespacio): 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.

Ciberoperaciones (Operaciones en el Ciberespacio): Actividades planificadas, organizadas y coordinadas 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.

Ciberpersona (Avatar): Representación o identidad virtual de una persona, grupo o entidad para navegar e interactuar en el Ciberespacio.

Ciberresiliencia: Capacidad de un sistema, organización o Estado-Nación, para resistir o recuperarse en el menor tiempo posible de un Ciberincidente o Ciberataque para la continuidad de las 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 una organización para proteger sus activos críticos en el Ciberespacio empleando personal especialista, controles tecnológicos, procedimientos, normatividad, estándares tecnológicos, políticas públicas y legislación, reduciendo los riesgos a sus Infraestructuras de Información Esenciales.

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 la persona adversaria.

Ciberusurpador: Personas 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.

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 Ciberoperaciones.

F

Fuerza Laboral del Ciberespacio: Son el personal profesional y técnico 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.

I

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 la ley de 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 negativo en la persona u organismos públicos o privados.

Inteligencia de Ciberamenazas: Proceso que emplea el ciclo de la inteligencia para analizar 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; así como técnicas, tácticas y procedimientos para poder contrarrestarlos.

Instalaciones Estratégicas: Espacios inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional.

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.C.D.N. (Cnto. Ops. Ciberespacio E.M.C.D.N.) y de la Coordinadora General del Ciberespacio del E.M.G.A. (EMCOGCIBER E.M.G.A.), definidos como:

Centro de Operaciones del Ciberespacio del E.M.C.D.N. (Cnto. Ops. Ciberespacio E.M.C.D.N.).

Es el Organismo del Estado Mayor Conjunto 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".

Cibercomando de la Armada de México (CIBERCOM-AM).

Esta Unidad tiene como misión: "Proteger y asegurar la infraestructura de las tecnologías de información y comunicación Institucional en todos los entornos operacionales de la Armada de México; así como, coadyuvar en el esfuerzo de Ciberdefensa nacional.

Coordinadora General del Ciberespacio del E.M.G.A. (EMCOGCIBER E.M.G.A.).

Área responsable de determinar y conducir la gobernanza del Ciberespacio para la seguridad de la infraestructura esencial de información de la Secretaría de Marina – Armada de México y coadyuvar al esfuerzo nacional en el mantenimiento de la integridad, estabilidad y permanencia del Estado Mexicano.

Ciudad de México a 31 de julio del 2024.

Autorizó

Secretaría de la Defensa Nacional
Estado Mayor Conjunto
de la Defensa Nacional

Centro de Operaciones del Ciberespacio

Gral. Brigadier D.E.M.
Director Cnto. Ops. Ciberespacio E.M.C.D.N.
Roger David Rodríguez Arosemena.

Autorizó

Secretaría de Marina
Estado Mayor General de la Armada

Coordinadora General del Ciberespacio

Contralmirante C.G. D.E.M.
Coordinador EMCOGCIBER del E.M.G.A.
Genaro García Cetina.

Referencias:

- Ley General del Sistema Nacional de Seguridad Pública, disponible https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf,2023
- Ley de Seguridad Nacional. Gobierno de México, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf,2021
- 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.

- Glosario de términos unificados por personal de la SEDENA y de SEMAR, 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.

Centro de Operaciones del Ciberespacio del Estado Mayor Conjunto de la Defensa Nacional.

Coordinadora General del Ciberespacio del Estado Mayor General de la Armada.