CIBERESPACIO, CIBERSEGURIDAD Y CIBERDEFENSA

(Confrontación de vulnerabilidades vs. agresiones como base de desarrollo de un Sistema Integrado de Ciberdefensa)

Capitán de Navío Ingeniero Pablo D. Sorrentino

1. Introducción

Desde que en 1968 Yoneji Masuda, sociólogo japonés, conceptualizó la idea de sociedad de la información en la cual las tecnologías facilitan la creación, tratamiento, modificación y distribución de la información y juegan un papel esencial en las actividades sociales, culturales y económicas, han transcurrido casi cinco **décadas. El propio Masuda no pudo haber imaginado cuan acertada sería su conceptualización ni el altísimo impacto que las tecnologías tendrían en las sociedades modernas.**

De todas las tecnologías de alto impacto, entendiendo por ello aquellas que son capaces de modificar la cultura, el desarrollo y la proyección de una sociedad, las Tecnologías de Información y Comunicaciones (TIC) han sido —y son— el principal motor de la Sociedad de la Información, y marcan un antes y un después en la forma en que los diferentes actores —sean estos individuales o colectivos— se expresan, comunican, debaten, informan y se desarrollan a nivel global.

Dentro de las TIC, hubo un elemento que, a pesar de no ser el único distintivo, fue el mayor vector de propagación de las tecnologías a nivel global. Su entrada en escena se remonta a 1969 y fue conocido como ARPANET (Advanced Research Projects Agency Network). Era una red desarrollada a partir de requerimientos del Departamento de Defensa de los Estados Unidos (DOD) a efectos de comunicar diferentes ámbitos académicos y fue el embrión de la actual internet, conocida como tal a mediados de 1990.

Internet, que en sus inicios fue la tibia insinuación de un posible cambio en el modo de intercambiar información y de comunicarnos, hoy ha transformado y redefinido la comunicación en general, ya sea esta telefónica, radial, televisiva o postal. Los diarios y las revistas han sido transformados por internet; nuestro modo privado de interrelacionarnos ha sido revolucionado mediante el *e-mail*, la telefonía IP, las redes sociales y toda una pléyade de aplicaciones que interactúan diariamente en y con nuestras relaciones personales.

La industria y el comercio globales se han visto afectados por este fenómeno, el surgimiento del comercio electrónico ha hecho crecer exponencialmente tanto a grandes cadenas como a pequeñas y medianas empresas, y los servicios financieros en línea han afectado las cadenas logísticas de industrias completas.

Cuando en 1999 Kevin Ashton comenzaba a desarrollar el concepto de Internet de las Cosas (IoT), estaba dando cuenta del vertiginoso desarrollo tecnológico en que nos encontrábamos inmersos. A pesar de que el gran público no lo hubiera notado de inmediato, se estaba gestando un nuevo paradigma que cambiaría radicalmente el modo de ver el mundo.

Tal ha sido la evolución que, en un artículo de 2009 para el diario *RFID*, «Esa cosa de la 'Internet de las cosas'», Ashton hizo la siguiente declaración:

«Los ordenadores actuales —y, por tanto, internet— son prácticamente dependientes de los seres humanos para recabar información. Una mayoría de los casi 50 *petabytes* (un *petabyte* son 1024 terabytes) de datos disponibles en internet fueron inicialmente creados por humanos, a base de teclear, presionar un botón, tomar una imagen digital o escanear un código de barras. Los diagramas convencionales de internet dejan fuera a los *enrouters* **más importantes de todos: las personas. El problema es que las personas tienen un tiempo, una atención y una precisión limitados, y no se les da muy bien conseguir información sobre cosas en el mundo real. Y eso es un gran obstáculo. Somos cuerpos físicos, al igual que el medio que nos rodea. No podemos comer** *bits*, ni quemarlos para resguardarnos del frío, ni meterlos en

tanques de gas. Las ideas y la información son importantes, pero las cosas cotidianas tienen mucho más valor. Aunque la tecnología de la información actual es tan dependiente de los datos escritos por personas que nuestros ordenadores saben más sobre ideas que sobre cosas. Si tuviéramos ordenadores que supieran todo lo que tuvieran que saber sobre las 'cosas', mediante el uso de datos que ellos mismos pudieran recoger sin nuestra ayuda, nosotros podríamos monitorizar, contar y localizar todo a nuestro alrededor; de esta manera, se reducirían increíblemente gastos, pérdidas y costes. Sabríamos cuándo reemplazar, reparar o recuperar lo que fuera, así como conocer si su funcionamiento estuviera siendo correcto. La internet de las cosas tiene el potencial para cambiar el mundo tal y como hizo la revolución digital hace unas décadas. Tal vez, incluso, hasta más».

Pero Ashton no tuvo en cuenta que el progreso que suponía el afianzamiento del concepto IoT (Internet of Things [internet de las cosas]), donde millones de dispositivos están interconectados: desde controladores lógicos en centrales nucleares hasta heladeras hogareñas, implicaría un aumento monumental de las vulnerabilidades cibernéticas. Toda tecnología implica riesgos, y la tecnología digital no es la excepción.

2. Antecedentes

Durante el transcurso de la historia humana, los cambios tecnológicos implicaron nuevos desafíos y crearon, asimismo, nuevas amenazas para el tejido social de cada época. Sin embargo, esos cambios, lentos al comienzo, fueron acelerándose con el devenir de los siglos hasta alcanzar su máxima expresión en el siglo xxi.

De tal modo, podemos identificar diferentes ámbitos operacionales para la actividad humana (Fig.1) comenzando con el terrestre, 5000 años atrás, con la invención de la rueda. Cuando el hombre se aventuró al mar hace 2500 años, surgió el marítimo. Luego, debieron pasar milenios para que el sueño de volar se convirtiese en realidad hace 110 años. Y hace apenas 53 años, el espacio dejó de ser una frontera para la humanidad.

Figura1

El desarrollo tecnológico siguió acelerándose y, en tan solo 21 años desde el afianzamiento de internet, en 1992, surgió otro ámbito operacional, totalmente nuevo, que interactúa e influye decisivamente en los ámbitos preexistentes. Ese nuevo ámbito lo conocemos como ciberespacio (Fig. 2).

Figura 2

3. Conceptos preliminares

Se han escrito innumerables definiciones del ciberespacio, pero ¿qué es? ¿Qué lo compone? ¿Cómo y con quién interactúa?

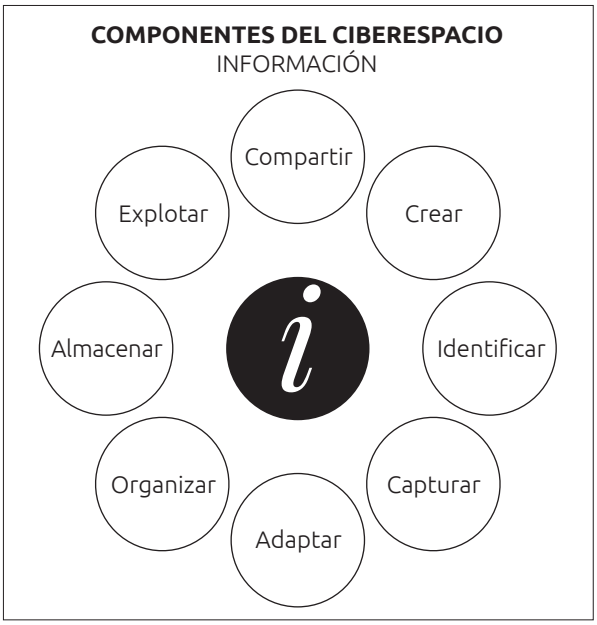
En primer lugar, podemos distinguir tres componentes primarios del ciberespacio:

- El primer componente es la infraestructura tecnológica (Fig. 3) que soporta y sostiene el concepto de la entidad ciberespacial. Está basada de modo excluyente en las tecnologías de información y comunicaciones (TIC), y los órganos que dan vida al sistema son los sistemas de transmisión de información, las redes de comunicaciones, sean estas digitales, analógicas, satelitales, radioenlaces u ópticas, el sistema nervioso del ciberespacio y los sitios de procesamiento y almacenamiento de información, como los *data center*, *cloud computing*, estaciones de trabajo, *smartphones* o cualquier dispositivo que esté en capacidad de procesar o de almacenar información digital.

Figura 3

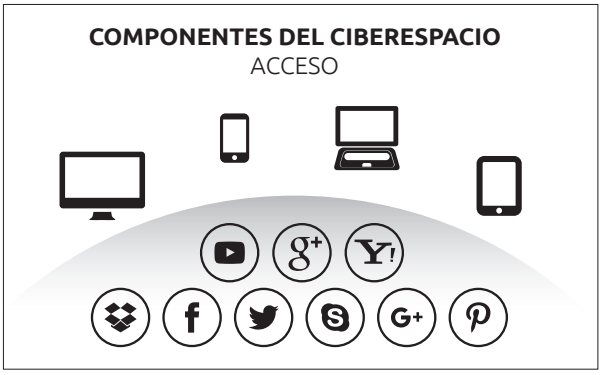
- El segundo componente es la información (Fig. 4) que se crea, identifica, captura, adapta, organiza, almacena, explota y se comparte en la infraestructura tecnológica, y que ha dado origen a la denominada sociedad de la información, donde la información juega un papel primordial en las actividades sociales, culturales y económicas.

Figura 4



- El tercer componente son los métodos de acceso (Fig. 5) al ciberespacio, caracterizados principalmente por los motores de búsqueda, las redes sociales y las herramientas de explotación de información, ya sean propietarias o libres.

Figura 5

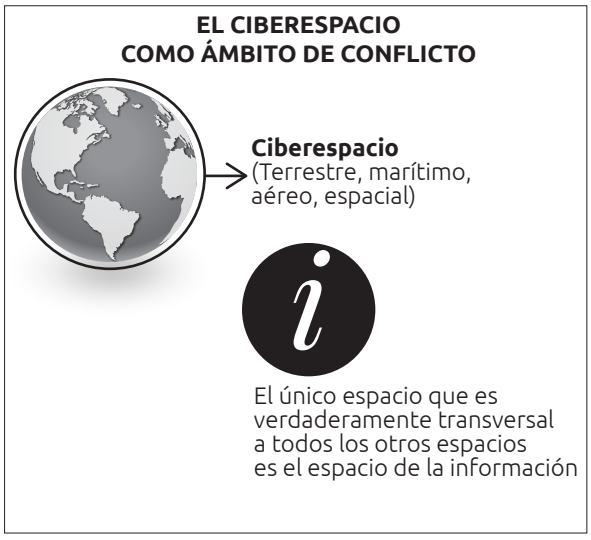


4. Conceptos

El ciberespacio es definido como «ámbito operacional virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y explotación de información digital, a través de redes interdependientes e interconectadas —vinculadas a internet o no— y el *software* y *firmware* de dispositivos asociados a ellas, siendo su carácter distintivo el empleo excluyente de las TIC (Tecnologías de Información y Comunicaciones) y la interacción permanente con los otros ámbitos operacionales».

El ciberespacio plantea un escenario de conflicto no convencional (Fig. 6), caracterizado por una libertad de maniobra absoluta en el uso de recursos globales, una ubicuidad sin barreras de tiempo y espacio, y modos de acción silenciosos e invisibles, donde es muy dificultoso identificar con certeza a un atacante. Este hecho lleva indefectiblemente a un cambio de paradigma, donde debe primar la adaptación permanente a los cambios tecnológicos para enfrentar nuevas metodologías de ataque con estrategias y medios no habituales.

Figura 6



A efectos de enfrentar el cúmulo de amenazas que surgen de la difusión, uso y aplicación de las nuevas TIC, se deben generar estrategias de ciberdefensa que tiendan a preservar y asegurar las características de confidencialidad, integridad, disponibilidad, autenticidad, protección de duplicación y no repudio de la información para permitir la continuidad de las operaciones de los sistemas de infraestructura crítica.

5. Problemática del manejo del ciberespacio

El ciberespacio ha tenido un vertiginoso desarrollo (Fig. 7). La velocidad de su evolución es la que define su complejidad, y su utilización requiere una constante capacidad de adaptación a los cambios que **él** impone, sean estos cambios tecnológicos, sociales o culturales (Fig.8); considerando que los componentes que conforman el ciberespacio e interactúan en él y con él son de carácter heterogéneo (Fig.9), se presenta una problemática respecto de su manejo, que se caracteriza por lo complejo de su control o, en muchos casos, por la ausencia total de él.

Figura 7

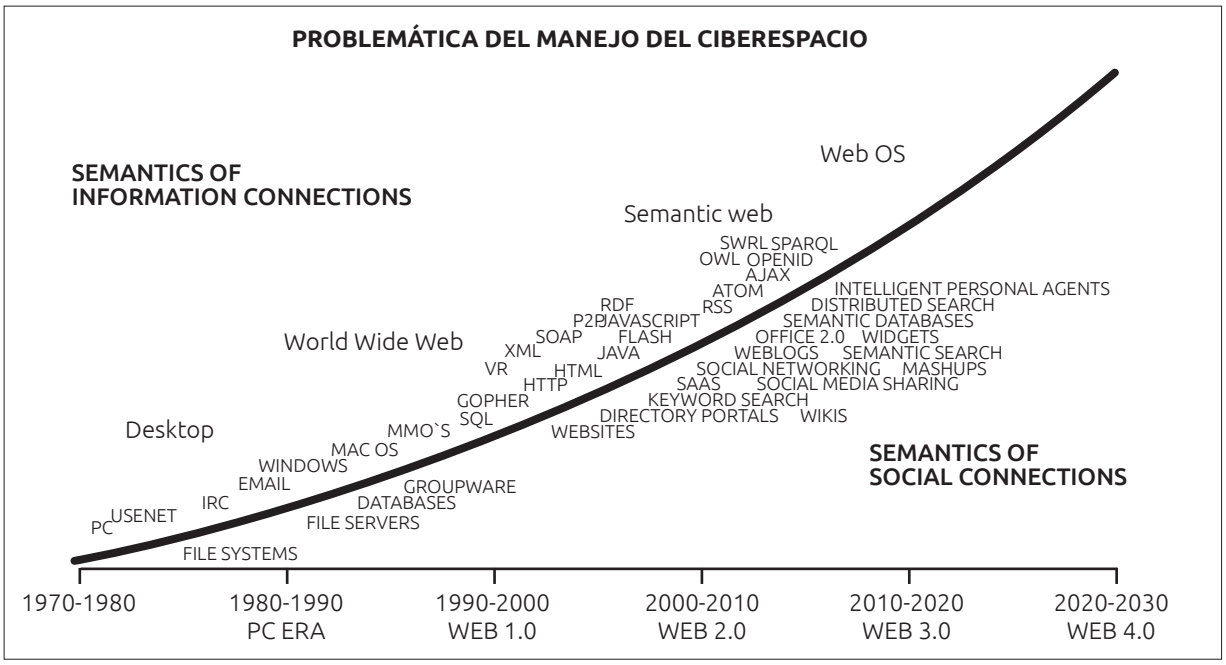


Figura 8

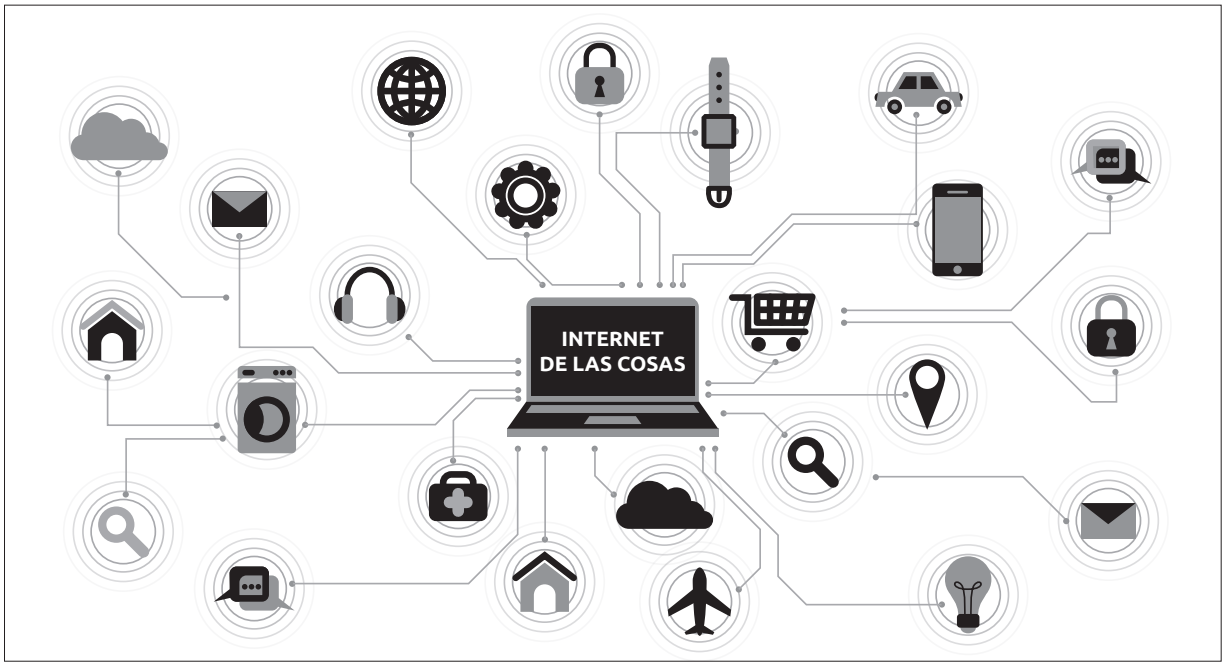


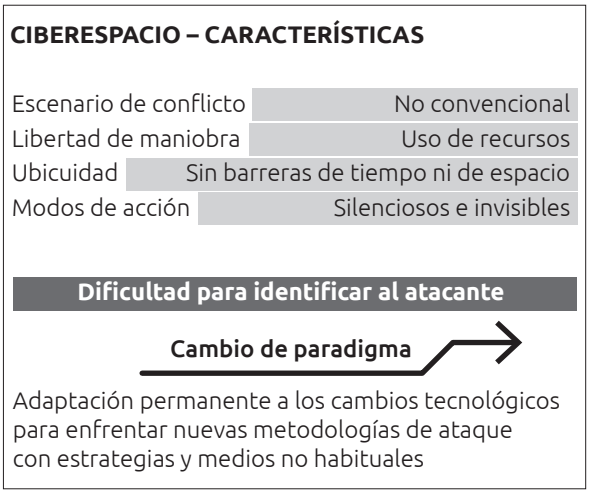
Figura 9

Esa misma heterogeneidad de elementos constitutivos —sistemas de comunicaciones, redes informáticas, bases de datos, utilitarios y sistemas aplicativos, facilidades de navegación en la web, usuarios, redes sociales, etc.— hace que las funciones de control y supervisión del buen uso de los recursos estén dispersas entre los distintos componentes y actores.

El ciberespacio es un escenario de conflicto no convencional (Fig. 10), donde los agresores tienen una amplia libertad de maniobra para el uso de los recursos del mismo

ciberespacio. Es un ambiente sin barreras de tiempo ni de espacio que limiten el accionar, lo cual permite modos de acción silenciosos e invisibles, lo que dificulta la identificación del atacante o la atribución del ataque complicando una respuesta proporcional a él.

Figura 10



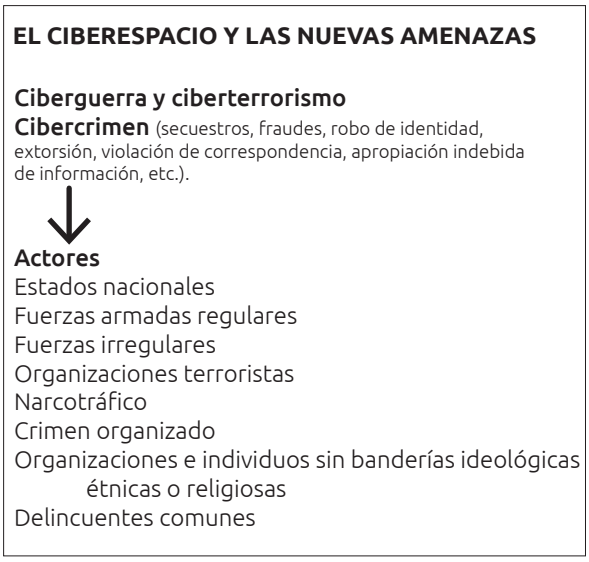
6. El ciberespacio y las nuevas amenazas

La misma heterogeneidad citada precedentemente, que sin duda es el principal motor del crecimiento, desarrollo y globalización del ciberespacio, también es la incubadora de nuevas amenazas, tales como el cibercrimen, el ciberterrorismo, la ciberguerra y el medio facilitador de viejas prácticas delictivas con nuevas herramientas tecnológicas (secuestros, fraudes, robo de identidad, extorsiones, violación de correspondencia, apropiación indebida de información, etc.).

Asimismo, los actores que generan y perpetran estas nuevas amenazas son disímiles y de dificultosa identificación y localización. Estos pueden ser desde Estados nacionales, fuerzas armadas regulares, fuerzas irregulares, organizaciones terroristas, narcotráfico, crimen organizado u organizaciones e individuos sin ninguna bandería ideológica, étnica o religiosa, hasta delincuentes comunes (Fig. 11).

El nuevo dominio ciberespacial, sus particulares característicos de conformación y las amenazas emergentes de él posibilitan la concreción del concepto de asimetría. Los ciberataques son un ejemplo claro de las amenazas a la seguridad actuales, no simétricas, donde, con recursos relativamente limitados, se podrían paralizar infraestructuras críticas, lo que afectaría a sociedades completas, usando solamente una computadora. En manos terroristas, estos ataques podrían ser mucho más peligrosos a futuro.

Figura 11



Las amenazas dentro del ambiente ciberespacial son subestimadas, debido a que no se han registrado o reportado pérdidas de vidas humanas aún; sin embargo, solo es cuestión de tiempo para que ello ocurra. Esto se debe a que una buena parte de las funcionalidades de la sociedad depende del correcto funcionamiento de los sistemas de infraestructura crítica (plantas potabilizadoras de agua, distribución eléctrica, ferrocarriles, señalización urbana, aeropuertos, centrales nucleares, etc.).

Asimismo, cabe destacar la relación directamente proporcional entre el nivel de penetración de internet en un país o región y el aumento de las vulnerabilidades en esa misma zona geográfica. Cuanto mayor es la cantidad de usuarios conectados a internet, mayor es la cantidad de blancos susceptibles de ser atacados o utilizados como plataformas de lanzamiento de ataques a terceros.

7. Ciberseguridad y ciberdefensa

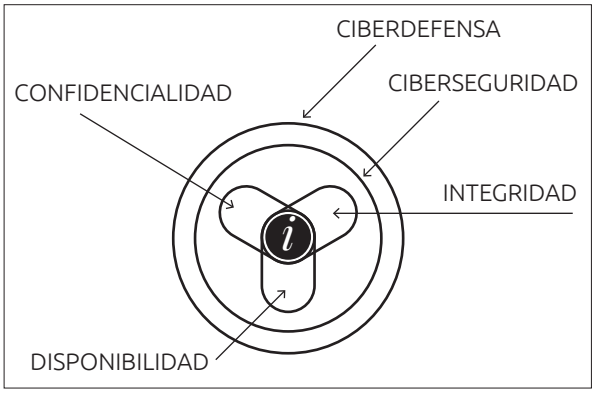
El uso masivo de las TIC, la interdependencia de la sociedad respecto de ellas, la ausencia de controles definidos a nivel global, el vacío de normas legales que regulen la utilización del ciberespacio y las amenazas surgidas de él exponen a las sociedades a ciberataques tanto a nivel colectivo como individual y acrecientan diariamente sus vulnerabilidades.

La ciberdefensa representa una nueva dimensión de conflicto que origina la necesidad de establecer nuevos modos de acción, estrategias y acuerdos a nivel internacional. Los Estados nacionales no pueden estar ajenos a esta realidad y deben tomar medidas en salvaguarda de los bienes, recursos y normal funcionamiento de la sociedad.

La implementación de una estrategia de ciberdefensa a niveles nacionales se presenta como la más adecuada manera de mitigar el impacto de las nuevas amenazas.

Si definimos la ciberseguridad como una herramienta cuyo objetivo es salvaguardar los atributos básicos de seguridad de los activos de información (confidencialidad, integridad y disponibilidad), podemos definir la ciberdefensa como el ámbito propicio para que la ciberseguridad alcance su grado máximo de desarrollo y maduración. Por lo tanto:

> «La ciberdefensa debe estar dirigida a combatir o contrarrestar una amenaza, sea esta inmediata, latente o potencial, originada en adversarios, enemigos, organizaciones criminales o individuos aislados, que pretenda atentar contra los principios de confidencialidad, integridad y disponibilidad de la información, debiéndose considerarse una función defensivo-ofensiva».



La ciberdefensa exige un adecuado proceso de gestión de riesgos en el cual se identifiquen las amenazas que pudiesen explotar vulnerabilidades exponiendo las infraestructuras críticas de valor estratégico

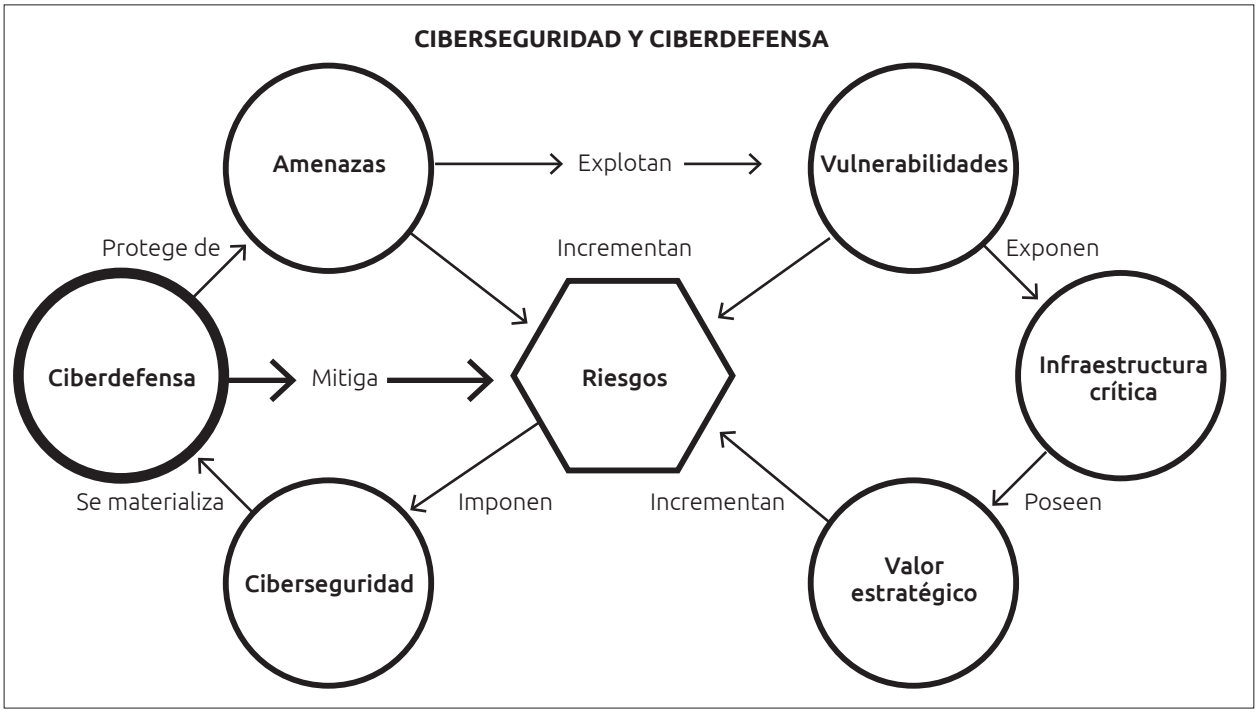
8. Agresiones en el ciberespacio (ciberagresiones)

Las particulares características del ciberespacio dificultan la identificación unívoca de las agresiones y del agresor. Para facilitar el delineamiento de una estrategia de ciberdefensa, es necesario generalizar el carácter de las agresiones definiéndolas como ciberagresiones genéricas (CG), siendo estas las que suceden dentro del ámbito ciberespacial sin distinción de origen, motivación o efecto.

Un modo de agrupar las CG para desarrollar una metodología defensiva es asociarlas al modelo de siete (7) capas OSI, para poder definir estrategias particulares en cada una de ellas ante las agresiones que explotan las vulnerabilidades subyacentes en cada nivel.

Asimismo, podemos consolidar el conjunto de ciberagresiones en un grupo de acciones que las materializan:

A1 (Infiltración): Acción caracterizada para la penetración de las defensas de un sistema controlado y protegido por *software* o *hardware*, de forma tal que puedan ser detectadas las vulnerabilidades del sistema sujeto de la agresión.



Nro.	Capa	Debilidad/Vulnerabilidad	Agresión	Mitigación
1	FÍSICA	Falta de respaldo de generación eléctrica.	Natural Técnica Social Espionaje Sabotaje Terrorismo	PIC (Protección Física de Infraestructura). CERT. Auditoría.
		Débil control de acceso y permanencia.		
		Falta de controles de cambios en el entorno.		
		Falta de redundancia de enlaces.		
		Falta de capacidad de resiliencia.		
2	DATA LINK	Deficiente control de direcciones de *hardware*.	A1, A2 *(ARP Spoof, MAC Flooding, Spanning Tree attack)*	PIC (VLAN. *Static ARP.* *STP Root priority*) CERT. Auditoría.
		Deficiencia en configuraciones Bridge o Switch.		
		Deficiente análisis de tráfico y colisiones de red.		
		Deficiente control de puntos de acceso wifi.		
		Falta de detectores de *sniffers*.		
3	NETWORK	Falla en el control de contraseñas de *router*.	A1, A2 (Accesos no autorizados. *SYN Flood.* *Ping of Death*)	PIC (*Firewalls.* Listas de control de acceso. VPN. Detección de intrusos. Filtrado de contenidos.) CERT. Auditoría
		Falta de control en configuración *router weak router configuration control*.		
		Falta de auditoría ARP.		
		Tablas de ruteo dinámicas.		
4	TRANSPORTE	Falta de control de sesiones.	A1, A2 (Accesos no autorizados. *SYN Flood.* Suplantación de identidad en *End Point.*)	
		Falta de control de paquetes UDP.		
		Falta de monitoreo de puertos UDP y TCP.		
		Deficiente configuración de *Proxy/Firewall*.		
5	SESIÓN	Mecanismos de autenticación débiles o inexistentes.	A2, A3 (Escalamiento de Privilegios. Do. RCP & Net *Bios Attack.* Robo de información.)	PIC (Encriptación. Parches de seguridad. Autenticación fuerte. Detección de intrusos. Antivirus. Antimalware. *Hardening.*) Auditoría. CERT.
		Intercambio de credenciales de sesión en claro.		
		Identificación de sesión débil.		
		Falta de control de autenticaciones fallidas.		
		Sesiones fallidas ilimitadas.		
6	PRESENTACIÓN	Dispositivos externos no controlados.	A2 (Gusanos, virus, troyanos, accesos no autorizados, robo de información.)	
		Mal manejo de accesos no autorizados.		
		Débil protección criptográfica (*software*).		
		Falla o debilidad en los métodos de autenticación.		
7	APLICACIÓN	Privilegios de acceso excesivo.	A3 (Escalamiento de privilegios. DoS. *Backdoors.* Gusanos. Virus. Troyanos. Accesos no autorizados. Robo de información.)	
		Control inadecuado de servicios y de recursos.		
		Falencias de seguridad en el diseño de las aplicaciones.		
		Falencias de seguridad en las capas anteriores.		
		Fallas de procedimientos de autenticación.		
		Fallas de lógica en la programación, accidental o no.		
		Falta de actualización de parches de seguridad.		
		Falta de actualización de antivirus.		
		Falta de actualización de antimalware.		
		Ausencia de IDS / IPS.		

A2 (Maniobra): Acción que se desarrolla después de A1 para la adquisición de datos dentro del sistema dejando el sistema intacto; su resultado es la sustracción, transferencia o alteración indetectable de datos que puedan afectar las capacidades de defensa del actor sujeto de la agresión de modo de permitir la efectiva explotación de las vulnerabilidades detectadas en A1.
A3 (Ataque): Acción ofensiva que se desarrolla después de A1 y A2 para lograr la efectiva destrucción o el cambio de parámetros de funcionamiento de los sistemas sometidos a la agresión, de modo de lograr la concreción del objetivo del ataque, ya sea este una denegación de servicios o el malfuncionamiento del sistema.

8.1. Ataque cibernético

La expresión más acabada de una ciberagresión es el ataque cibernético, es decir, las medidas adoptadas a través del uso de las redes informáticas para interrumpir, negar, degradar o destruir información albergada en estaciones de trabajo y redes informáticas del adversario, o las estaciones de trabajo y las redes mismas.

El ataque cibernético no es un hecho puntual y temporalmente acotado; es producto de un proceso y un planeamiento asociado a él. Dentro del proceso de ataque cibernético, se pueden identificar tres (3) fases y dos (2) momentos por cada una de las fases.

Fase 1: Infiltración

Momento 1: Reconocimiento

El reconocimiento está basado principalmente en la obtención de información del ciberambiente del objetivo a través de la explotación de fuentes abiertas (OSINT [*Open Source Intelligence*]), tales como información pública (*websites*, *web servers*, redes sociales), o de Ingeniería Social (*phishing*, suplantación de identidad, inducción, extorsión, revisión de documentos descartados, etc.).

Momento 2: Exploración

La exploración consiste en el relevamiento de la infraestructura, escaneo de puertos e interrogación de servicios y firmas de sistemas operativos a efectos de evaluar las vulnerabilidades primarias del objetivo.

Fase 2: Maniobra

Momento 1: Acceso

Una vez finalizada la primera fase y obtenidas las credenciales suficientes, se produce el acceso al sistema objetivo y el correspondiente escalamiento de privilegios que permitan realizar movimientos laterales en la infraestructura.

Momento 2: Exfiltración

Durante la exfiltración, se recaba en profundidad y se extrae información del objetivo buscando acceder a los datos y las configuraciones de dispositivos y de sistemas vulnerables ya detectados que permitan ejecutar con éxito la fase siguiente.

Fase 3: Ataque

Momento 1: Asalto

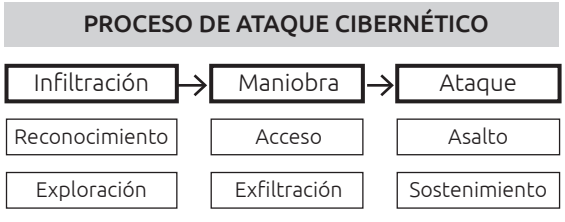
El asalto busca lograr un efecto sobre el objetivo, tal como la denegación de servicios (privar al adversario del uso de su propia infraestructura), la degradación de la infraestructura (sin negar el servicio, lograr su mal funcionamiento de modo velado con el objeto de causar perjuicios a mediano plazo), el engaño (posibilitar el desvío de tráfico e información sin ser detectado por medio de artilugios) o la destrucción de la infraestructura del objetivo o su puesta fuera de servicio por períodos prolongados.

Momento 2: Sostenimiento de la acción

El sostenimiento de la acción se basa en el necesario equilibrio entre la persistencia de un ataque y su encubrimiento por un determinado período de tiempo.

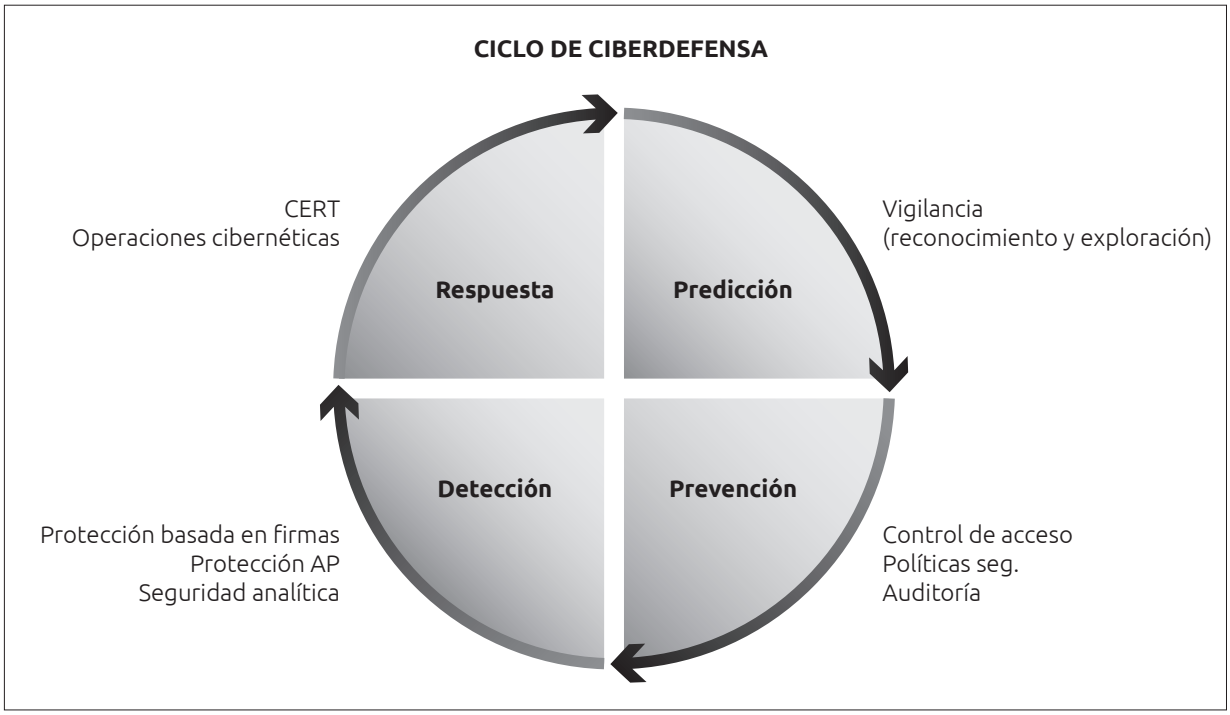
ATAQUE CIBERNÉTICO

Medidas adoptadas a través del uso de las redes informáticas para interrumpir, negar, degradar o destruir información albergada en estaciones de trabajo y redes informáticas del adversario, o a las estaciones de trabajo y las redes mismas.



9. Desarrollo de un sistema integrado de ciberdefensa

En base a las CG (Ciberagresiones Genéricas) que explotan las vulnerabilidades de cada capa del modelo OSI, se proponen herramientas de mitigación para cada una



de ellas. De ello, surge un Sistema Integrado de Ciberdefensa (SIC) que debe responder a un ciclo específico y continuo de ciberdefensa. Dicho ciclo comprende las siguientes etapas:

Predicción: Debe materializarse por medio de la vigilancia, el reconocimiento y la exploración tanto del ciberespacio de interés propio como del de aquellos actores en capacidad de perpetrar agresiones cibernéticas.

Prevención: Básicamente consiste en la implementación de todas aquellas medidas que limiten, impidan o neutralicen el acceso, la permanencia o la dispersión de amenazas dentro del ciberespacio propio y de su infraestructura involucrada.

Detección: Comprende los sistemas automatizados de detección y de contención de amenazas, sean estas basadas en firmas (*Malware* en general = virus, gusanos, troyanos, *ramsonware*, etc.), amenazas persistentes avanzadas, vulnerabilidades del día cero o ataques de diseño.

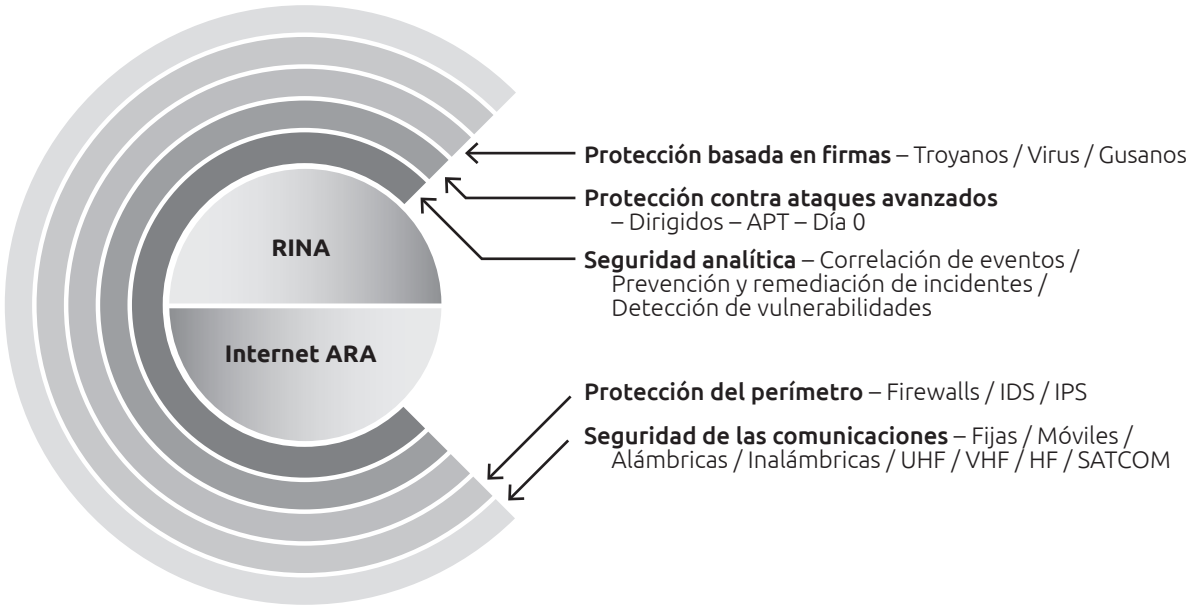
Respuesta: Mediante acciones pasivas y activas expos llevadas a cabo por los sistemas y los equipos de respuesta a incidentes cibernéticos (CERT) o las medidas y las acciones proactivas ejecutadas mediante las operaciones cibernéticas.

Asimismo, la implementación de un sistema de ciberdefensa requiere la puesta en marcha del concepto de defensa en profundidad, donde sucesivos anillos específicos de defensa permiten el funcionamiento de un sistema integrado de modo fluido y efectivo: Asegurando la efectiva protección de los atributos de confidencialidad, integridad y disponibilidad de la información en la infraestructura crítica (centros de procesamiento de datos, redes de transmisión de información y sistemas de información asociados) a fin de garantizar su continuidad operativa, logrando el máximo nivel de seguridad posible en todos los elementos componentes, minimizando las debilidades y desarrollando, mediante el adecuado análisis de riesgo, los procesos de recuperación que garanticen su capacidad de supervivencia llevados adelante mediante un proceso permanente de mejora continua, teniendo en cuenta el estado del arte y la evolución de las amenazas. Generando un sistema dinámico de respuestas ante alertas y emergencias con la apropiada aptitud de reacción ante incidentes y de adopción de las medidas preventivas y reactivas necesarias, sobre la base del análisis de los riesgos del entorno, para finalmente coordinar, en forma centralizada, la seguridad de la información (redes y sistemas informáticos).

10. Requisitos para la implementación de un sistema integrado de ciberdefensa

- Debe basarse en la normativa vigente: Política de Seguridad de la Información para la Administración Pública Nacional, Código Penal, Ley de Protección de Datos Personales, etc.

CENTRO DE CIBERDEFENSA / DEFENSA EN PROFUNDIDAD



- Actualizarse en base a las mejores prácticas y estándares internacionales.
- Desarrollarse dentro de una estructura orgánica que garantice una adecuada segregación de funciones que permitan el control por oposición y la necesaria libertad de maniobra.
- Ser interoperable de modo que permita compartir información proveniente de otros sistemas a nivel nacional o regional.
- Escalabilidad que asegure la incorporación constante de nuevas tecnologías.
- Modularidad para proyectar el diseño y el desarrollo del sistema en forma armónica y priorizada por etapas, contemplando la incorporación de los medios necesarios.
- Flexibilidad referida a los procesos, configuración del sistema y explotación de información, de modo de permitir la fusión en tiempo real del ciberambiente con los otros ambientes operacionales.
- Capacidad de cooperación, integración y coordinación con diferentes sistemas de ciberdefensa a nivel nacional.
- Redundancia en materia de integración de sistemas, especialmente en la vigilancia asociada a la inspección, detección e identificación de amenazas cibernéticas.
- Disponibilidad permanente del sistema, asegurando el conocimiento en tiempo real de la situación en el ciberespacio requerida por cada usuario.
- Independencia tecnológica y logística para asegurar la autonomía sin restricciones en el desarrollo de las tecnologías involucradas y el soporte a los medios que conformen las capacidades del sistema, así como también el pleno acceso al *software* y *hardware* involucrados en el sistema.
- Máxima automatización de los sistemas y sus subsistemas asociados para operar en forma continua y con mínima atención de personal a fin de asegurar la eficacia del sistema de ciberdefensa.

La marcha de la tecnología y el progreso garantizan que, incluso mientras debatimos esta problemática, nuestro uso del ciberespacio ha alcanzado ya el punto donde una gama cada vez más amplia de actores sociales, políticos, económicos y militares son dependientes de él y, por tanto, vulnerables a la interrupción de su uso y la usurpación de sus capacidades. ■