CIBERSEGURIDAD Y DERECHO

Dr. Julio Téllez Valdés
Doctor en Derecho Informático
Presidente de la FIADI

1) Definición de Ciberseguridad

La Unión Internacional de Telecomunicaciones (UIT) emitió recientemente la Resolución 181, mediante la cual, se aprobó una definición de ***ciberseguridad*** tal como se expresa en la Recomendación UIT–T X.1205 y según la cual: "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, las 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 de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

2) Unión Europea

Para la Unión Europea, en su Estrategia en materia de Ciberseguridad (Un Ciberespacio abierto, protegido y seguro) de principios de éste año, se señala que de manera reciente se ha comprobado que el mundo digital aporta grandes beneficios, pero que también es vulnerable. Los incidentes de ciberseguridad, tanto deliberados como accidentales, están incrementándose a un ritmo alarmante y podrían llegar a perturbar el suministro de servicios esenciales que damos por descontados como el agua, la asistencia sanitaria, la electricidad o los servicios móviles. Las amenazas pueden tener varios orígenes, entre ellos los ataques delictivos, por motivos políticos, terroristas o patrocinados por los Estados, así como catástrofes naturales o errores no intencionados. La economía de la UE se ve ya afectada por actividades de ciberdelincuencia

contra el sector privado y las personas. Los ciberdelincuentes recurren a métodos cada vez más complejos para introducirse en los sistemas de información, sustraer datos críticos o exigir rescates a las empresas. El aumento del espionaje económico y de las actividades alentadas por los Estados en el ciberespacio representa una nueva categoría de amenaza para las administraciones públicas y empresas de la UE. Asimismo, las autoridades de terceros países pueden emplear abusivamente el ciberespacio para ejercer vigilancia y control sobre sus propios ciudadanos. La UE considera que se debe contrarrestar esta situación fomentando la libertad en línea y velando por el respeto de los derechos fundamentales en la red.

Todos estos factores explican que los Gobiernos de todo el mundo hayan comenzado a desarrollar estrategias de ciberseguridad y a considerar el ciberespacio un asunto internacional cada vez más importante. Por ello la UE ha intensificado su intervención en este ámbito. La estrategia de ciberseguridad de la Unión Europea presentada por la Comisión y la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (Alta Representante), expone la visión de la UE en este campo, aclara funciones y responsabilidades y establece las medidas necesarias, basadas en una protección y una promoción amplias y efectivas de los derechos de los ciudadanos con el fin de que el entorno en línea de la UE llegue a ser el más seguro del mundo.

Para la UE, los valores esenciales lo son tanto en el mundo físico como en el digital y por tanto las leyes y normas aplicables en otros ámbitos de nuestras vidas cotidianas lo son también en el ciberespacio, por lo que algunos de los principios insoslayables son:

a) ***Protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad.-*** La ciberseguridad solo puede resultar positiva y eficaz si se basa en los derechos fundamentales y las libertades enunciados en la Carta de los Derechos Fundamentales de la Unión Europea y en los valores esenciales de la UE. Por su parte, los derechos individuales no pueden protegerse sin redes y sistemas seguros. Todo intercambio de información a efectos de ciberseguridad en que se manejen datos personales debe cumplir la normativa de protección de datos de la UE y tomar plenamente en consideración los derechos de las personas en este ámbito.

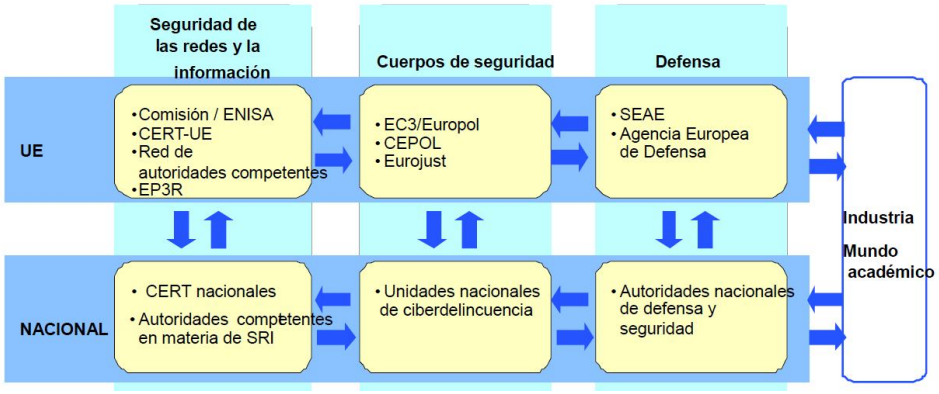
b) ***Acceso para todos***.- Un acceso limitado o nulo a Internet y el analfabetismo digital constituyen una desventaja para los ciudadanos, dada la omnipresencia del mundo digital en las actividades que se desarrollan en nuestra sociedad. Todos los ciudadanos deberían poder acceder a Internet y a un flujo de información libre de trabas. Deben garantizarse la integridad y la seguridad de Internet para así hacer posible un acceso seguro para todos.

c) ***Gobernanza multilateral democrática y eficaz***.- El mundo digital no está controlado por una sola entidad. Actualmente intervienen en él varias partes, muchas de las cuales son entidades comerciales y no gubernamentales que participan en la gestión diaria de los recursos, protocolos y normas de Internet y en su futuro desarrollo. La UE reafirma la importancia de todas las partes interesadas en el actual modelo de gobernanza de Internet y respalda este planteamiento de gobernanza multilateral.

d) ***Garantizar la seguridad: una responsabilidad compartida.-*** La creciente dependencia de las tecnologías de la información y de las comunicaciones en todas las esferas de la vida humana ha hecho surgir una serie de puntos vulnerables que es preciso delimitar debidamente, analizar exhaustivamente, subsanar o atenuar. Todas las partes interesadas, ya sean las administraciones públicas, el sector privado o los ciudadanos, han de reconocer esta responsabilidad compartida, tomar medidas para protegerse y, en caso necesario, ofrecer una respuesta coordinada para reforzar la ciberseguridad.

La visión estratégica de la UE sobre el tema, se articula en torno a cinco prioridades:

- Lograr la ciberresiliencia
- Reducir drásticamente la ciberdelincuencia
- Desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD)
- Desarrollar recursos industriales y tecnológicos de ciberseguridad
- Establecer una política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE.



Estrategia de Ciberseguridad de la Unión Europea

3) Organización de Estados Americanos (OEA)

Con la promulgación de la Estrategia Interamericana de Seguridad Cibernética, una iniciativa única a nivel regional, los Estados Miembros de la Organización de Estados Americanos (OEA), establecieron ciertos mandatos para poder desarrollar medidas eficaces para prevenir, tratar y responder a los ataques cibernéticos, luchar contra la delincuencia cibernética y proteger la infraestructura crítica asegurando las redes informáticas. Estos mandatos fueron asignados al Comité Interamericano contra el Terrorismo (CICTE), a la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) y a la Comisión Interamericana de Telecomunicaciones (CITEL), respectivamente. Desde la adopción de esta Estrategia, estas tres entidades han venido implementando diversas iniciativas y apoyando a los Estados Miembros a través de capacitación.

En el caso de la Secretaría del CICTE, siguiendo el mandato que los Estados Miembros de la OEA le encomendaron a través de la Asamblea General, el programa de Seguridad Cibernética ha venido promoviendo la creación de Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRTs, por sus siglas en inglés) gubernamentales en las Américas, y al mismo tiempo se ha estado conformando una Red Hemisférica de CSIRTs y Autoridades en Seguridad Cibernética.

Según la OEA, los principales desafíos a nivel nacional son : a) falta de conciencia sobre seguridad cibernética en los niveles políticos, b) ausencia de un marco nacional de seguridad cibernética y falta de efectiva coordinación interinstitucional, c) falta de apoyo para el personal

técnico de los países, y d) falta de continuidad en los proyectos relacionados con la seguridad cibernética. Y desde una perspectiva regional, los desafíos que han identificado son: a) inadecuadas líneas de comunicación entre las autoridades regionales, b) asimetría entre los niveles de capacidad de distintos Estados Miembros, y c) ausencia de estándares regionales en lo relativo a los CSIRTs gubernamentales.

4) Instrumentos Internacionales en materia de ciberseguridad y ciberdefensa

INSTRUMENTO	MATERIA
Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como el Convenio sobre Cibercriminalidad de Budapest). Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004.	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas. Único instrumento vinculante vigente sobre el tema en el ámbito internacional y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos. El Consejo considera que el delito cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional. Cabe resaltar que si bien el CCC tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo.
Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Estipula tres vías de acción: a) Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT. Este cometido fue asignado al Comité Interamericano Contra el Terrorismo - CICTE. b) Identificación y adopción de normas técnicas para una arquitectura segura de Internet. Esta labor

	es desarrollada por la Comisión Interamericana de Telecomunicaciones. c) Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones Unidas. (2009)	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información Esta resolución continúa el seguimiento de la Asamblea, con las resoluciones 53/70, de 4 de diciembre de 1998; 54/49, de 1° de diciembre de 1999; 55/28, de 20 de noviembre de 2000; 56/19, de 29 de noviembre de 2001, 57/53, de 22 de noviembre de 2002; 58/32, de 8 de diciembre de 2003; 59/61, de 3 de diciembre de 2004; 60/45, de 8 de diciembre de 2005; 61/54, de 6 de diciembre de 2006; 62/17, de 5 de diciembre de 2007; y 63/37, de 2 de diciembre de 2008.

5) Colombia

Por Decreto número 0032 del 14 de enero de 2013, el Presidente de Colombia creo la Comisión Nacional Digital y de Información Estatal cuyo objeto será la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano, emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno Nacional en materia de políticas para el sector de tecnologías de la información y las comunicaciones, de conformidad con la definición que de éstas hace la Ley. Es decir, una de las funciones principales de dicha Comisión, será la de asesorar al gobierno colombiano, en temas de ciberseguridad.

6) Estrategias y Acciones Internacionales

PAÍS	ACCIÓN TOMADA POR EL GOBIERNO
ALEMANIA	En febrero de 2011, el gobierno alemán lanzó su Estrategia de Seguridad Cibernética. En abril de 2011 el Ministerio del Interior puso en marcha el Centro Nacional de Ciberdefensa.
AUSTRALIA	Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio.
CANADÁ	El Departamento de Seguridad Pública implementó el Centro Canadiense de Repuesta a Incidentes Cibernéticos (CCIRC), y en octubre de 2010 adoptó la Estrategia Canadiense de Seguridad Cibernética.
ESTADOS UNIDOS	Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), DHS: *National Cyber Security Division*, US-CERT: *United States Computer Emergency Readiness Team* y la oficina de Seguridad Cibernética de la Casa Blanca. En mayo de 2011 fue adoptada la Estrategia Internacional para el Ciberespacio.
ESTONIA	En 2008 creó conjuntamente con otros países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciberamenazas. En este mismo año es adoptada una Estrategia de Seguridad Cibernética.
FRANCIA	Creó la Agencia de Seguridad para las Redes e Información (ANSSI), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. En febrero de 2011 fue adoptada una Estrategia de Defensa y Seguridad de los Sistemas de Información.

7) México

En el Diario Oficial de la Federación de fecha 6 de septiembre de 2011, en el que se publica el **Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal**, en el Artículo Segundo, fracción IX se define al *Ciberespacio* como "el conjunto de medios y procedimientos basados en las tecnologías de la información y comunicaciones, configurados para la prestación de servicios digitales", y por otro lado, la fracción X, define a la *Ciberseguridad*, como: "la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada".

Por su parte, el **Plan Nacional de Desarrollo 2013-2018**, en la Meta Nacional México en Paz, en el Objetivo 1.2. *Garantizar la Seguridad Nacional*, Estrategia 1.2.3. *Fortalecer la inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas a la Seguridad Nacional*, establece como una de las líneas de acción a seguir el "impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad".

Dicho documento también contempla el diseñar y operar un Sistema Nacional de Inteligencia Civil, que permita contar oportunamente con información para la producción eficiente y oportuna de inteligencia estratégica para la Seguridad Nacional; así como, en su caso, diseñar e implementar sistemas de interconexión de bases de datos nacionales para el acceso legítimo a información útil que eficiente el ejercicio de las atribuciones de las autoridades del País. De igual forma, fortalecer a la inteligencia civil como un órgano de fusión de las inteligencias especializadas del Estado Mexicano, tanto militar como naval y promover, con las instancias de la Administración Pública Federal y las Fuerzas Armadas, una doctrina de inteligencia que unifique los procedimientos de inteligencia de las instancias de Seguridad Nacional del Estado Mexicano, creando instancias de coordinación interinstitucional que generen estudios, investigaciones y proyectos que sustenten la Política General de Seguridad Nacional y ubique los

intereses estratégicos de México en el entorno global, así como integrar una nueva agenda de riesgos de seguridad nacional del País, que identifique las amenazas que pudieran atentar en contra de los objetivos e intereses nacionales estratégicos.

Actualmente en México se pretende privilegiar el uso de inteligencia policial, por encima del uso de la fuerza, a efecto de reducir la violencia y la impunidad, a partir de la premisa de que la obtención de información y su utilización sistematizada, constituyen un factor determinante para hacer más eficiente las acciones del Estado en el combate a la delincuencia. Se busca contar con el máximo de capacidades tecnológicas que se tengan al alcance, a fin de garantizar la interconexión e intercambio de información de inteligencia por medio de una base de datos extensa, actualizada y confiable.

El marco jurídico que rige la Seguridad Nacional en México es el siguiente:

a) **Constitución Política de los Estados Unidos Mexicanos**, en la fracción VI de su artículo 89, establece como responsabilidad del Jefe del Estado Mexicano, el C. Presidente de la República, preservar la Seguridad Nacional, en los términos de la ley expedida por el Congreso de la Unión en ejercicio de la facultad que le confiere a éste la propia Constitución en la fracción XXIX-M de su artículo 73.

b) **Ley de Seguridad Nacional**, publicada en el Diario Oficial de la Federación el 31 de enero de 2005. Establece que corresponde al Titular del Ejecutivo Federal la determinación de la política en la materia (artículo 2). Señala que en el Plan Nacional de Desarrollo y en el programa que de él derive se definirán temas de Seguridad Nacional (artículo 7). Dispone que el Consejo de Seguridad Nacional conocerá del Programa para la Seguridad Nacional (fracción III del artículo 13) y se desprende que lo hará a partir de la propuesta de contenido que haga la Secretaría Técnica del propio Consejo (fracción IV del artículo 15). Esta ley crea el **Consejo de Seguridad Nacional** como una instancia deliberativa cuya finalidad es establecer y articular la política en la materia (está pendiente de emitirse por parte del Presidente, la Agenda Nacional de Riesgos el cual es el documento que orienta las actividades de los integrantes del Consejo), así como una **Comisión Bicamaral sobre Seguridad Nacional** compuesta por tres Senadores y tres Diputados

Federales para ejercer control y evaluación sobre las políticas y acciones vinculadas con la Seguridad Nacional.

c) **Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional,** publicado el 29 de noviembre de 2006 en el Diario Oficial de la Federación, tiene por objeto establecer las políticas, normas, criterios, sistemas, procesos y procedimientos conforme a los cuales se promoverán las acciones de coordinación en materia de Seguridad Nacional. Establece que uno de los elementos que guiará la ejecución de la política al seno del Consejo de Seguridad Nacional es el Programa para la Seguridad Nacional.

d) **Reglamento Interior de la Secretaría de Gobernación** (vigente), publicado en el Diario Oficial de la Federación el 2 de abril de 2013, en su artículo 71 menciona que el **Centro de Investigación y Seguridad Nacional** (conocido como CISEN y creado el 13 de febrero de 1989), es un órgano administrativo desconcentrado con autonomía técnica, operativa y de gasto, adscrito directamente al Secretario, que tiene a su cargo las atribuciones que le confiere la ley de seguridad nacional. Es una de las autoridades que conforman actualmente el llamado Gabinete Especializado de México en Paz

e) **Tratados internacionales**, es importante señalar que el marco jurídico de la Seguridad Nacional en México también se encuentra en los tratados internacionales ratificados y que según la Constitución Política de los Estados Unidos Mexicanos (artículo 133) son Ley Suprema de la Unión (la Suprema Corte de Justicia confirmó que el orden jerárquico que tienen los tratados internacionales es superior al de las leyes federales y estatales, sólo debajo de la propia Constitución). En materia de seguridad, los Estados Unidos Mexicanos forman parte de distintos instrumentos jurídicos internacionales que dan sustento a la cooperación bilateral y multilateral para hacer frente a amenazas y riesgos trasnacionales; los cuales inciden directamente sobre la Seguridad Nacional de los Estados y atañen claramente a la paz y seguridad internacionales.

8) Glosario de términos y acrónimos en materia de Ciberseguridad

(Referidos en el documento *"Retos y Amenazas a la Seguridad Nacional en el Ciberespacio"* elaborado por el Ministerio de Defensa de España en 2010 y basado fundamentalmente en conceptos emitidos por la OTAN.

Amenaza (Threat) : La posibilidad de compromiso, pérdida o robo de información clasificada OTAN o de servicios y recursos que la soportan. Una amenaza puede ser definida por su origen, motivación o resultado y puede ser deliberada o accidental, violenta o subrepticia, externa o interna.

ANS: Autoridad Nacional de Ciberdefensa

Bot Botnet: Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación [distribuida] de servicio.

Brecha de seguridad (Security breach): Una acción u omisión, deliberada o accidental, contraria a la Política de Seguridad de la OTAN o normativas de aplicación de la Política que resulte en un compromiso real o potencial de información clasificada OTAN o los servicios y recursos que la soportan.

Caballo de Troya: Ver troyano

CACD: Centro Asesor para la ciberdefensa (CACD)

Carding: Uso ilegítimo de las tarjetas de crédito.

Catálogo Nacional de Infraestructuras Estratégicas: La información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.

CCC: Centro de Coordinación de Ciberdefensa.

CCN: Centro Criptológico Nacional

CCRIS: Centro de coordinación y respuesta a incidentes de Seguridad

CERT: Computer Emergency Response Team

Ciberataque: Forma de ciberguerra / ciberterrorismo donde combinado con un ataque físico o no se intenta impedir el empleo de los sistemas de información del adversario o el acceso la misma

Ciberdefensa: La aplicación de medidas de seguridad para proteger las los diferentes componentes de los sistemas de información y comunicaciones de un ciberataque.

Ciberespacio (Cyberspace): El mundo digital generado por computadoras y redes coexistentes con las personas y el cual incluye todos los aspectos de la actividad “online”.

Ciberevento (Cyber event): Cualquier suceso observable en un sistema de información y comunicaciones.

Ciberincidente (Cyber incident): Ciberevento adverso en un sistema de información y comunicaciones o la amenaza de que se produzca.

Ciberseguridad: Protección de los componentes de las infraestructuras de los sistemas de información y comunicaciones ante amenazas cibernéticas

Ciberterrorismo: Un ciberataque para causar la inutilización o interrupción de redes de computadoras o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico

Código dañino o malicioso (malicious code o software): Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.

EGC: *European Government CERT*

Exploit: Pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado).

FIRST: Forum for Incident Response and Security Teams

Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Gestión del riesgo (Risk Management): Según la OTAN es la aproximación sistemática, basada en la valoración de las amenazas y las vulnerabilidades, para la determinación de las contra-medidas necesarias para la protección de la información o los servicios y recursos que la soportan.

Información: Conocimiento que puede ser comunicado de cualquier forma.

Información clasificada (Classified information): Información o materia determinada que requiere protección contra revelación no autorizada y a la que, consecuentemente, se le ha asignado un grado de clasificación de seguridad.

Infraestructuras críticas (IC): Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales

Infraestructuras estratégicas (IE): Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios públicos esenciales

Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Interdependencia: Los efectos que una interrupción en el funcionamiento de la instalación o servicio produciría en otras instalacioneso servicios, distinguiéndose las repercusiones en el propio sector y/o en otros sectores, y las repercusiones de ámbito local, regional, nacional o internacional.

OTAN: *North Atlantic Treaty Organization (*Organización del Tratado del Atlántico Norte)

Phishing: Los ataques de «phishing» usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura “spam” para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de

convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc.

RAT: *Remote Administrations Tool.* Herramienta de administración remota. Estas apliaciones pueden ser legítimas o no y pueden ser utilizadas con o sin autorización del usuario. En el mundo del malware estas aplicaciones generalmente son troyanos que abren una puerta trasera (backdoor) en el equipo del usuario para permitir dicha administración.

RAT (2): *Troyano de Acceso Remoto.* Son programas de software malintencionados que permiten a los delincuentes controlar un equipo mediante la conexión a Internet. Un RAT puede permitir a un delincuente ver y cambiar los archivos y funciones del equipo, supervisar y registrar sus actividades y utilizar su equipo para atacar a otros.

Riesgo (Risk): La probabilidad de que una vulnerabilidad sea explotada con éxito por una amenaza produciendo un compromiso de confidencialidad, integridad y/o disponibilidad y daños.

Rootkit: Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos.

SCADA: Supervisory Control And Data Acquisition Control Supervisor y Adquisición de Datos, nombre de los sistemas de control industrial.

Sistema de Información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Spam: *Correo basura* Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de usuarios están expuestos a este correo basura, más del 80% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.

Spyware: Código dañino diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario.

STIC: Seguridad de las Tecnologías de Información y Comunicaciones.

TERENA: *Trans-European Research and Education Networking Association* Grupo de coordinación de CERT,s europeos

TF-CSIRT (TERENA): Trans-European Research and Education Network Association

Troyano – Caballo de Troya: Introducción subrepticia en un medio no propicio, con el fin de lograr un determinado objetivo.Diccionario de la Lengua Española. Vigésimo segunda edición. Programa que no se

replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.

Vulnerabilidad (Vulnerability): Una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada OTAN o los servicios y recursos que la soportan.

Vulnerabilidad: Una debilidad que puede ser aprovechada por una amenaza.

Zombi: Ver bot / botnet