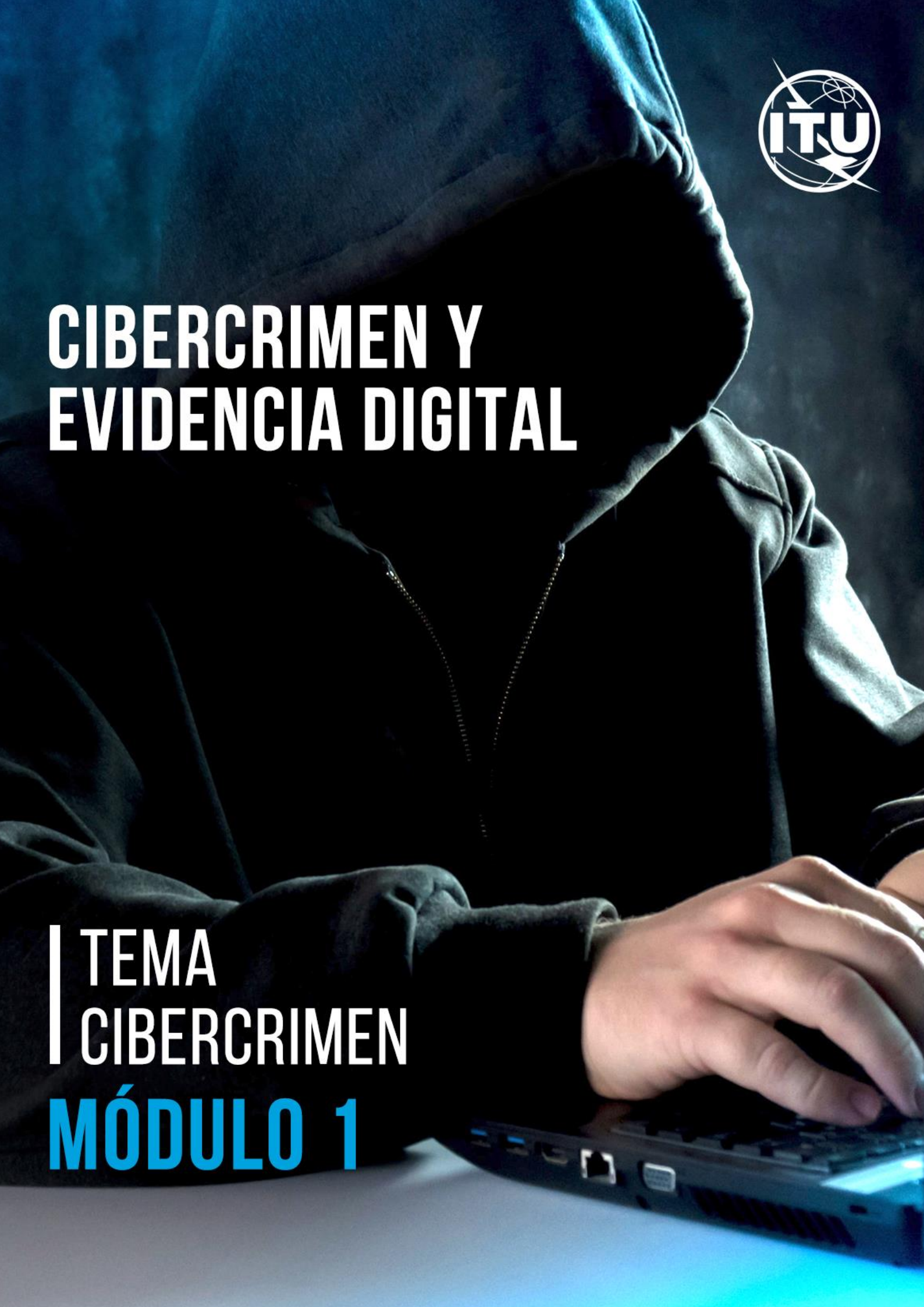


CIBERCRIMEN Y EVIDENCIA DIGITAL

TEMA CIBERCRIMEN

MÓDULO 1

TABLA DE CONTENIDOS

MÓDULO 1 3

CIBERCRIMEN 3

1. INTRODUCCIÓN 3

2. CIBERSEGURIDAD 4

Información 5

Seguridad de la información 8

Ciberseguridad 10

Amenazas y vulnerabilidades 12

3. CIBERCRIMEN 14

Ciberdelincuencia 15

Crecimiento del cibercrimen 16

Ciberdelincuentes 17

4. CIBERTERRORISMO 20

Ataques contra las infraestructuras críticas 21

5. BIBLIOGRAFÍA 21

MÓDULO 1

En el presente módulo se contempla una breve introducción a los aspectos básicos de la ciberseguridad y el cibercrimen, así como su interrelación con el mundo físico.

CIBERCRIMEN

El Objetivo del módulo es aprender y aplicar los conceptos básicos ciberseguridad, cibercrimen y ciberterrorismo.

1. INTRODUCCIÓN

En el mundo físico hablamos a menudo de la delincuencia que azota las ciudades. Hay bloques de noticias en los diarios, radio y televisión dedicados a la delincuencia todos los días. Por su parte, el Gobierno invierte recursos en mejorar la infraestructura y brindar más capacidades a la policía, ministerio público, poder judicial y otros actores locales para dar respuesta al quehacer criminal.

Hoy en día, el uso y aplicación de las tecnologías de la información y comunicación (TIC) son transversales a todas las actividades humanas y de una u otra manera nos vamos involucrando cada vez más en el uso de dispositivos conectados a internet, tal como una computadora, un teléfono, una televisión, una cámara de video, una luminaria o cualquier otra “cosa”, y sabemos que el uso y aprovechamiento adecuado nos hace más productivos y eficientes tanto en el trabajo y en los estudios como en el hogar y a nivel personal. También usamos las tecnologías de la información y comunicaciones para actividades sociales, entretenimiento y ocio en general.

Esto mismo ocurre con los delincuentes, y por lo tanto sus dispositivos electrónicos de TIC pueden contener información vital que puede usarse como pruebas de los delitos cometidos.

Por otro lado, la posibilidad de tener dispositivos conectados y la interacción con el internet ha dado origen a un universo virtual, al que llamamos ciberespacio y así se ha constituido una dimensión nueva, dónde los delincuentes también pueden llevar a cabo actos ilícitos o delitos. En efecto, la dependencia de las TIC ha llevado a los delincuentes a incursionar en un nuevo ámbito, desarrollando nuevas habilidades y descubriendo nuevas modalidades para cometer sus acciones ilícitas, cuyas repercusiones en el mundo físico pueden tener consecuencias como pérdidas económicas, daños en

infraestructuras críticas, afectación a los servicios públicos, y hasta pérdida de vidas humanas.

2. CIBERSEGURIDAD

Desde finales del siglo pasado se empezó a hablar de la "sociedad de la información" para dar énfasis al uso intensivo de las tecnologías de la información y comunicación y su papel fundamental para el desarrollo de la economía de los países.

En el 2001, la Asamblea General de las Naciones Unidas acordó realizar la "Cumbre Mundial sobre la Sociedad de la Información (CMSI)"[1], la cual se desarrolló en dos fases: Ginebra (2003) y Túnez (2005).

En la primera fase, en Ginebra, se aprobaron los "Principios de Ginebra" y el "Plan de Acción". En la segunda fase, en Túnez, se aprobaron los "Agenda" y el "Compromiso de Túnez" para la Sociedad de la Información. En cada documento, se incluyeron aspectos relacionados a la seguridad de la información y la ciberseguridad como aspecto básico para el desarrollo de la Sociedad de la Información.

.

En la "Declaración de Principios - Construir la Sociedad de la Información: un desafío global para el nuevo milenio", indica lo siguiente:

B5) Fomento de la confianza y seguridad en la utilización de las TIC

35.El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la Sociedad de la Información orientados al desarrollo.

[1] https://www.itu.int/net/wsis/

36. Si bien se reconocen los principios de acceso universal y sin discriminación a las TIC para todas las naciones, apoyamos las actividades de las Naciones Unidas encaminadas a impedir que se utilicen estas tecnologías con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, y que podrían menoscabar la integridad de las infraestructuras nacionales, en detrimento de su seguridad. Es necesario evitar que las tecnologías y los recursos de la información se utilicen para fines criminales o terroristas, respetando siempre los derechos humanos.

37. El envío masivo de mensajes electrónicos no solicitados ("spam") es un problema considerable y creciente para los usuarios, las redes e Internet en general. Conviene abordar los problemas de la ciberseguridad y "spam" en los planos nacional e internacional, según proceda.

Fuente: https://www.itu.int/net/wsis

Información

La información es algo que se obtiene luego del procesamiento de un conjunto de datos. En un sistema básico de comunicación, la información es el mensaje que es enviado desde un transmisor a través de un canal (medio) hasta un receptor. De esta manera la información se ha enviado desde la fuente hasta un destinatario.

La información puede tomar forma de documentos, imágenes, audio, video, etc. en soporte físico (papel, disco compacto, disco duro, etc), almacenada (en algún arreglo de servidores, localmente en un ambiente, o en la nube) y/o circulando a través de las redes de comunicaciones y el internet.

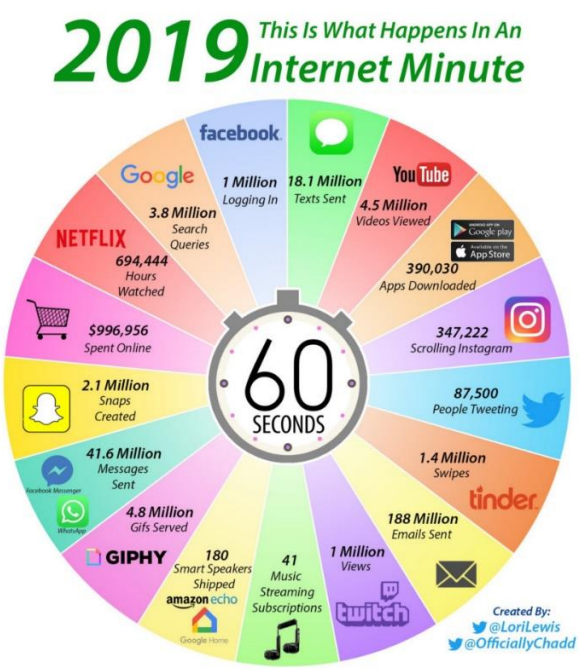
Con el avance tecnológico, la expansión de la infraestructura y los servicios de tecnologías de la información y comunicaciones cada vez más usuarios acceden a Internet y crece el número de conexiones de banda ancha. Esto se traduce en un incremento día a día del tráfico digital a nivel global. Este tráfico está compuesto de información que se genera, transcurre a través de las redes y se almacena en formato digital y, por lo tanto, la información también crece exponencialmente.

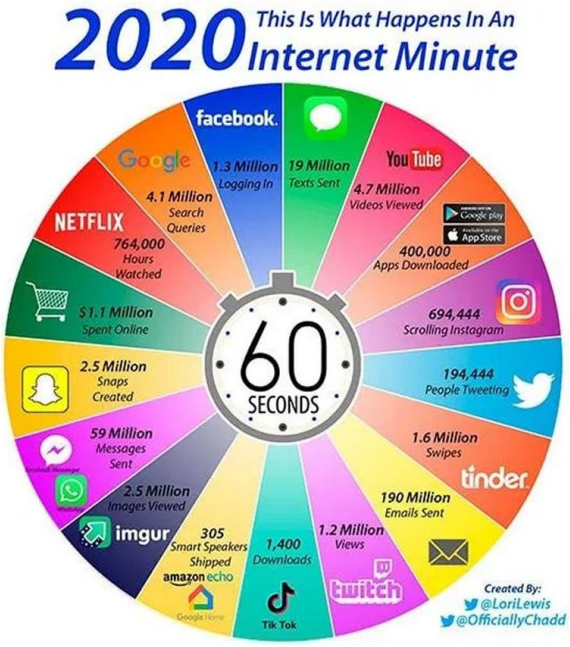
Parte de toda esta información que se produce, circula y se almacena digitalmente corresponde a datos privados y datos personales, como grabaciones de audio y video, imágenes, mensajería, etc. En el ámbito académico, corporativo y

gubernamental, la cantidad de información también crece de manera exponencial. Y las amenazas son cada vez más sofisticadas frente a las vulnerabilidades también crecientes.

En la infografía ¿qué pasa en internet en un minuto?, podemos apreciar la representación de la gran cantidad de información en forma de mensajes de texto, audio, videos y transacciones electrónicas en general se realizan en un minuto. Y esto seguirá creciendo.

Infografía: ¿QUÉ PASA EN INTERNET EN UN MINUTO?





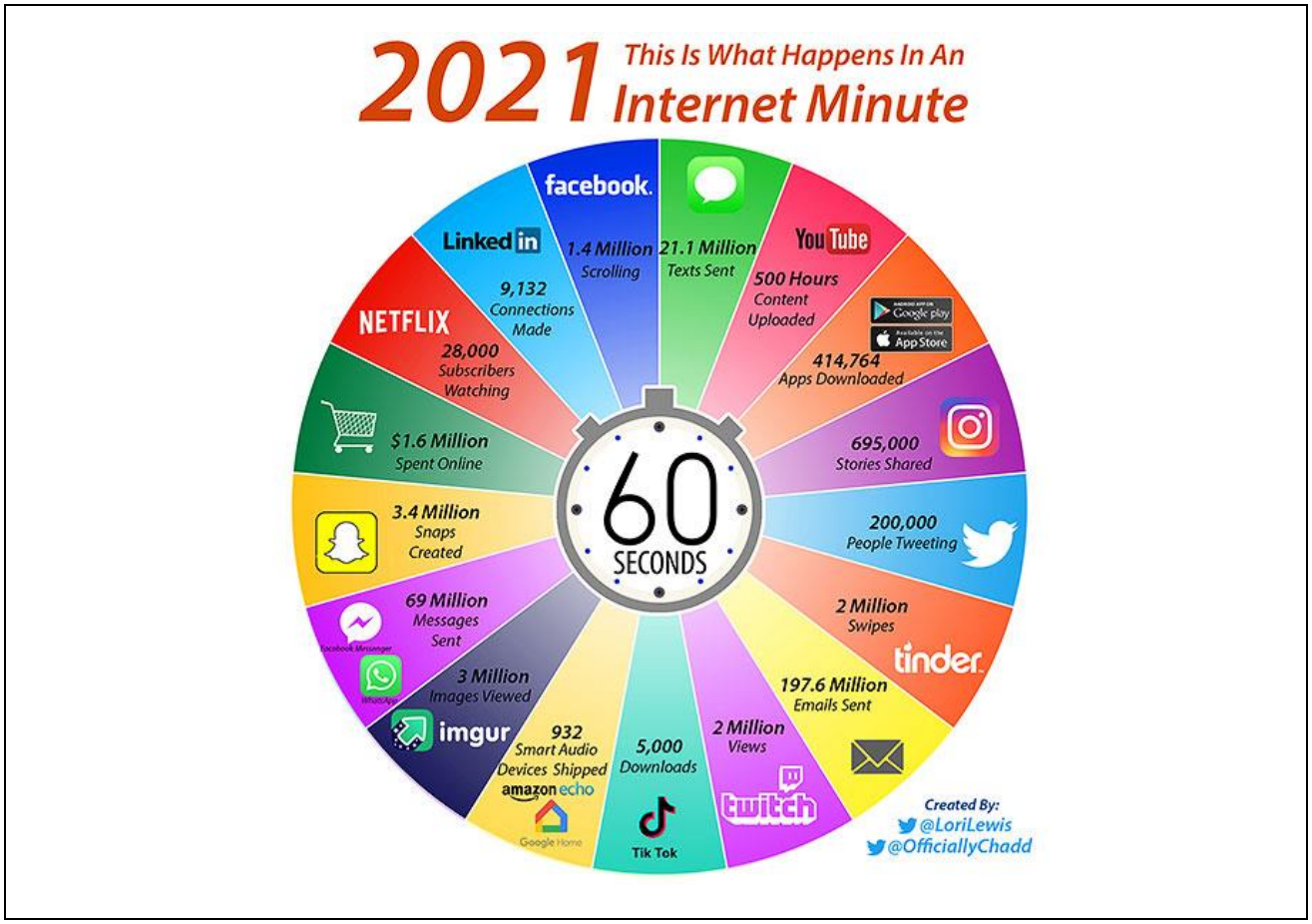


Fig. 1. Infografía ¿qué pasa en internet en un minuto

Fuente: @LoriLewis, @OfficiallyChadd

Teniendo en cuenta lo anterior veamos la definición oficial de la “International Organization for Standardization” en la ISO/IEC 27000:2018 Overview and vocabulary.

Definición Información

La información es un activo que, al igual que otros activos importantes de la empresa, es esencial para el negocio de una organización y, por lo tanto, requiere ser protegido adecuadamente. La información puede ser almacenada en muchas formas, incluyendo: formato digital (ejemplo: archivos de datos almacenados en medios electrónicos u ópticos), forma material (ejemplo: en papel), así como información en forma de conocimiento de los empleados. La información puede ser transmitida por diversos medios, incluyendo: mensajería, comunicación electrónica o verbal. Cualquiera que sea el formato de la información, o los medios por los que se transmita, siempre necesita una protección adecuada.
En muchas organizaciones, la información depende de la tecnología de la información y las comunicaciones. Esta tecnología es a menudo un elemento esencial en la organización y ayuda a facilitar la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de la información.

Fuente: ISO/IEC 27000:2018(E), Fifth edition 2018-02, Information technology — Security techniques — Information security management systems — Overview and vocabulary

Y esta información producida ¿tiene algún dueño? ¿es de acceso público? ¿es privada? ¿todos podrían utilizarla? ¿se comenten crímenes haciendo uso de información? Hay muchas preguntas al respecto; sin embargo, queda claro que debemos proteger la información importante, aquella que es crítica y que de sufrir alguna vulneración pudiera existir consecuencias negativas. Entonces, proteger la información es una necesidad y para ello la información debería clasificarse y aplicar los controles adecuados para brindar el nivel de seguridad de la información requerido.

Cada día es más complicado proteger de manera efectiva la información sea física y digital, y no solamente por el creciente volumen de información y la sofisticación de los ataques, sino también por una carencia de recursos humanos con las habilidades y competencias necesarias para mejorar el nivel de seguridad de la información y la ciberseguridad.

La “Seguridad de la Información” está referida a la protección de la información, sin importar el formato o el medio dónde se encuentra, contra el acceso no autorizado, la manipulación o alteración, daño o robo.

Definición Seguridad de la Información

La seguridad de la información garantiza (asegura) la confidencialidad, disponibilidad e integridad de la información. La seguridad de la información implica la aplicación y la gestión de controles apropiados que involucra la consideración de una amplia gama de amenazas, con el objetivo de asegurar el éxito y continuidad del negocio sostenido, y minimizar las consecuencias de los incidentes de la seguridad de la información.

La seguridad de la información se logra a través de la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos y gestionados mediante un SGSI (sistema de gestión de seguridad de la información), incluyendo políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información identificados. Estos controles necesitan ser especificados, implementados, monitoreados, revisados y mejorados cuando sea necesario, para asegurar que se cumple la seguridad de la información y los objetivos empresariales de la organización.
Se espera que los controles de seguridad de la información pertinentes se integren perfectamente con los procesos empresariales de una organización.

Fuente: ISO/IEC 27000:2018(E), Fifth edition 2018-02, Information technology — Security techniques — Information security management systems — Overview and vocabulary

La seguridad de la información se basa en tres pilares o propiedades: la confidencialidad, la integridad y la disponibilidad.

- Asegurando la confidencialidad, mantenemos la privacidad y protegemos la información contra el acceso no autorizado, se evita, por ejemplo, la divulgación de la información.
- Asegurando la integridad protegemos la información contra modificaciones no autorizadas.
- Asegurando la disponibilidad protegemos la información para que siempre permanezca accesible y sin interrupciones.

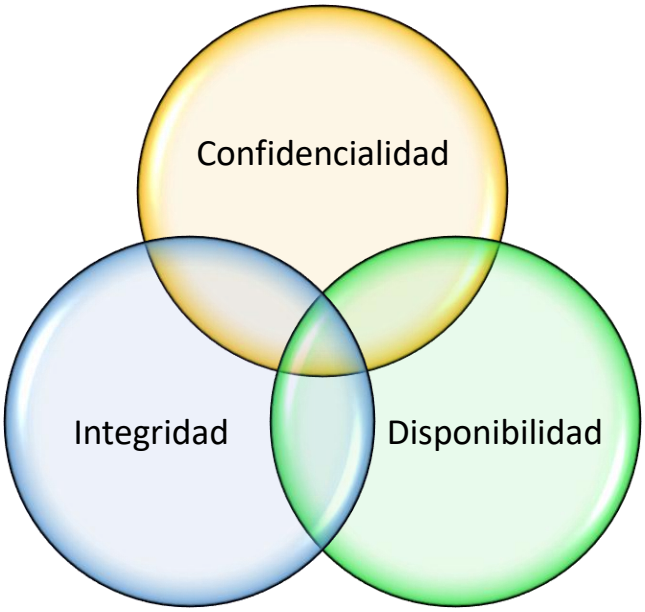


Fig. 2. Triada de la Seguridad / ciberseguridad

Hoy en día se da por hecho la existencia de “información” en todos los aspectos de nuestra vida, y en muchos casos esta información depende en gran medida de las tecnologías de información y comunicación. Sin embargo, aún tenemos pendiente concientizar a la población en temas de seguridad de la información y ciberseguridad.

Ciberseguridad

Cuando hablamos de ciberseguridad, nos referiremos a la seguridad de la información en entornos digitales conectados. En este sentido, podría entenderse que la ciberseguridad se encuentra contenida en el alcance de la seguridad de la información.

La ciberseguridad tiene como objetivo proteger los activos de información digital de los individuos u organizaciones, es decir de aquella información se encuentre procesada, almacenada y transportada por sistemas de información interconectados (tecnologías de la información y comunicación). Estos activos de información digital se encuentran en lo que denominamos “ciberespacio”. Para la Real Academia Española, ciberespacio significa “ámbito virtual creado por medios informáticos”.

Se puede inferir que la ciberseguridad es parte de la seguridad de la información, sin embargo, algunos autores sostienen que la ciberseguridad, adicionalmente, puede incluir actividades de respuesta activa y ataque.

Los tres pilares de la seguridad de la información también lo son cuando hablamos de ciberseguridad: Confidencialidad, Integridad y Disponibilidad. En el siguiente cuadro, presentamos la definición de la ciberseguridad de acuerdo a la Recomendación ITU-T X.1205 de la Unión Internacional de Telecomunicaciones.

Definición ciberseguridad

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. Las propiedades de seguridad incluyen una o más de las siguientes:

- disponibilidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- confidencialidad.

* Ciberentorno: Esto incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes.

Fuente: Recomendación ITU-T X.1205, 04/2008, Seguridad en el Ciberespacio – Ciberseguridad -Aspectos generales de la ciberseguridad.

Sin embargo, algunas definiciones van un poco más allá, cómo la planteada por la Organización Internacional de Estandarización (ISO) en la Norma ISO/IEC 27032 Guidelines for cybersecurity:

Definición ciberseguridad

Condición de estar protegido en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales, o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el ciberespacio que se pueda considerar no deseable.

Definición de Ciberespacio
Entorno complejo que resulta de la interacción de personas, software y servicios en internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física.

Fuente: ISO/IEC 27032:2012(E), Information technology -- Security techniques -- Guidelines for cybersecurity.

Al hablar de ciberseguridad debemos incorporar los conceptos de ciber-entorno/ciberespacio. Y, si la información crece con gran aceleración, podemos inferir que el ciberespacio también está crecimiento, como el espacio sideral. Por ello, podemos concluir que la ciberseguridad tiene un rol importante para mantener un ambiente estable y confiable tanto en el ciberespacio como en el mundo real, atenuando las consecuencias a nivel del ciudadano, de las organizaciones y también en el ámbito nacional (incluyendo la seguridad nacional) e internacional.

Amenazas y vulnerabilidades

La utilización de las redes de telecomunicaciones, el Internet y la interoperabilidad de tecnologías y sistemas, entre otros factores, han hecho posible no solamente el aumento de nuestra productividad, sino que nos ha expuesto mundialmente a amenazas capaces de aprovechar vulnerabilidades locales para acceder maliciosamente a nuestros recursos informáticos e información.

- ✓ Activo: Algo que tiene valor para la organización.
- ✓ Amenaza: Evento que puede provocar un incidente en la organización produciendo daños o pérdidas materiales y/o inmateriales.
- ✓ Vulnerabilidad: Susceptibilidad de algo para absorber negativamente incidencias externas. Falta de control.

Fuente: Recomendación ITU-T X.1205, 04/2008, Seguridad en el Ciberespacio – Ciberseguridad -Aspectos generales de la ciberseguridad

Las amenazas a que nos enfrentamos son de diversa índole, por ejemplo, los ataques de denegación de servicios son cada vez más potentes, el robo de datos financieros y personales es cada vez más frecuente, los fallos de red y la interrupción de comunicaciones de voz y datos también se han incrementado. El malware, tal como los virus, gusanos, caballos de Troya, ransomware, etc. son cada vez más sofisticados.

En ciberseguridad, las amenazas se pueden clasificar de acuerdo al tipo de activo:

- Amenazas a activos personales
  Estas amenazas tienen el objetivo, por ejemplo, de sustraer información personal para cometer fraudes bancarios o chantaje personal, secuestrar los dispositivos de conexión para utilizar su poder de procesamiento para fines delictivos, etc.

- Amenazas a activos organizacionales
  Estas amenazas tienen variados objetivos, tal como el robo de información, la divulgación de información, crear indisponibilidad de servicios, etc.

- Amenazas a activos críticos nacionales
  Estas amenazas tienen como objetivo a las infraestructuras críticas nacionales, generalmente con fines de terrorismo.

Las ciber amenazas tomarán ventaja sobre las vulnerabilidades para tener éxito en su objetivo. Una vulnerabilidad, en ciberseguridad, es un defecto o debilidad del diseño o implementación de un sistema de información o su entorno, que se podría aprovechar de manera intencional o no intencional para afectar desfavorablemente los activos u operaciones de una organización (ISO/IEC TR 19791:2006).

Entonces, para evitar que las ciber amenazas tengan éxito, las vulnerabilidades deben ser tratadas y reducidas constantemente.

La ciberseguridad necesita de un conjunto de actividades para gestionar los riesgos y reducir el impacto negativo que pudiera producir una amenaza aprovechando una vulnerabilidad, de tal manera que podemos conseguir un nivel adecuado de la

confidencialidad, disponibilidad e integridad de la información. Para la gestión de riesgos debemos seguir un proceso, que en líneas generales se resume en:

1. Determinar el contexto del análisis de riesgos
2. Identificar, valorar y elegir los activos que se protegerán
3. Identificar y valorar las amenazas a los activos que se protegerán
4. Identificar y valorar las vulnerabilidades a los activos que se protegerán
5. Identificar y evaluar los riesgos teniendo en cuenta su impacto
6. Identificar y establecer controles de seguridad para contrarrestar los riesgos y reducirlo a un nivel aceptable
7. Aceptación del riesgo.

- Riesgo: efecto de la incertidumbre sobre los objetivos. [ISO/IEC 27000:2018]
  Nota 1: un efecto es una desviación de lo esperado: positivo o negativo.
  Nota 2: la incertidumbre es el estado, incluso parcial, de la deficiencia de información relacionada con, la comprensión o el conocimiento de, un acontecimiento, su consecuencia, o la probabilidad.
  Nota 3: el riesgo se caracteriza a menudo por referencia a posibles "eventos" y "consecuencias", o una combinación de estos.
  Nota 4: el riesgo se expresa a menudo en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la "probabilidad" asociada de ocurrencia.
  Nota 5: en el contexto de los sistemas de gestión de la seguridad de la información, los riesgos de seguridad de la información pueden expresarse como efecto de incertidumbre sobre los objetivos de seguridad de la información.
  Nota 6: el riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten vulnerabilidades de un activo de información o un grupo de activos de información de tal manera que cause daño a una organización.

3. CIBERCRIMEN

Considerando el escenario actual, dónde el avance tecnológico hace posible que el usuario conectado tenga a disposición muchos servicios y contenidos, lo que incrementa también la probabilidad de que una amenaza aproveche una vulnerabilidad. Por ello, al referirnos al ciberespacio y la ciberseguridad es necesario abordar a los ciberdelitos. El ciberdelito y la ciberseguridad son aspectos que difícilmente pueden considerarse separados en un entorno interconectado (Gercke, 2014).

Las vulnerabilidades, el incremento de amenazas, la falta o deficiencias de los planes de tratamiento de riesgos, y las limitaciones en la implementación de controles de seguridad en las tecnologías digitales contribuyen a crear un ambiente con cierto nivel de inseguridad, lo cual es aprovechado por los ciberdelincuentes o cibercriminales.

Ciberdelincuencia

Teniendo en cuenta la existencia del ciberespacio, los delincuentes también encuentran un nuevo ámbito para cometer sus actos ilícitos; por ello, la erradicación del ciberdelito es una preocupación importante para nuestras autoridades a nivel global. Los países realizan acciones a nivel jurídico, técnico e institucional, y establecen marcos de cooperación internacional teniendo en cuenta que en el ciberespacio no existen las fronteras geográficas.

El ciberdelito o cibercrimen es una actividad criminal que implica que los servicios o aplicaciones en el ciberespacio se utilicen o sean blanco de un crimen (ISO/IEC 27032), lo que significa que el ciberespacio es la fuente, herramienta, blanco o lugar de un crimen.

Ciberdelincuencia

En el taller que tuvo lugar con ocasión del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente se elaboraron dos definiciones de ciberdelincuencia o cibercrimen:

- Ciberdelincuencia en sentido estricto (delito informático) comprende cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y de los datos que éstos procesan.
- En sentido general, ciberdelincuencia (delitos relacionados con los computadores) comprende cualquier comportamiento ilícito cometido por medio de un sistema informático o una red de computadores, o relacionado con éstos, incluidos delitos tales como la posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadores.

Fuente: Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica. Autor: Prof. Dr. Marco Gercke. Oficina de Desarrollo de las Telecomunicaciones de la UIT.

El 23 de noviembre de 2001, en Budapest, se firmó el Convenio sobre Ciberdelincuencia, desarrollado bajo el auspicio del Consejo de Europa. Tras la ratificación de cinco Estados, entró en vigencia desde el 2004. Fue el primer tratado de carácter internacional que tiene el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. Los aspectos más importantes de este Convenio son:

- Derecho penal sustantivo: Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos informáticos; delitos relacionados con el contenido; delitos relacionados con infracciones a la propiedad intelectual y derechos afines;
- Derecho procesal: almacenamiento rápido de los datos informáticos y de los relativos al tráfico y a su entrega rápida a las autoridades competentes; a la conservación y protección de la integridad de los datos durante el tiempo necesario; al mandato u orden de presentación; a la captura y registro de los datos almacenados; al registro de datos en tiempo real; a la protección adecuada de los derechos humanos y libertades;
- Jurisdicción: Los Estados deben adoptar las medidas legislativas y de otra índole, necesarias para establecer como infracción penal, sin perjuicio de las leyes nacionales, los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, así como los delitos informáticos. Los Estados deben establecer sus competencias respecto a toda infracción penal siempre que ésta se haya cometido en su territorio; a bordo de un barco o aeronave;
- Cooperación internacional: extradición; colaboración y asistencia mutua, procedimientos aplicables, medidas provisionales, investigación, creación de una red de colaboración 24/7 (disponible las veinticuatro horas de los siete días de la semana).

A nivel internacional existe predisposición para establecer marcos jurídicos y cooperación, sin embargo, es muy difícil coordinar la realización de acciones operativas para la lucha contra la ciberdelincuencia y el crimen organizado.

Crecimiento del cibercrimen

Como ejemplos de cibercrimenes o ciberdelitos podemos mencionar las siguientes infracciones: robo, sabotaje de información, ataques a los derechos de copia, al derecho

de autor, a la violación del secreto profesional, de la intimidad digital, de la propiedad intelectual, difusión de contenidos ilegales, ataques contra la competencia, espionaje industrial, violación de los derechos de las marcas, difusión de informaciones falsas, denegación de servicio, fraudes diversos, etc.

En nuestra sociedad actual, el cibercrimen ha encontrado muchas facilidades para su accionar:

- La desmaterialización y la facilidad de comunicación permite utilizar esquemas que permiten el anonimato y el cifrado, lo cual hace posible que los cibercriminales puedan comunicarse en forma segura para realizar su accionar delictivo (organizar, planificar y ejecutar cibercrimenes).
- El mundo virtual abre la posibilidad de explotar vulnerabilidades con fines malintencionadas, por ejemplo: usurpación de identidad, falsificación de direcciones, accesos indebidos, explotación fraudulenta de recursos, infección, deterioro, destrucción, modificación, divulgación, robo de datos, chantaje, extorsión, intimidación, denegación de servicio, etc.
- La falta de conciencia en ciberseguridad, permite que muchas personas estén expuestas fácilmente a cibercrimenes, tales como robo de identidad, el control de dispositivos de cómputo, etc.
- La disponibilidad de herramientas de detección y explotación de vulnerabilidades facilita la ejecución de ataques informáticos.
- Inexistencia de un marco jurídico armónico entre los Estados y la falta de coordinación eficaz de las políticas.
- Problemas para identificar los rastros de los autores de un delito, e identificar y obtener la evidencia o prueba digital. Además, los rastros digitales se podrían extender en varios sistemas de distintos países.
- La desvinculación territorial en el ciberespacio, permite variedad de opciones a los cibercriminales al no existir jurisdicción física de los Estados.
- Existencia de paraísos digitales, dónde no existen leyes que repriman el delito informático.

Ciberdelincuentes

Un agente de amenaza es un individuo o grupo de individuos que tiene cualquier rol en la ejecución o soporte de un ataque. El entendimiento de sus motivos (religiosos, políticos, económicos, etc.), capacidades (conocimiento, financiamiento, tamaño, etc.) e intenciones (diversión, crimen, espionaje, etc.) es crucial en la evaluación de vulnerabilidades y riesgos, así como en el desarrollo y despliegue de controles.

En efecto, para protegernos del accionar de los cibercriminales o ciberdelincuentes es necesario adelantarnos tomando las acciones preventivas necesarias. Esto no solamente incluye la evaluación de vulnerabilidades y aplicación de los controles respectivos, sino también la evaluación de las amenazas; y en este caso, se debe evaluar el perfil de los atacantes para saber de quién se le debe proteger los activos de información.

Diversos autores clasifican de diversas formas a los ciberdelincuentes; una de ellas corresponde a dos grandes tipos de ciberdelincuentes: los profesionales cuyas actividades son directamente rentables, y los aficionados que suelen estar animados por una gran necesidad de reconocimiento social.

Los profesionales son generalmente:

- competidores directos de la organización objetivo;
- funcionarios al servicio del Estado;
- mercenarios (que pueden actuar por encargo de instituciones tanto privadas como públicas);
- malhechores de cualquier tipo.

Estos ciberdelincuentes con conocimiento avanzados son capaces de penetrar en las computadoras o redes para obtener acceso por varios motivos. Teniendo en cuenta su motivación, Cisco System los clasifica como:

- Hacker de sombrero blanco: penetran en las redes o los sistemas informáticos para descubrir las debilidades a fin de mejorar la seguridad de estos sistemas. Los propietarios del sistema les otorgan permiso para realizar la interrupción y reciben los resultados de la prueba
- Hacker de sombrero gris están en algún lugar entre los atacantes de sombrero blanco y negro. Los atacantes de sombrero gris pueden encontrar una vulnerabilidad y señalarla a los propietarios del sistema si esa acción coincide con sus propósitos. Algunos hackers de sombrero gris publican los hechos sobre la vulnerabilidad en Internet para que otros atacantes puedan sacarles provecho.
- hacker de sombrero negro: aprovechan las vulnerabilidades para obtener una ganancia ilegal personal, financiera o política

Entre los aficionados, destacan:

- los técnicos, sucesores de los primeros aficionados, piratas informáticos de los primeros tiempos, cuya motivación esencial era el deseo de dominar cada vez más las tecnologías;
- los curiosos;
- los inmaduros: que se suelen denominar «script-kiddies» o «kiddiots», que tienen pocas habilidades o ninguna, y generalmente usan herramientas existentes o instrucciones que se encuentran en Internet para realizar ataques;
- los psicópatas;
- los militantes, movidos por ideologías o religión, que además se suelen encontrar a mitad de camino entre los aficionados y los profesionales.

Muchos de los ataques en el Ciberespacio se llevan a cabo usando software malicioso como spywares, gusanos y virus. La información se suele recolectar a través de técnicas de suplantación de identidad. Un ataque puede ocurrir como un vector de ataque único o llevado a cabo como un mecanismo de ataque combinado. Estos ataques se pueden propagar vía, por ejemplo, sitios Web no confiables, descargas de archivos no verificados, correos electrónicos basura (spam), explotación remota y medios extraíbles infectados.

Los ataques pueden venir desde dos categorías principales:

- Ataques desde dentro de una red privada
  Estos ataques se lanzan normalmente dentro de la red privada de una organización, típicamente la red de área local, y pueden ser iniciados por empleados o por alguien que obtenga acceso a un computador o red en las instalaciones de una organización o individuo. El atacante puede usar mecanismos como un software analizador de paquetes para obtener contraseñas u otra información de identidad. De manera alternativa, el atacante se puede enmascarar como una entidad autorizada y actuar como intermediario para robar información de identidad.
- Ataques desde fuera de una red privada.
  Hay muchos ataques diferentes que se pueden lanzar desde el exterior de una red privada, incluyendo Internet.
  Si bien el ataque Inicial siempre tendrá como objetivo un sistema de cara al público (por ejemplo, router, servidor, firewall, sitio Web, etc.), los atacantes pueden también buscar explotar activos que estén dentro de la red privada.
  Los atacantes son cada vez más sofisticados y normalmente combinan diferentes técnicas y mecanismos de ataque para maximizar su éxito, lo que hace que la detección y prevención de ataques sean más difíciles.
  Por ejemplo, un atacante puede realizar el escaneo de puertos de un servidor para confirmar qué puertos están “abiertos” y luego obtener otra información del servidor (sistema operativo, servicios, software, etc.) para realizar ataques como Denegación de Servicio, explotación de vulnerabilidades del servidor, suplantación de IP, etc.

  Hay casos en que los ataques son una combinación tanto desde dentro como desde fuera de una red privada. Otros mecanismos que han crecido, tanto en uso como en sofisticación, son aquellos que se basan en la ingeniería social y en el uso de archivos corrompidos en sitios Web legítimos.

Finalmente, no podemos dejar de mencionar a los Hackers organizados, organizaciones de delincuentes informáticos, hacktivistas, terroristas y hackers patrocinados por el Estado. Estos ciberdelincuentes, generalmente, son grupos de delincuentes profesionales centrados en el control, la energía y la riqueza. Los delincuentes son muy sofisticados y organizados, e incluso pueden proporcionar el delito cibernético como un servicio. Los hacktivistas hacen declaraciones políticas para concientizar sobre los problemas que son importantes para ellos.

Los atacantes patrocinados por el Estado reúnen inteligencia o sabotean en nombre de su gobierno. Estos atacantes suelen estar altamente capacitados y bien financiados.

4. CIBERTERRORISMO

Aunque hasta la fecha no hay consenso en la definición de ciberterrorismo, podemos decir que el ciberterrorismo implica el uso de las tecnologías de la información y comunicación, tal como equipos de cómputo, con la intención de causar daño, con el fin de coaccionar a una población civil e influir en la política del gobierno objetivo o afectar su conducta.

Las tecnologías de la información y la comunicación (TIC) pueden utilizarse con múltiples objetivos relacionados con el desarrollo, educación, bienestar, etc., sin embargo, también facilita la comisión de delitos incluyendo actos relacionados con el terrorismo (una forma de terrorismo propiciado por medios cibernéticos) o pueden ser el objetivo de los terroristas (una forma de terrorismo dependiente de la cibernética). Concretamente, las TIC pueden utilizarse para promover, apoyar, facilitar o participar en actos de terrorismo. El internet puede utilizarse con fines terroristas, como la difusión de «propaganda (incluido el reclutamiento, la radicalización y la incitación al terrorismo), la financiación [del terrorismo], el entrenamiento [de terroristas], la planificación [de ataques terroristas] (incluso a través de la comunicación secreta y la información de fuente abierta), la ejecución [de ataques terroristas] y los ciberataques» (UNODC, 2012, pág. 3).

El ciber-terrorismo tiene varias características distintas. Estas características ayudan a diferenciar mejor entre un ciber-terror y un mero ataque o actividades de un hacker. Según Chanbey, el ciberterrorismo mostrará y puede mostrar los siguientes signos:

a) El ataque está predefinido y las víctimas son un objetivo específico.
b) El ataque tiene el objetivo de destruir o dañar objetivos específicos, como políticos, económicos, infraestructuras energéticas, civiles y militares
c) El ataque puede incluso tener como objetivo las infraestructuras de información de grupos religiosos opuestos específicos para comprender el pandemonio religioso.
d) El propósito de cualquier ataque es crear temor a las intenciones del grupo y promover su propia agenda u objetivos políticos o ganar compañerismo al tener éxito en sus ataques.
e) Destruye las capacidades del enemigo.

f) Persuadir a otros para que crean que la víctima o víctimas son vulnerables y su estabilidad negligente.
g) Crear mayor lealtad y orgullo dentro del grupo en base a sus éxitos.

Ataques contra las infraestructuras críticas

El ciberterrorismo puede apuntar a las Infraestructuras Críticas para lograr sus objetivos. Las infraestructuras críticas esenciales para el buen funcionamiento de la sociedad (energía, agua, transportes, logística alimentaria, telecomunicaciones, bancos y servicios financieros, servicios médicos, funciones gubernamentales, etc.), resultan más vulnerables por su creciente utilización e interacción con las tecnologías de la información y comunicación asociadas al Internet.

Es fundamental asegurar las infraestructuras críticas y crear, ya sea a nivel regional o nacional, organismos encargados de su protección. Los Gobiernos están tomando medidas para la ciberseguridad y la protección de sus infraestructuras críticas a través de regulación y fortalecimiento de dichas infraestructuras. Las iniciativas también se realizan a nivel internacional con la finalidad de combatir más efectivamente este riesgo.

5. BIBLIOGRAFÍA

ISO/IEC 27000:2018(E), Fifth edition 2018-02, Information technology — Security techniques — Information security management systems — Overview and vocabulary
ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity.
CompTIA® Security+® (Exam SY0-501), Pamela J. Taylor, Jason Nufryk
Fundamentos de la Ciberseguridad, ISACA,2015
Guía de ciberseguridad para los países en desarrollo. Edición 2007, Unión Internacional de Telecomunicaciones
Recomendación UIT-T X.805 Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo
RECOMMENDATION ITU-T X.1051 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
Recommendation ITU-T X.1052 Information security management framework
Recomendación UIT-T X.1205 Aspectos generales de la ciberseguridad


ITU