# 1. Introducción a la Ciberseguridad

## 3. Amenazas a la Ciberseguridad

### 3.1 Introducción

Para poder aplicar medidas de seguridad y controles definidos por normas como las ISO 27000, es necesario conocer las amenazas a las que nos enfrentamos.

Las amenazas pueden dividirse en cuatro áreas clave:

- Amenazas a los activos personales;
- Amenazas a los activos de la organización;
- Amenazas a los activos virtuales, y
- Amenazas a la infraestructura.

Las **amenazas personales** giran principalmente en torno a la privacidad y la identidad, y los problemas que plantea la pérdida o el robo de información personal o información relativa a la información de crédito.

Si la identidad en línea de una persona es robada o falsificada, esa persona puede ser privada del acceso a servicios y aplicaciones clave.

En escenarios más graves, las consecuencias pueden ir desde incidentes financieros a incidentes a nivel nacional.

El acceso no autorizado a la información financiera de una persona también abre la posibilidad de robo de dinero de la persona y el fraude.

Otra amenaza es la posibilidad de ser un zombie o bot. Los dispositivos de computación personal pueden verse comprometidos y formar parte de una botnet más grande.

Por otro lado, la presencia de las **organizaciones** en línea y los negocios en línea son a menudo amenazados o secuestrados a. Las compañías son amenazadas por la delincuencia organizada con atacar sus sitios web, o con dañar su reputación a través de acciones como el defacement.

El **Mundo Virtual** de hoy vale un montón de dinero. Las divisas en línea tienen un valor en dinero del mundo real. Y los avatares, armas y elementos de un juego en línea se pueden vender y cambiar en el mundo real también.

Sin embargo, ¿cómo protegemos esos artículos, ante la ausencia de cajas fuertes y cerraduras a las que estamos acostumbrados en el mundo real? ¿Cómo podemos demostrar la propiedad y evitar el robo de identidad?

En el ámbito nacional o internacional, el ciberespacio es un área gris en la que el terrorismo prospera. Una de las razones es la facilidad de comunicación que proporciona. Debido a la naturaleza del ciberespacio, y concretamente a la dificultad de definir los límites y las fronteras, es complicado regular y controlar la forma en que se puede utilizar.

Los grupos terroristas pueden comprar aplicaciones, servicios y recursos que faciliten su causa, o pueden recurrir a medios ilegales de obtener estos recursos para evitar la detección y el

seguimiento. Esto puede incluir la adquisición de enormes recursos informáticos a través de botnets.

### 3.2 Amenazas

Las amenazas emergentes incluyen no sólo las transacciones en línea y aplicaciones de hoy en día - incluyendo los juegos de azar y apuestas -, sino también los sistemas de control industrial, robótica, domótica y sistemas de a bordo:

Los sistemas SCADA para monitorización, control, y gestión técnica remota y los sistemas de satélites también pueden ser objeto de amenaza.

Los servicios de Cloud Computing bajo demanda seguirán siendo objetivo de programas maliciosos dirigidos a los usuarios.

Todas las innovaciones técnicas están abiertas a los ataques, ya que los productos vienen a menudo con errores de diseño o de funcionamiento.

Los cambios en las redes sociales, junto con un creciente interés entre los usuarios en las comunicaciones electrónicas, sin duda van a generar amenazas contra las personas, empresas, organizaciones públicas y gobiernos.

Las posibilidades de chantaje y extorsión dirigidos a empresas y gobiernos podrían utilizar dichas redes para desacreditar, como por ejemplo al combinar el potencial de WikiLeaks y Facebook.

Los riesgos en Bioinformática, teniendo como objetivo la información médica personal para causar daño con fines delictivos, también deben ser tenidos en cuenta.

http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

Por un lado, el nivel de complejidad de la amenaza no se relaciona directamente con la complejidad de la tecnología. Por otro lado, hay que esperar que las amenazas se harán más innovadoras y sofisticadas. Se mejorará en localizar y explotar nuevas vulnerabilidades o antiguas sin corregir para el robo masivo de datos, a pesar de las medidas existentes y la vigilancia.

Además, los métodos de ingeniería social se harán más sutiles, y destinados a los usuarios de una forma más personalizada, como es el caso del Spear Phising.

**Amenazas a Activos Personales:**

Como hemos dicho, las amenazas a activos personales suelen relacionarse con la identidad y la información personal.

Por ejemplo, se vende información crediticia en el mercado negro que posteriormente podría usarse para facilitar el robo de identidad.

Posibles amenazas a activos e información personal:

- Scam
- Robo de datos
- Robo de dispositivos móviles: GPS, smartphones,…
- Robo de identidad digital, spoofing
- Robo de datos RFID
- Uso fraudulento de datos personales
- Robo masivo de datos bancarios, financieros y de tarjetas
- Invasión de privacidad
- Localización geográfica

- Chantaje, revelación de información comprometedora

Además de lo anterior, otros activos virtuales que están en el punto de mira son los bienes personales en los mundos virtuales y los juegos en línea. Los activos en un mundo virtual o en el mundo de los juegos en línea son objeto de ataques y explotación.

Robo virtual y atraco virtual son algunos de los neologismos de este tipo de ataques. La seguridad, en este caso, dependerá de la cantidad de la información del mundo real que sea accesible, así como del marco de la seguridad del mundo virtual en sí y de cómo se ha definido e implementado por su administrador.

Mientras que las normas y los reglamentos para la protección de los activos físicos reales, en relación con el ciberespacio, siguen en desarrollo, los relativos a los bienes virtuales son casi inexistentes.

Son los participantes los que deberán llevar poner en marcha las técnicas de protección necesarias para asegurar sus activos virtuales.

**Amenazas a Activos de Organizaciones:**

Las tres amenazas más comúnmente citadas son comunes a las empresas, las organizaciones y los gobiernos:

- Falta de disponibilidad: denegación de servicio, sabotaje, acceso bloqueado, parálisis
- Daños a los datos: estratégicos, personales, confidenciales, sensibles
- Daños a la imagen: desinformación, difamación, compromiso

En el caso de un ataque con éxito, la información personal de los empleados, clientes, socios o proveedores podría revelarse y dar lugar a sanciones en contra de las organizaciones, si se comprueba que estos activos estaban insuficientemente protegidos, lo que ha contribuido a facilitar el ataque.

Las regulaciones financieras también podrían verse violadas si se dan a conocer resultados de la organización de manera no autorizada.

Los gobiernos tienen información sobre seguridad nacional, estratégica, asuntos militares, de inteligencia, entre muchos otros elementos relacionados con el gobierno y el Estado, y también una gran cantidad de información sobre individuos, organizaciones y la sociedad en su conjunto.

Con una tendencia creciente y en expansión de ofrecer servicios de gobierno electrónico a través del ciberespacio, este es un nuevo canal, entre otros, para lanzar ataques y acceder a la información anterior que, si tiene éxito, podría causar graves riesgos para una nación, su gobierno y su sociedad.

### 3.3 Agentes de Amenazas

Un agente de amenaza es un individuo o grupo de individuos que tienen algún papel en la ejecución o el apoyo de un ataque.

Una completa comprensión de sus motivos (políticos, religiosos, económicos, etc), las capacidades (conocimientos, financiación, tamaño, etc) y las intenciones (diversión, crimen, espionaje, etc) es fundamental en la evaluación de vulnerabilidades y riesgos, así como en el desarrollo y la implementación de controles. Por otra parte, además del cibercrimen también debemos tener en cuenta que pueden producirse pérdidas debidas a fallos, funcionamientos incorrectos, negligencia y errores humanos.

Al hablar de los agentes podemos clasificarlos en tres categorías:

- Internos
- Externos
- Mixtos

La estimación general es que el 80% son amenazas internas y el 20% son amenazas externas, pero estas cifras no se basan en una fuente confiable y pueden llegar a ser contradictorias en términos de ocurrencia e impacto.

En cuanto a las tendencias algunos expertos señalan un aumento en la distribución de las amenazas internas, mientras que otros (que representan la mayoría) citan un aumento de las amenazas externas.

Entre los argumentos a favor de un incremento de las amenazas internas tenemos:

- La facilidad de llevar a cabo amenazas dirigidas
- El deterioro del clima social interno de organizaciones públicas y privadas
- El impacto de las insuficiencias internas y la negligencia
- La dificultad de llevar a cabo las amenazas externas debido al incremento de los niveles de seguridad

Entre los argumentos a favor de un incremento de las amenazas externas tenemos:

- El número de usuarios que están capacitados en nuevas tecnologías
- La mezcla de alta velocidad, contexto y conflictos internacionales
- Los incidentes relacionados con socios y agencias establecidas en otros países
- El desarrollo de crimen masivo relacionado con el desarrollo de Internet en los países emergentes
- Sistemas interconectados, con acceso fácil a los datos de la empresa y a los datos personales, y personas que siempre están conectadas
- La delincuencia organizada transnacional, que es difícil de contrarrestar con las mejoras tecnológicas, seguirá creciendo gracias a las lagunas perpetuas en la cooperación internacional.

Igualmente, también hay argumentos a favor de un incremento de las amenazas mixtas:

- La dificultad de los ataques sin ningún conocimiento desde el exterior
- El uso de medios sutiles de ingeniería social
- Ganancias compartidas con terceros externos durante los períodos de crisis

En la actualidad, la mayoría de los expertos coinciden en que la amenaza es principalmente interna, como resultado principalmente de accidentes o malicia humana.

En los próximos cinco años, la amenaza interna se espera que disminuya por efecto de mayores medidas de seguridad adoptadas por las empresas. Sin embargo, la amenaza externa se espera que aumente debido al desarrollo general de la interconectividad de Internet y de los sistemas.

El aumento de la ingeniería social se espera que conduzca a un aumento de este enfoque, que mezcla la actividad interna y externa

Además, el Cloud Computing externalizará los riesgos y hará que aumenten algunas amenazas externas.

**Agentes: Perfiles y Tipos**

La mayoría de los expertos encuentran una fuerte tendencia relacionada con la organización industrial de las actividades de la delincuencia cibernética, que incluye un modelo de negocio, planes de negocio, y políticas de precios tomadas del mundo comercial e incluso su servicio al cliente.

Esta observación implica que el perfil de hacker/cibercriminal independiente desaparecerá para dar lugar a una fuerza de trabajo mercenario contratado para llevar a cabo una misión, basado en las habilidades y el trabajo en equipo, para compartir el trabajo - y el riesgo - debido a la dispersión internacional.

En este sentido, parece que hay especialidades nacionales, como el software en Rusia, el hardware en Japón, …

También hay grupos de hackers especializados en propaganda, desestabilización y manipulación, que serán capaces de utilizar las redes sociales y los métodos de producción y falsificación que hasta ahora han sido reservados a los falsificadores.

Más allá de esta tendencia principal, algunos mencionan la persistencia de criminales de baja intensidad (ej. estafadores) que se aprovecharán de las oportunidades y el anonimato de los flujos digitales.

Los grupos de activistas (grupos partidistas, terrorista o extremista) representan una amenaza creciente, buscando el efecto multiplicador de los medios de comunicación y el anonimato de sus acciones a través de las tecnologías de la información. Estos movimientos usan Internet cada vez más a menudo como una forma de apoyar sus acciones.

**Agentes: Habilidades y Recursos**

La tendencia actual en las habilidades que se están demandando para estos agentes está cambiando.

Particularmente significativa es la importancia del dominio y venta de kits que hacen posible la creación o expansión de la actividad cibercriminal. Con los nuevos procedimientos que seguro que surgirán, especialmente para automatizar y ocultar los ataques, habrá grupos de delincuentes especializados en la reventa de servicios delictivos, así como otros grupos más diversos, que utilizarán estos servicios o trabajarán para grupos más grandes.

También se están demandando habilidades legales y financieras avanzadas, para después de llevar a cabo el lavado de dinero y acciones para proteger a los autores.

Cuanto más complejas sean las defensas, más avanzado debe ser el nivel de ataque.

Es más fácil penetrar en los sistemas (sistemas críticos, bancos, etc) para los que jugaron un papel en su desarrollo. Será importante garantizar que las personas que crean estos sistemas son leales.

Es más fácil penetrar en los sistemas (sistemas críticos, bancos, etc) para los que jugaron un papel en su desarrollo. Será importante garantizar que las personas que crean estos sistemas son leales.

Lo mismo ocurre para las personas que luchan contra la delincuencia informática, el riesgo es que se pueda comprometer un sistema debido al clima social, su nivel de compensación, o incluso una falta de reconocimiento.

Por tanto, debemos esperar un mayor nivel de habilidades y equipamiento para la ciberdelincuencia organizada, con la disponibilidad de expertos en operaciones delictivas.

A todo esto se une la industrialización y la creación de una economía real basada en los delitos informáticos, incluyendo:

- Niveles más altos de habilidad para los creadores de los recursos: herramientas y equipos
- Habilidades inferiores o similares para los usuarios de tales recursos.

El cibercrimen está considerado como un servicio, con la idea "CyberCrimeware as a Service". Ya se alquilan botnets y proxies para ataques DDoS y campañas de spam, troyanos que se compran y venden en sitios de subastas especializados, y que están disponibles para el público en general.

**Agentes: Estructuras y Organizaciones**

La delincuencia organizada está creando poderosas estructuras, como las empresas de delitos digitales que existen hoy en el antiguo bloque soviético, y como se espera ocurrirá en África y América del Sur.

Es y será un jugador importante con operaciones a gran escala, incluyendo malversación, fraude financiero y económico, lavado de dinero, en formas que serán menos visibles en relación con el número de incidentes.

Diversas actividades que antes se hacían en el mundo real se encuentran ahora en el mundo virtual, incluida la explotación sexual, la prostitución, el juego, el lavado de dinero, las ventas ilegales, y la falsificación, todo se hace a través de Internet.

Esto también incluye información falsa con el propósito de desestabilizar las empresas o países que interfieren en las actividades de estos grupos.

### 3.4 Vulnerabilidades

*"Una vulnerabilidad es una debilidad de un activo o de un control que puede ser aprovechada por una amenaza. En el contexto de un sistema de información, ISO/IEC TR 19791:2006 también define la vulnerabilidad como un fallo, debilidad o propiedad del diseño o la implementación de un sistema de información (incluidos los controles de seguridad) o de su entorno que podría ser explotada intencionalmente o no para afectar adversamente los activos u operaciones de una organización."*

El análisis y evaluación de vulnerabilidades debe ser una tarea constante. Cuando un sistema recibe un parche, una actualización o se le añaden nuevos elementos, podría añadirse una nueva vulnerabilidad.

Debe mantenerse un inventario de las vulnerabilidades conocidas con el protocolo de acceso más estricto y preferiblemente separado, física y lógicamente, del activo o el control al que es aplicable.

En el caso de que se produzca un acceso no autorizado y el inventario de vulnerabilidades se vea comprometido, el inventario de vulnerabilidad sería una de las herramientas más eficaces en el arsenal de un agente de amenaza a la hora de perpetrar un ataque.

### 3.5 Mecanismos de Ataque

Muchos de los ataques en el ciberespacio se llevan a cabo utilizando malware, como spyware, gusanos y virus.

Se recopila información a menudo a través de técnicas de phishing.

Un ataque puede ocurrir como un vector de ataque único o llevarse a cabo como un mecanismo de ataque mezclado.

Estos ataques se pueden propagar a través de, por ejemplo, sitios web sospechosos, descargas sin verificar, correos electrónicos de spam, explotación remota o medios extraíbles infectados.

Los ataques pueden provenir de dos categorías principales:

- Ataques desde dentro de la red privada
- Ataques de fuera de la red privada.

Hay casos, sin embargo, en que los ataques son una combinación de ambos.

Otros mecanismos que están creciendo en uso y sofisticación, para llevar a cabo ataques, son los basados en sitios web de redes sociales y el uso de archivos dañados en sitios web legítimos.

Las personas tienden a confiar implícitamente en **mensajes y contenidos recibidos de contactos previamente aceptados** en sus perfiles en las redes sociales.

Una vez que un atacante, a través de robo de identidad, se puede ocultar como un contacto legítimo, el atacante puede comprometer a otros, y esto abre nueva vía para el lanzamiento de los distintos tipos de ataques previamente discutidos.

Los sitios web legítimos también pueden ser hackeados e infectar algunos de sus archivos para usarlos como un medio para perpetrar ataques.

Las personas tienden a confiar en sitios web comúnmente visitados, y aún más los que utilizan mecanismos de seguridad tales como **SSL (Secure Sockets Layer)**.

Mientras que la autenticación de las partes y la integridad de la información transmitida o recibida siguen vigentes, SSL no hace diferencia entre el contenido original y el nuevo contenido dañado, plantado por un atacante, lo que expone a los usuarios de ese sitio web a los ataques.

Algunos ejemplos de ataques desde la red privada son:

- Un administrador puede abusar de los privilegios que tiene para iniciar un ataque u obtener información privilegiada.
- Usar un punto de acceso falso para robar credenciales.
- Malware que envía paquetes de escaneo para localizar otros ordenadores vulnerables en la red.
- Malware que usa el modo promiscuo de la tarjeta de red para capturar información que pasa por la red interna.
- Keyloggers.

Algunos ejemplos de ataques desde fuera de la red son:

- Escaneo de los puertos de un servidor en Internet.
- Usar una botnet para lanzar un ataque DoS a gran escala.
- Buffer overflow para comprometer un servidor público.