DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ataques a la seguridad informática

CURSOS EN LÍNEA

Ataques a la seguridad informática

La evolución en las redes de telecomunicaciones y el desarrollo de dispositivos electrónicos con altas capacidades de procesamiento han significado una revolución en la forma en la que las personas y organizaciones crean, comparten, almacenan y utilizan la información.

Es justamente la creación de sistemas complejos de información lo que permite el desarrollo de los diversos procesos productivos de una organización. Por lo tanto, la información se considera su principal activo ya que es la fuente de conocimiento que orienta la toma de decisiones y permite a las empresas ser competitivas.

Por otro lado, a nivel personal también se ha presentado una transformación en la forma en la que nos relacionamos. Los dispositivos informáticos nos permiten entrar en contacto con otras personas y se han convertido en la principal forma de interacción de nuestro tiempo. En este contexto, el tratamiento de la información se vuelve aún más complejo, dado que es posible que se cuente con información sensible relacionada con la esfera más íntima de las personas.

Así, tanto en el ámbito organizacional como en el personal, se vuelve necesaria la comprensión de los riesgos y amenazas que pudieran comprometer la seguridad de la información. De esta manera, se puede reconocer la necesidad de establecer mecanismos para su protección. A continuación, se exponen de manera general los conceptos fundamentales que ayudarán a una mejor comprensión de la seguridad de la información y los ataques informáticos en el contexto de los sistemas digitales de procesamiento de datos.

Seguridad de la información vs seguridad informática

Para comenzar, será necesario establecer la diferencia entre la seguridad de la información y la seguridad informática. La seguridad informática es solo una parte de la seguridad de la información que se limita a la seguridad de los equipos informáticos. Es importante tomar en consideración esta diferencia, pues muchos autores manejan los términos de manera intercambiable y resulta conveniente su contextualización para definir su importancia y relación.

Figura 1. Relación Seguridad de la información y seguridad informática.

Seguridad de la información

La **seguridad de la información** representa todas aquellas medidas de protección que se establecen para asegurar la confidencialidad, la integridad y la disponibilidad de la información. En esta definición conviene aclarar cada uno de estos conceptos pues se trata de las propiedades deseables de la información en un contexto de seguridad.

La confidencialidad, integridad y disponibilidad son conocidos en su conjunto como la tríada de la seguridad de la información y representan uno de los principios fundamentales para el establecimiento de medidas de protección.

Confidencialidad. Se puede entender a la confidencialidad como aquella "propiedad de acuerdo a la cual la información no debe ser divulgada, revelada, o que se encuentre disponible para individuos, entidades o procesos no autorizados"[1]. Por lo tanto, esta propiedad hace referencia a que la información, idealmente, solo podrá ser consultada por individuos, entidades o procesos autorizados. Es decir, la información deberá permanecer inaccesible para cualquier persona o entidad ajena que no tenga derechos sobre ella. Así, el objetivo de la confidencialidad en la seguridad de la información puede entenderse como el esfuerzo que se realiza para mantener la información privada y accesible solo a las personas a las que se ha concedido este privilegio.

Figura 2. Tríada Confidencialidad, Integridad y Disponibilidad.

Integridad. Es la "propiedad de exactitud y completitud de la información"[2]. Puede considerarse como la propiedad deseable de la información por la que el almacenamiento, uso y mantenimiento de la misma sea implementado, de manera tal, que se asegure que la información se presenta completa, correcta, de manera consistente y utilizable para un propósito determinado. Es decir, esta cualidad de la información se alcanza cuando se establecen mecanismos de seguridad para lograr que no puedan hacerse modificaciones (intencionales o accidentales) a la información por parte de usuarios no autorizados. Así que podemos comprender la cualidad de integridad como el aseguramiento de que la información y datos que se presentan a los usuarios no han sido modificados y que, mientras se encuentra almacenada o en tránsito, ésta permanecerá inalterada.

[1] ISO. (2022). ISO27000: "Sistemas de Gestión de Seguridad de la Información".
[2] Ibídem.

Disponibilidad. Podemos entenderla como la "propiedad de la información que la hace permanecer accesible y utilizable de acuerdo a la solicitud de una entidad autorizada"[3]. En este sentido, con esta cualidad se busca el aseguramiento y confiabilidad en el acceso y uso de la información de manera oportuna por parte de usuarios autorizados. Por lo tanto, la disponibilidad es la propiedad de la información que se obtiene cuando esta se mantiene disponible, completa y utilizable en el momento preciso en que un usuario autorizado la necesite.

La definición de estos conceptos resulta vital para el entendimiento de los objetivos de la seguridad de la información y comprenden de manera global los esfuerzos que se realizan para su preservación.

Seguridad informática

Por otra parte, la **seguridad informática** puede comprenderse como todas aquellas medidas que se establecen para la protección de los sistemas informáticos. En este punto conviene analizar sus partes y establecer la definición de Informática y sistemas informáticos para poder comprender las medidas de seguridad que pudiera llegar a implementarse para su protección.

La **Informática** "es un conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras; reúne diversos aspectos teóricos y prácticos de la ingeniería, teoría de la información, lógica, electrónica, matemáticas y su campo abarca desde la programación y arquitectura informática hasta la inteligencia artificial, la robótica e inclusive el comportamiento humano."[4]

Figura 3. La Informática abarca una amplia gama de conocimientos y técnicas que permiten el tratamiento de la información.

Como se ha mencionado, la evolución de distintas tecnologías ha permitido la creación de sistemas informáticos complejos que facilitan el procesamiento y comunicación de información. La adopción de estos sistemas, en un nivel empresarial, permite a las organizaciones ser competitivas, mientras que, a nivel personal, han facilitado la interacción y compartición de información.

Los sistemas informáticos influyen tanto en las organizaciones como en la vida privada de las personas. Así que, dada su importancia, se vuelve necesario su análisis. Un **sistema** consiste en

[3] Óp. cit. ISO. (2022).
[4] FCA, UNAM. (2016). Informática I. Apuntes Digitales.

un conjunto de elementos interrelacionados entre sí con el objetivo de realizar una tarea específica. Los elementos, sus funciones y la forma en que interactúan entre sí determinarán la articulación del sistema y por ende sus resultados.

Así, podemos entender a los **sistemas informáticos** como el conjunto de elementos físicos y lógicos (personas, dispositivos electrónicos, hardware, software, datos, redes de comunicación, procesos, etc.) que participan en la captura, procesamiento, almacenamiento y transmisión de la información.

Es muy importante asimilar cada una de las partes que incluyen los sistemas informáticos (incluidas las personas) porque es necesario tomar medidas de protección que garanticen o mejoren la seguridad de cada uno de estos elementos.

Hasta este punto se han mencionado una serie de conceptos fundamentales que permitirán la comprensión general de todo aquello que engloba la seguridad de la información y la diferencia que existe entre ésta y la seguridad informática. Recuerde, la idea principal es que la seguridad informática es solo una parte de la seguridad de la información.

Por otro lado, para tomar medidas de seguridad informática es importante considerar los elementos que componen a un sistema informático, que, como hemos estudiado, puede llegar a comprender desde las personas, programas, dispositivos, procesos, hasta la infraestructura de red de comunicación que permite su interacción.

Además, será preciso recordar la triada de la seguridad de la información que representan los objetivos principales para su protección.

¿Por qué es necesaria la seguridad de la información?

A nivel empresarial, la información puede ser considerada como un activo estratégico, pues permite a las organizaciones obtener una ventaja competitiva, obtener diferentes perspectivas de su contexto, así como mejorar la toma de decisiones e impulsar innovaciones. Por lo tanto, al proteger la seguridad de la información se está protegiendo la competitividad de la organización. A su vez, en un nivel personal, la información que generamos y almacenamos forma parte de nuestra intimidad que, en algunos casos, pudiera llegar a comprometer nuestra integridad si ésta llegará a ser revelada. Así, en ambos escenarios, la seguridad de la información es necesaria para la preservación, subsistencia y plenitud de nuestra libertad y derechos.

Sin embargo, y a medida que el mundo digital ha crecido, también han surgido diferentes tipos de amenazas que pueden llegar a poner en riesgo la información tanto a nivel organizacional como a nivel personal. Tal es el caso de los ataques informáticos que han aumentado de manera exponencial en los últimos años, por lo tanto, resulta fundamental la implementación de medidas de seguridad en los activos de información, pues de lo contrario, se puede ser una víctima de robo, filtración, pérdida o daño de la información.

Pero, además, los sistemas informáticos no son perfectos y presentan una serie de vulnerabilidades que pueden ser aprovechadas por personas maliciosas que cuenten con los conocimientos técnicos necesarios para sobrepasar sus controles de seguridad y configuraciones predeterminadas. Por lo tanto, la información de los sistemas informáticos se encuentra en un riesgo latente que resulta necesario mitigar en lo posible (no existe sistema cien por ciento seguro) con controles de seguridad preventivos, detectivos y correctivos acordes a su contexto específico.

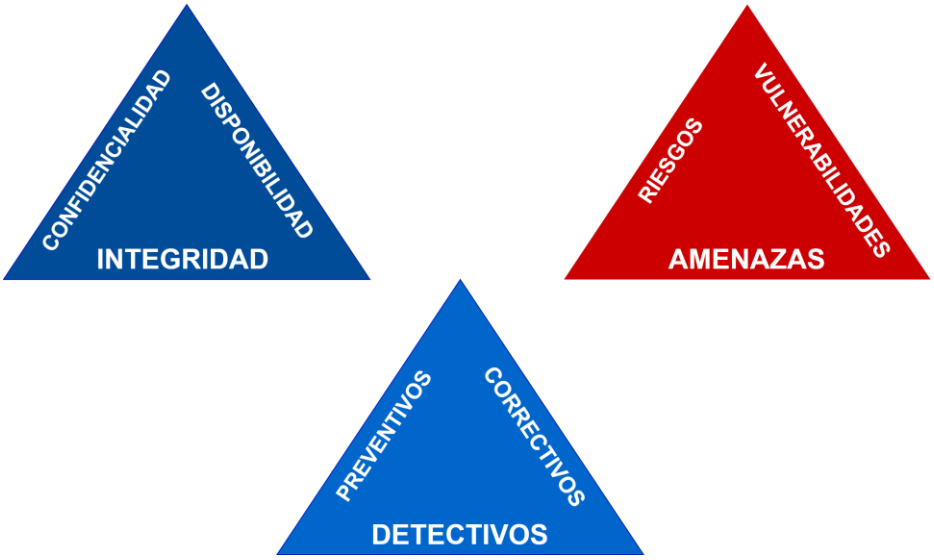

Figura 4. Los objetivos de seguridad se logran por medio del establecimiento de controles que permitan llevar los riesgos, vulnerabilidades y amenazas a niveles aceptables.

En los siguientes apartados estudiaremos los conceptos generales de los ataques informáticos que permitirán identificar sus características y permitirán hacer consciencia sobre los riesgos y amenazas a los que nos enfrentamos.

Definición y características de ataque a la seguridad informática

Como se ha mencionado, la información en la era digital es el activo más valioso, tanto para las organizaciones como para las personas, así que los sistemas informáticos encargados de su procesamiento y comunicación se vuelven el principal blanco de un ataque.

> Un activo es todo aquel elemento que resulta valioso, tanto en el ámbito organizacional como en el personal, para el procesamiento, almacenamiento y comunicación de la información. Por ejemplo, un equipo de cómputo, dispositivos móviles, infraestructura de red, entre otros.

Un **ataque informático** es toda acción que atenta contra la confidencialidad, integridad y disponibilidad de la información. La norma ISO 27000 define a los ataques como "cualquier intento de destruir, exponer, alterar, inhabilitar, robar o ganar acceso no autorizado sobre un activo"[5]. Por lo tanto, se puede considerar un ataque como todo esfuerzo por superar los controles de seguridad de un sistema informático.

[5] Óp. cit. ISO. (2022).

Amenazas informáticas

Una amenaza en el contexto de la seguridad informática es toda aquella entidad con motivos, recursos y capacidad para afectar los sistemas informáticos. Las amenazas pueden manifestarse en muchas formas, de hecho, existen autores que consideran también los desastres naturales y otros siniestros como posibles amenazas, sin embargo, con el fin de limitar y representar a las amenazas informáticas, nos concentraremos en aquellas personificadas por agentes maliciosos como pueden ser:

- Hackers. Un hacker es una persona que cuenta con las habilidades técnicas para ganar o forzar acceso no autorizado a sistemas informáticos. A pesar de que el nombre tiene una connotación negativa, existen diferentes tipos de hackers:
  - Sombrero negro. Son hackers malintencionados que no cuentan con la autorización para realizar sus actividades. Cuando se habla de un hacker como una amenaza estamos considerando a este tipo de hacker que es aquel que aprovecha sus conocimientos para acceder de manera no autorizada a sistemas informáticos para realizar acciones maliciosas por satisfacción o para obtener un beneficio personal.
  - Sombrero blanco. Son considerados hackers éticos pues dedican sus esfuerzos a la identificación de vulnerabilidades en los sistemas para mejorar su protección. Realizan sus actividades en los sistemas informáticos con la autorización de sus propietarios.
  - Sombrero gris. Esta clasificación de hacker se encuentra justo en medio de las dos anteriores, son un tipo de hacker que se considera tienen buenas intenciones, pero que sus actividades o motivaciones pueden llevarlos a realizar acciones más allá de lo éticamente correcto.
- Hacktivista. Un hacktivista es un hacker que, usualmente, sigue ideales políticos o son guiados por un sentimiento de injusticia social. Existen muchos grupos que realizan actividades en manifestación de ideales y es común que se formen grupos identificados como es el caso del grupo Anonymous o el grupo Guacamaya que recientemente llegó a hackear a la SEDENA en nuestro país.
- *Script kiddies*. Se llama así a las personas que no cuentan con las habilidades técnicas suficientes para ser considerados hackers. Estas personas utilizan herramientas de ataque preconfiguradas. Su falta de competencia permite que se identifiquen rápidamente y, usualmente, sus técnicas son fáciles de prevenir, sin embargo, incluso las personas menos habilidosas pueden llevar a provocar grandes desastres.
- Amenazas internas. Este tipo de amenaza es llamada así porque forma parte de la misma organización. Son personas que cuentan con acceso físico a las instalaciones e, incluso, con cuentas y contraseñas que les dan acceso directo a los sistemas de información. Este tipo de actores están motivados por diversos factores tales como venganza, envidia, o incluso, por simple desconocimiento que puede llevarlos a afectar sin intención los sistemas de información. Apuesto a que usted conoce a alguien con estas características.
- Competidores. Se considera a un competidor a cualquier otra organización con la que se tiene una disputa comercial o económica. La motivación de los competidores es ganar información que le ponga en ventaja ante otra. Sin embargo, es posible que se sobrepase los niveles de lo legalmente permitido para convertirse en una amenaza a la seguridad de los sistemas de información.

- Sindicatos criminales. Esta amenaza está compuesta por grupos de personas dedicadas a actividades ilícitas. Son organizaciones altamente especializadas en actividades ilegales para obtener un beneficio económico. Por ejemplo, existen grupos especializados en el secuestro de información digital por la que solicitan un rescate para su liberación.

Características de un ataque

Existen dos modalidades principales en la que los ataques se desarrollan:

- De manera pasiva. Se basan en la escucha y monitoreo de datos. Este tipo de ataques son complicados de descubrir pues el usuario, muchas veces, no puede observar un cambio sustancial en el comportamiento de los sistemas. Este ataque está orientado al conocimiento y uso de la información del sistema para aprender su configuración, arquitectura y operación, así como a la intercepción de los mensajes que emite y recibe sin afectar sus recursos por lo que en muchas ocasiones puede ser el precursor de un ataque activo.
- De manera activa. Esta forma de ataque implica la alteración de la información y de los servicios de un sistema. Están planeados para afectar las operaciones normales del sistema por medio de la destrucción, inhabilitación o modificación de sus elementos.

Por otro lado, es posible realizar una clasificación de ataques con base en su forma de ejecución:

- Ataques indirectos.
- Los ataques directos.

A continuación, estudiaremos cada uno de estos.

Ataques indirectos

Los ataques indirectos intentan llegar a tantos sistemas como sea posible. Típicamente, se realizan a través de internet por medios como el correo electrónico y sitios web especialmente creados para el ataque. El malware (software malicioso como virus, gusanos y troyanos) es un ejemplo de ataque indirecto automatizado.

Analicemos el proceso que conlleva un ataque indirecto:

- El atacante prepara los artefactos necesarios para realizar el ataque indirecto. Como se ha mencionado, puede ser la fabricación de malware con características especiales, o bien, la creación de un sitio web en donde se ejecute código malicioso.
- El atacante distribuye los artefactos por el medio o medios elegidos. Por ejemplo, por medio de correo electrónico automatizado o por la creación de mensajes que contengan enlaces al sitio web malicioso.
- Cuando los artefactos se ejecutan en un sistema víctima, comienzan a realizar las acciones para las que han sido diseñados. Estas acciones pueden ser muy variadas, pero, típicamente, implican el análisis de vulnerabilidades del sistema, la destrucción, exfiltración o modificación de información, entre otros. También es posible que el código malicioso realice una llamada o conexión con el centro de control del atacante para informarle que se ha logrado comprometer el sistema. En este momento el atacante toma control y puede realizar diferentes acciones.

Ataques directos

Los ataques directos están orientados hacia un objetivo en particular. Esto puede ser una organización, sistema o persona en la que el atacante tenga algún interés específico. Este tipo de ataque es muy peligroso pues está orientado a la afectación concreta del objetivo. Para el análisis de este tipo de ataques existen muchos marcos de trabajo que permitirán comprender su funcionamiento y características. Entre ellos se puede mencionar el marco de trabajo *Cyber Kill Chain*.

Un marco de trabajo es un conjunto estandarizado de conceptos, prácticas y criterios.

Cyber Kill Chain

El marco de trabajo *Cyber Kill Chain* está basado en conceptos militares, sin embargo, se ha adoptado para la identificación, prevención y contención de ataques informáticos. Este marco permite descomponer un ataque informático en fases para comprender las acciones que realiza un atacante durante un ataque. Estas fases son:

- Reconocimiento. En esta fase el atacante intenta recopilar la mayor cantidad de información posible sobre la víctima (persona u organización). Existen diferentes técnicas que podría llegar a utilizar tal como la compilación de información de fuentes abiertas como la que aparece en los buscadores y sitios web, redes sociales, entre otros, con el objetivo de adquirir la mayor cantidad de información posible y definir posibles vulnerabilidades.
- Preparación. Esta fase trata sobre la preparación del ataque. Con la información recabada el atacante puede elaborar algún artefacto (código malicioso, script o herramienta determinada) o planear una técnica específicamente diseñada para la víctima o vulnerabilidades encontradas.
- Entrega. En esta fase se lleva a cabo el ataque realizando la entrega del artefacto o técnica diseñado por el medio elegido. Por ejemplo, una memoria USB con código malicioso que se coloca en un sistema, o bien, el envío de un correo electrónico con un archivo adjunto malicioso (las posibilidades dependerán del tipo de víctima que se está atacando).

Figura 5. Fases del marco de trabajo Cyber Kill Chain.

- Aprovechamiento. En la fase de aprovechamiento, el artefacto explota las vulnerabilidades del sistema. Por ejemplo, código que se instala en el sistema y lo modifica para su conveniencia.
- Instalación. En esta etapa, el atacante buscará la persistencia en el sistema por medio de la instalación de software especializado que le permita el reingreso al sistema. De nueva cuenta, las posibilidades son muy variadas, en esta fase se puede realizar la descarga de programas adicionales que le permitirán al atacante el acceso y comunicación en tiempo real para la siguiente fase.
- Comando y control. Esta fase implica el establecimiento de comunicación entre el sistema de la víctima y el del atacante. El atacante puede ejecutar comandos y controlar el sistema de manera remota, incluso sin que la víctima pueda observar ninguna actividad relevante.
- Acciones sobre objetivos. En la fase final el atacante realiza las acciones y consigue los objetivos por los que ha comenzado el ataque. Típicamente, la exfiltración, destrucción o secuestro de la información del sistema.

Aceptar la existencia de distintos riesgos y amenazas que aprovechan las vulnerabilidades de los sistemas informáticos nos permitirá adoptar una mejor postura de prevención y seguridad. Además, comprender las características y fases generalizadas de un ataque ayudará a la comprensión e identificación de posibles indicadores de estos en nuestros sistemas.

AUTOR

ELIER EMANUEL LÓPEZ BASILIO