Módulo 1. Introducción ciberseguridad (CIA)

Introducción

Introducción

"La ciberseguridad es la práctica de proteger a las personas, los sistemas y los datos de los ciberataques mediante el uso de diversas tecnologías, procesos y políticas.

A nivel empresarial, la ciberseguridad es clave para la estrategia general de gestión de riesgos y, en concreto, para la gestión de ciberriesgos. Las amenazas comunes a la ciberseguridad incluyen el *ransomware* y otros *malware*, las estafas de *phishing*, el robo de datos y, más recientemente, los ataques impulsados por inteligencia artificial (IA)". (Jonker et al., s.f., https://n9.cl/mbcr4p)

Los sistemas informáticos se protegen mediante un conjunto de prácticas, tecnologías y procesos para redes y datos, accesos no autorizados y daños, salvaguardando información personal, financiera y operativa de individuos y organizaciones. Estos sistemas son cruciales para la confianza y el cumplimiento normativo en el mundo digital actual, involucrando a personas, procesos y tecnología.

Componentes clave

- **Protección de datos:** Salvaguardar información confidencial (personal, financiera).
- **Protección de sistemas y redes:** Asegurar *hardware*, *software* y la infraestructura de la

tecnología de la información (TI).

- **Prevención de ataques:** Usar herramientas y procesos contra *malware*, *phishing*, etc..
- **Respuesta a incidentes:** Manejar y recuperarse de brechas de seguridad.
- **Concienciación:** Educar a usuarios para evitar errores humanos, una vulnerabilidad clave.

Por qué es importante

- **Protege activos:** Evita pérdidas financieras y de datos.
- **Mantiene la confianza:** Asegura la confianza del cliente y el cumplimiento de regulaciones.
- **Sostiene operaciones:** Previene interrupciones en servicios críticos.
- **Fomenta la seguridad general:** Crea un entorno digital seguro para todos.

Amenazas comunes

- ***Malware*:** *Software* malicioso (virus, *ransomware).*
- ***Phishing*:** Engaños para obtener información sensible.

- ***Ransomware*:** Secuestro de datos.
- **Robo de identidad/datos:** Acceso no autorizado a información personal.
- **Ataques DoS/DDoS:** Inundar sistemas para hacerlos inaccesible.

El triángulo CIA

Es un modelo que representa los tres principios clave para proteger la información. Si uno falla, la seguridad se ve comprometida. Los tres principios son:

- Confidencialidad: garantizar que la información solo sea accesible para **personas autorizadas.**
- Integridad: asegurar que la información **no sea alterada** de forma no autorizada, manteniéndose exacta y confiable.
- Disponibilidad: garantizar que la información y los sistemas estén **accesibles cuando se necesiten**, por usuarios autorizados.

CONTINUAR

1. Seguridad de la información o ciberseguridad

1. Seguridad de la información o ciberseguridad

Si bien las definiciones de seguridad informática o seguridad de la información (Romero Castro et al., 2018) varían según sus autores, aquí se unificarán en un solo término: **ciberseguridad**. La ciberseguridad es un área transversal en la industria 4.0, IoT (Internet de las cosas), inteligencia artificial, realidad virtual, realidad aumentada, *big data*, etc.

Existen cuatro acciones que involucran a todas las áreas de seguridad, y son:

- Prevención del riesgo (en ciberseguridad serían las acciones y medidas proactivas).
- Transferir el riesgo.
- Mitigar el riesgo (en *ciberseguridad* serían las acciones y medidas reactivas).
- Aceptar el riesgo.

A las empresas con presencia en el ciberespacio, se les recomienda tener ciertos niveles de ciberseguridad sobre algunos actores, a saber:

- **Los usuarios**: Kaspersky (Pankov, 2020) publicó un informe titulado *El impacto del coronavirus en la seguridad corporativa* en el que visibiliza que el usuario es el eslabón más débil de la cadena:

    1. El 73 % de los empleados reconocen no haber recibido preparación en ciberseguridad.
    2. 42 % de estos utilizan medios propios para proteger sus equipos.
    3. Solo un 53 % de los colaboradores utiliza una VPN al trabajar desde casa.

- **La información**: es uno de los principales activos a proteger.

- **La infraestructura**: debe poder controlarse toda acción que debilite el funcionamiento de una la empresa, organización o estado. Esta necesidad quedó demostrada en los distintos ciberataques que padeció la industria energética de Ucrania y documentada por distintos medios de prensa e informes.

En otras palabras, independientemente de la infraestructura tecnológica que se utilice, esta debe mantener una sólida protección de los pilares de la información mencionados anteriormente (**confidencialidad**, **integridad** y **disponibilidad)**.

Las organizaciones, Estados, empresas, individuos, etc. deben analizar sus riesgos y dotar de las previsiones necesarias en ciberseguridad para que, cualquiera sea el incidente que pudiera alcanzar, no les afecte más allá de su perímetro o entorno.

Dado que la criminalidad y delincuencia se han trasladado al quinto dominio, es necesario trabajar con estándares de ciberseguridad que sirvan como pilares que ayuden a amortiguar los ciberataques. Los ataques, podrían afectar sensiblemente a una nación en forma directa o por medio de terceros (empresas, personas, etc.).

Los estándares de ciberseguridad se encuadran en *frameworks* de trabajo que sugieren medidas preventivas y reactivas. En estos marcos, se destaca el análisis de riesgos que utiliza los conceptos de **activos y vulnerabilidad** (Gobierno de España, 2012).

Existen distintas herramientas automatizadas y metodologías para el análisis de riesgo. A continuación se mencionan algunas:

- **NIST SP 800-30**: "Este método nació en el Instituto Nacional de Estándares y Tecnología. Fue fundado para evaluar los riesgos de seguridad de la información, especialmente en sistemas TI (Tecnología de la Información), con el objetivo de apoyar a las organizaciones con todo lo relacionado a tecnología". (PMG, 2021, https://n9.cl/s63v2).

- **ISO/IEC 31000**: "BS ISO 31000 es la norma internacional para la gestión del riesgo. Al proporcionar principios integrales y directivas, esta norma ayuda a las organizaciones con su análisis y evaluación de riesgos" (Omega Corp, s.f., https://n9.cl/9d80v).

- **ISACA COBIT:** Control Objectives for Information and Related Technologies.

- **ENS MAGERIT:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Norma Española.

- **SEI OCTAVE:** Operationally Critical Threat, Asset and Vulnerability Evaluation.

Infraestructura crítica

Se entiende como infraestructura crítica aquellas tecnologías, instalaciones, servicios, redes, información y equipos físicos esenciales para las funciones sociales vitales como la salud, la seguridad, el bienestar social y la economía de los ciudadanos de un país. Los Gobiernos y las empresas tienen la obligación de implementar medidas que disminuyan cualquier tipo de riesgo en estas infraestructuras, ya que su perturbación o destrucción afectaría gravemente diferentes ámbitos, como el económico, el detrimento de la confianza como nación y algo más grave que pudiera ser la pérdida de vidas. La infraestructura crítica puede ser propiedad de particulares o del Estado.

OEA

La Organización de Estados Americanos (OEA) publicó un documento que pone en relieve la importancia del cuidado de las infraestructuras críticas. Invitamos a leerlo en el siguiente enlace: https://n9.cl/tn8ew.

En 2013, el presidente de EE.UU. (Barack Obama) emite un comunicado que expresa: “Dado un aumento sostenido de la cantidad de incidentes de ciberseguridad en los EEUU, el presidente Barack Obama, el 12 de febrero de 2013, emite la orden ejecutiva 13636, en donde se encarga al Instituto de Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) el desarrollo del Marco de ciberseguridad para la protección de infraestructuras críticas, lo que hoy se conoce como el Cybersecurity Framework (CSF). EEUU identifica 16 sectores de infraestructuras críticas; estos son: químico; instalaciones comerciales; comunicaciones; fabricación crítica; presas/represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; comida y agricultura; instalaciones gubernamentales; salud y salud pública; tecnología de información; reactores nucleares, materiales y residuos; sistemas de transporte; sistemas de agua y aguas residuales.

. . .

El Marco tomó como estrategia basarse en estándares de la industria ya aceptados por el ecosistema de ciberseguridad (NIST SP 800-53 Rev.4, ISO/IEC 27001:2013, COBIT 5, CIS CSC, entre otros)". (Contreras, 2019, https://n9.cl/ocfrn)

El marco NIST fue, y sigue siendo, desarrollado y promovido a través del compromiso continuo y con el aporte de las partes interesadas, tanto actores del gobierno, como de la industria y el ámbito académico. En 2018, su actualización a la versión 1.1 dio lugar a expertos e industria, así como a gobiernos y empresas no estadounidenses, por ejemplo Israel y la empresa Huawei Tech.

> "La OTAN ya había desarrollado una serie de manuales orientados hacia la protección de infraestructuras críticas para la defensa nacional, como es el caso del 'Manual del Marco de Trabajo de Ciberseguridad Nacional' (National Cyber Security Framework Manual). Esto no quiere decir que el CSF de NIST excluya estos documentos; al contrario, los complementa y mejora.

Empresas, academia y gobiernos han adoptado de manera voluntaria el CSF como parte de su estrategia de ciberseguridad. Incluso organizaciones líderes en la generación de normas y estándares han incorporado el CSF, como por ejemplo ISACA e ISO. En particular, ISO generó la ISO/IEC TR 27103:2018 que proporciona orientación sobre cómo aprovechar los estándares existentes en un marco de ciberseguridad, en otras palabras, cómo utilizar el CSF". (Contreras, 2019, https://n9.cl/ocfrn)

"La Directiva Europea 2008/114/CE (documento publicado por el Centro Criptológico Nacional de España) el 8 de diciembre de 2008 estableció por infraestructura crítica a:

El elemento, sistema o parte de este, situado en los Estados miembros, que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o

destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

A pesar de que las infraestructuras críticas son similares en todos los países, su práctica puede variar en función de las necesidades, recursos y nivel de desarrollo de cada país en particular". (LISA Institute, s.f., https://n9.cl/dvw2o)

Infraestructura crítica en Argentina

La normativa vinculada a la infraestructura crítica en Argentina se encuentra detallada en el sitio web de la Dirección Nacional de Ciberseguridad donde se exponen las leyes, resoluciones y decretos referidos a este tema. Para conocer las normativas vigentes en lo que respecta a la ciberseguridad en Argentina, entrar al siguiente *link*: https://n9.cl/hmzrh.

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos.
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de Aplicaciones Seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.

- Resolución 1523/2019. Definición de infraestructuras críticas.

Infraestructuras críticas en empresas

La infraestructura crítica de una empresa puede afectar gravemente a un organismo gubernamental. A continuación, se enumeran algunos ejemplos de repercusión mundial:

a) **SolarWinds:** El caso SolarWinds corresponde a un ataque informático a la cadena de suministro, en el que se explotó una vulnerabilidad conocida como Sunburst o Solorigate. Al comprometer el *software* Orion, utilizado por miles de empresas y organismos gubernamentales, los atacantes lograron infiltrarse de forma indirecta en múltiples instituciones públicas y privadas, incluyendo agencias federales y grandes corporaciones. Este incidente evidenció la magnitud del riesgo que supone la dependencia de proveedores tecnológicos ampliamente distribuidos. (Solarwinds, 2021)

b) **"FireEye** tiene 9600 clientes en 103 países del mundo . . . En el año 2014, Sony sufrió uno de los mayores ataques de seguridad de la historia (que el FBI atribuyó más tarde a Corea del Norte), FireEye fue la empresa contratada para poner remedio a la brecha de seguridad. Ofrece a las empresas herramientas para que puedan detectar si algún *hacker* los ataca con el *software* que le han robado. La marca tiene entre sus clientes al gobierno de Estados Unidos" (Bécares, 2020, https://n9.cl/f2non).

c) En 2020, durante la pandemia por covid-19, la Agencia Europea de Medicamentos, vacunas experimentales de Johnson & Johnson y Novavax, farmacéuticas surcoreanas Genexine, Shin Poong y Celltrion y la británica AstraZeneca (también conocida como vacuna de Oxford) han declarado haber sido víctimas de ciberataques (Biontech, 2020).

Confidencialidad, integridad y disponibilidad

“De acuerdo con el marco de gestión y de negocio global para el gobierno y la gestión de las TI (Tecnología Informática) de la empresa (COBIT, por sus siglas en inglés), las características que debe poseer la información son: efectividad, eficiencia, apego a los estándares, confiabilidad, confidencialidad, integridad, disponibilidad” (Baca Urbina, 2016, p. 12). Explicaremos y haremos hincapié en estos tres aspectos:

Confidencialidad

La confidencialidad consiste en asegurar que solo las personas autorizadas accedan a la información indicada; puede estar amparada por la legislación de protección de datos y, para garantizarla, se utilizan tres recursos:

1. **Autenticación de usuarios**: identificar que la persona que accede a la información es quien dice ser.
2. **Gestión de privilegios**: los usuarios que acceden a un sistema podrán operar solo con la información que se les autoriza y solo en la forma que se les autorice; por ejemplo, gestionando permisos de lectura o escritura en función del usuario.
3. **Cifrado de información**: denominado encriptación, evita que esta sea accesible a quien no está autorizado, aplicable tanto a la información que está siendo transmitida como a la almacenada.

- **Ejemplos:**
  - Contraseñas y autenticación.
  - Cifrado de datos (ej.: WhatsApp con cifrado de extremo a extremo).

- Control de acceso (ej.: permisos en carpetas compartidas).

- **¿Qué la amenaza?**

  - *Hackeos*, *phishing*, espionaje, robo de dispositivos.

Integridad

Consiste en asegurarse de que la información no se pierda ni se vea comprometida voluntaria e involuntariamente. Para garantizar la integridad de la información, se debe considerar lo siguiente

1. Monitorear el tráfico de red para descubrir posibles intrusiones.
2. Auditar los sistemas para implementar políticas de auditorías que registren quién hace qué, cuándo y con qué información.
3. Implementar sistemas de control de cambios, por ejemplo, comprobar los resúmenes de los archivos de información almacenados en el sistema para corroborar si cambian o no.
4. Como otro recurso, se deben tener las copias de seguridad para recuperar un estado anterior.

Disponibilidad

La información debe estar disponible para quien la necesita en todo momento; también se deben implementar las medidas necesarias para que tanto la información como los servicios estén disponibles.

- Ejemplos:
  - Copias de seguridad (backups).
  - Sistemas redundantes (por ejemplo, servidores espejo).
  - Protección contra ataques de Denegación de Servicio (DDoS).

Ciberseguridad en Argentina

NIC Argentina define la **ciberseguridad** como la rama de la informática que procura detectar vulnerabilidades que ponen en juego la integridad, disponibilidad y confidencialidad de los sistemas informáticos. Una de sus áreas es forense digital (*digital forensics*) que comprende funciones del peritaje informático, delitos informáticos, etc.

Principal objetivo

"La ciberseguridad tiene como objetivo principal ***resguardar la infraestructura y la información*** de los usuarios involucrados en ella. Se constituye como una esfera con distintos protagonistas: empresas que ofrecen servicios asociados, expertos y analistas que investigan nuevas soluciones, desarrolladores de nuevas herramientas (tanto a nivel *hardware* como *software*), y aquellos usuarios que utilizan diferentes medios preventivos. Es en este circuito que también actúan aquellos personajes que quieren interferir en estos sistemas, ya sea con fines delictivos, políticos o por el hecho de demostrar sus habilidades. Estos últimos, son conocidos coloquialmente como *hackers*, aunque esta denominación es muy discutida, ya que en realidad no refiere a cuestiones

ilícitas, sino que se vincula con la manera de denominar a aquellos expertos que detectan fallos y vulnerabilidades en los sistemas

Las amenazas más comunes son

. . .

- Virus informáticos [en la cátedra utilizaremos el concepto de *malware]*.
- *Phishing*
- Denegación de servicios (DoS).
- *Spoofing*
- *Ransomware*

. . .

Medidas preventivas:

- Antivirus.
- *Firewall* o cortafuegos.
- Encriptación de la información.
- Contraseñas o *passwords*". (NIC Argentina, 2018, https://n9.cl/u7w6h).

Varios acontecimientos mundiales hicieron tomar conciencia acerca de la importancia de la ***ciberdefensa***, algunos de estos sucesos serán los ejes centrales para debatir los

conceptos que se aprenderán en esta materia.

Ahora nos concentraremos en la lectura del siguiente relato: Edward Joseph Snowden (nacido en Elizabeth City, Carolina del Norte, el 21 de junio de 1983), era consultor tecnológico estadounidense y empleado de la Agencia Central de Inteligencia (CIA) y luego de la Agencia Nacional de Seguridad (NSA) de Estados Unidos.

En junio de 2013, los periódicos The Guardian y The Washington Post, hicieron públicos documentos de alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore que Snowden habría dado a conocer ¿Qué es lo que hacían estos programas? Los diarios internacionales de la época informaban sobre el espionaje masivo a ciudadanos de distintos países, incluyendo a presidentes. Algunos de los programas revelados fueron

- ***Programa PRISM***: Lanzado en 2007 por la NSA, permite "captar correos electrónicos, videos, fotografías, llamadas de voz e imagen, actividad en los medios sociales, contraseñas y otros datos de usuarios contenidos por las principales empresas de internet en EEUU siendo algunas de ellas: Microsoft y su división Skype, Google y su división YouTube, Yahoo, Facebook, AOL, Apple. Captación de datos telefónicos de millones de usuarios". (Cortés, 2013, https://n9.cl/eoowd).

- ***Programa TEMPORA***: Según el informe, la agencia británica de escuchas electrónicas (la Oficina Central de Comunicación del Gobierno o GCHQ, por sus siglas en inglés) "pinchaba" cables de fibra óptica que transportan comunicaciones globales y que las compartían con la NSA.

Siguiendo la línea periodística, el Pentágono concluyó que se filtraron 1.7 millones de documentos y la NSA realmente no sabe qué otra información robó Snowden y, más importante aún, ¿Cómo logró apoderarse de documentos altamente protegidos? Puesto que su cargo en la empresa no le daba acceso a tal información. Invitamos a leer la noticia completa:

BBC Mundo (31 de octubre de 2013). Cómo espía EE. UU., según Snowden. *BBC Mundo*. https://n9.cl/yehk0.

Cabe aclarar que, desde esta materia no tomamos posición ni damos opinión alguna de los casos que se mencionan; solo se presentan los hechos. De la lectura de la noticia de BBC Mundo pueden surgir algunas preguntas más, por ejemplo: ¿Por qué medio le fue posible a Snowden llevarse la información? ¿Utilizó papel, un pendrive, etc.? ¿Tuvo ayuda o actuó solo? Ante la importancia y magnitud de lo que se realizaba en la NSA, ¿qué pudo haber sucedido con los controles de acceso de entrada y salida al edificio, oficina, equipo, etc.? ¿No existían validaciones para sacar información de los servidores o dispositivos de trabajo? ¿No quedaron registros de las actividades realizadas por los usuarios en *logs*? Al contratar a Snowden, ¿se analizó su estado emocional o psíquico?, etc.

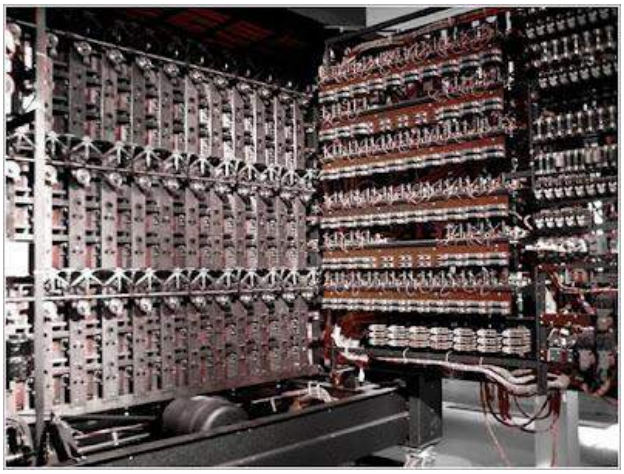
En el caso mencionado, es posible que hubieran intervenido peritos informáticos con distintas áreas del conocimiento en combinación con uno o varios equipos en criminalística y que todo lo actuado en el peritaje forense posiblemente haya seguido una línea de investigación fielmente apegada a la legislación norteamericana.

Primeros pasos de la computación moderna

Uno de los principales influyentes de la computación moderna e inteligencia artificial fue Alan Turing (1912 – 1954, matemático, criptógrafo, etc.) quien destacadamente puede haber sido una de las piezas fundamentales en la Segunda Guerra Mundial, ya que por medio de una computadora logró descifrar los mensajes (desencriptar) que eran enviados en formato papel por los nazis (Bejerano, 2014).

En la película *El código Enigma,* muestra que la computadora que decodificaba los mensajes (una máquina de gran tamaño), en alguna oportunidad dejaba de funcionar debido a la presencia de insectos (***bugs***). Este término se utiliza en la actualidad para describir fallos inesperados en la ejecución del programa o para indicar la presencia de un virus o *malware*.

Figura 1: Colossus, la máquina de Turing



Fuente: Ortiz, 2011, https://n9.cl/dq9fl.

A continuación, definimos algunos conceptos fundamentales.

Virus informático

"¿Qué es un virus informático? Esta idea se debatió por primera vez en una serie de conferencias presentadas por el matemático John von Neumann (1903 – 1957, Matemático húngaro-estadounidense, realizó contribuciones a ciencias de la computación, cibernética, etc.) a fines de la década del cuarenta en un informe publicado en 1966 llamado *Teoría del autómata autorreproductor*. De hecho, el informe fue un experimento de pensamiento en el que se especulaba sobre la posibilidad de que un organismo "mecánico" (como un código informático) causara daño en equipos,

se replicara e infectara nuevos equipos host, de la misma manera que un virus biológico". (Navarro Hidalgo, 2025, https://n9.cl/4uzls)

El primer virus informático se llamó Creeper (Bob Thomas, investigador de BNN Technologies, 1971), fue diseñado como una prueba de seguridad para comprobar si era posible crear un programa capaz de replicarse. Con cada disco duro nuevo infectado, Creeper trataba de eliminarse a sí mismo del equipo anfitrión anterior. Creeper no tenía una intención maliciosa y solo mostraba un mensaje simple: «*I'M THE CREEPER. CATCH ME IF YOU CAN*!» (Soy Creeper, ¡atrápame si puedes!). Siguiendo la línea de tiempo, el primer virus que se transmitió fuera de laboratorios de pruebas o entornos controlados fue el Elk Cloner para Apple**,** creado en 1981. Por otro lado, en 1986 surgía el primer virus para IBM Personal Computer, el BRAIN.

Malware

Avast describe las diferencias entre *malware*, antivirus y amenaza:

- Virus: "diseñado para copiarse a sí mismo y propagarse a otros dispositivos tanto como sea posible". (Avast, 2020, https://n9.cl/wnp92).
- *Malware* o código malicioso. Son ataques mediante la utilización de troyanos, son de precisión dirigidos a objetivos específicos (dispositivos, configuración o componente específico de la red).
- Amenazas: engloban el *malware* y también otros peligros en línea como el *phishing*, el robo de identidad, la inyección SQL y otros.

Figura 2: Virus, malware y amenaza

Fuente: Avast, 2020, https://n9.cl/wnp92.

Antivirus

"El honor de ser la primera persona en eliminar un virus de una computadora corresponde a Bernard Fix, que "limpió" el virus Vienna, aunque parece ser que lo hizo más con técnicas artesanales que con el *software* que creó para ello, y que solo hacía una parte del trabajo.

La corriente de opinión mayoritaria sobre quién creó el primer *software* antivirus tal y como lo conocemos hoy en día se podría decir que fue ***G Data***, una empresa alemana que creó una solución de este tipo para la plataforma Atari ST.

También en 1987/89, John McAfee fundaba en Estados Unidos la compañía que llevaría su apellido, lanzando a finales de año ***VirusScan***, su primer producto de este tipo, y coincidiendo en el año con los checoslovacos (el país todavía existía antes de escindirse en Eslovaquia y República Checa) de ***NOD***.

> Las principales empresas del sector de la seguridad informática que tenemos hoy en día surgieron en el periodo que abarca desde finales de la década de los ochenta y finales de la de los noventa: F-PROT en 1989, Panda Software (más tarde Panda Security) en 1990, Symantec/Norton en 1991, así como AVG, Bitdefender en

1996 y Kaspersky en 1997". (González, 2019, https://n9.cl/ri6be.

En la actualidad, existen varias marcas de antivirus que brindan soluciones para sus clientes y donde el uso de la inteligencia artificial permite la detección cambiante de los *malware* en sus vectores de ataque. Elegir qué antivirus es el que conviene a una organización no es una tarea sencilla como en décadas anteriores; ahora es necesario un análisis previo.

Vulnerabilidad

Una **vulnerabilidad informática** se puede definir como una debilidad en el *software* o en el *hardware* que permite a un atacante **comprometer** la **integridad, disponibilidad o confidencialidad** del sistema o de los datos que procesa." Por su parte, una **amenaza** es toda acción que aprovecha una vulnerabilidad. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización, pueden ser tanto **internas** como **externas"**. (INCIBE, 2017, https://n9.cl/leo8i)

El **riesgo** es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños.

Figura 3: Amenaza, vulnerabilidad, sistema de información y riesgo

Fuente: INCIBE, 2017, https://n9.cl/leo8i.

Algunas de las fuentes de amenazas más comunes en el ámbito de sistemas de información se producen por diversos ciberataques y son:

- "Ingeniería social: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.

- Amenazas persistentes avanzadas (*advanced persistent threats*): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.

- *Botnets*: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del *botnet* controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.

- Servicios en la nube: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad esté demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.

Algunos incidentes pueden implicar problemas legales que pueden suponer sanciones económicas y daños a la reputación e imagen de la empresa. Por eso, es importante conocer los riesgos, medirlos y evaluarlos para evitar en la medida de lo posible los incidentes, implantando las medidas de seguridad adecuadas". (INCIBE, 2017, https://n9.cl/leo8i).

INCIBE (2017) define fases que ayudan a identificar los activos críticos que pueden suponer un riesgo para la empresa, realizando el siguiente análisis de riesgos.

Figura 4: Fases

Fuente: INCIBE, 2017, https://n9.cl/leo8i.

“Este análisis nos servirá para averiguar la magnitud y la gravedad de las consecuencias del riesgo a la que está expuesta nuestra empresa y, de esta forma, gestionarlos adecuadamente. Para ello tendremos que definir un umbral que determine los riesgos asumibles de los que no lo son. En función de la relevancia de los riesgos, podremos optar por:

- Evitar el riesgo eliminando su causa, por ejemplo, cuando sea viable optar por no implementar una actividad o proceso que pudiera implicar un riesgo.
- Adoptar medidas que mitiguen el impacto o la probabilidad del riesgo a través de la implementación y monitorización de controles.
- Compartir o transferir el riesgo con terceros a través de seguros, contratos, etc.
- Aceptar la existencia del riesgo y monitorizarlo”. (INCIBE, 2017, https://n9.cl/leo8i)

Medidas de protección

Recordando que podemos ser el medio o transporte del aprovechamiento de vulnerabilidades o malware, se enunciarán algunos *tips* que hacen al cuidado de la infraestructura crítica:

1. Usar patrones, *pin*, huella dactilar, etc., en dispositivos móviles, PC, *notebook*, etc., verificando que quede bloqueada la pantalla a efectos que no se puedan ver las notificaciones que llegan.

2. No anotar en papel datos confidenciales de la empresa. Si fuese extremadamente inevitable, asegurarse de que la misma esté protegida en algún lugar.

3. Al iniciar sesión en alguna aplicación, es recomendable usar un gestor de contraseñas (algunos antivirus suelen traerlos o algunos de los servicios de Google para almacenar contraseñas).

4. Si inevitablemente debe enviar sus credenciales de acceso, asegúrese de hacerlo por medio de un sistema de encriptación robusta; nunca envíe datos comprometedores en formato plano.

5. No use la misma contraseña para todos los accesos que tenga.

6. Si usa un navegador web, asegúrese de que la URL sea segura, es decir, tenga la “s” final (***https***) esto indica que los datos viajan

encriptados hasta el destino. No obstante, esto no garantiza la seguridad.

7. No haga clic sobre ventanas emergentes que le indiquen que ha ganado algún premio como un teléfono móvil, viaje, suscripción de televisión, NetFlix, etc., sea precavido.

8. No utilice versiones gratuitas de antivirus.

9. Restrinja el uso de ingreso de información no autorizada al equipo, tales como *pendrive*, etc.

10. Todo ingreso de información a una organización (*e-mail*, mensajería, etc.) debe mínimamente ser escaneada por el antivirus de la empresa y organización.

11. Si usa información confidencial, la misma debe estar protegida mediante algún mecanismo de encriptación robusta.

12. Los correos electrónicos que usa deben tener sistema de encriptación (algunos son gratuitos).

13. Realice *backup* programados, verificando previamente que no tenga *malware* la información.

14. Si se conecta remotamente a su trabajo, usa redes públicas, etc., hágalo mediante una red privada virtual (VPN, *virtual private network*) esto evitará el ciberataque llamado "*man in the middle*".

15 Tome los recaudos necesarios para prevenir miradas curiosas sobre la pantalla de su equipo.

16 Use un destructor de papel para eliminar la información sensible que haya escrito.

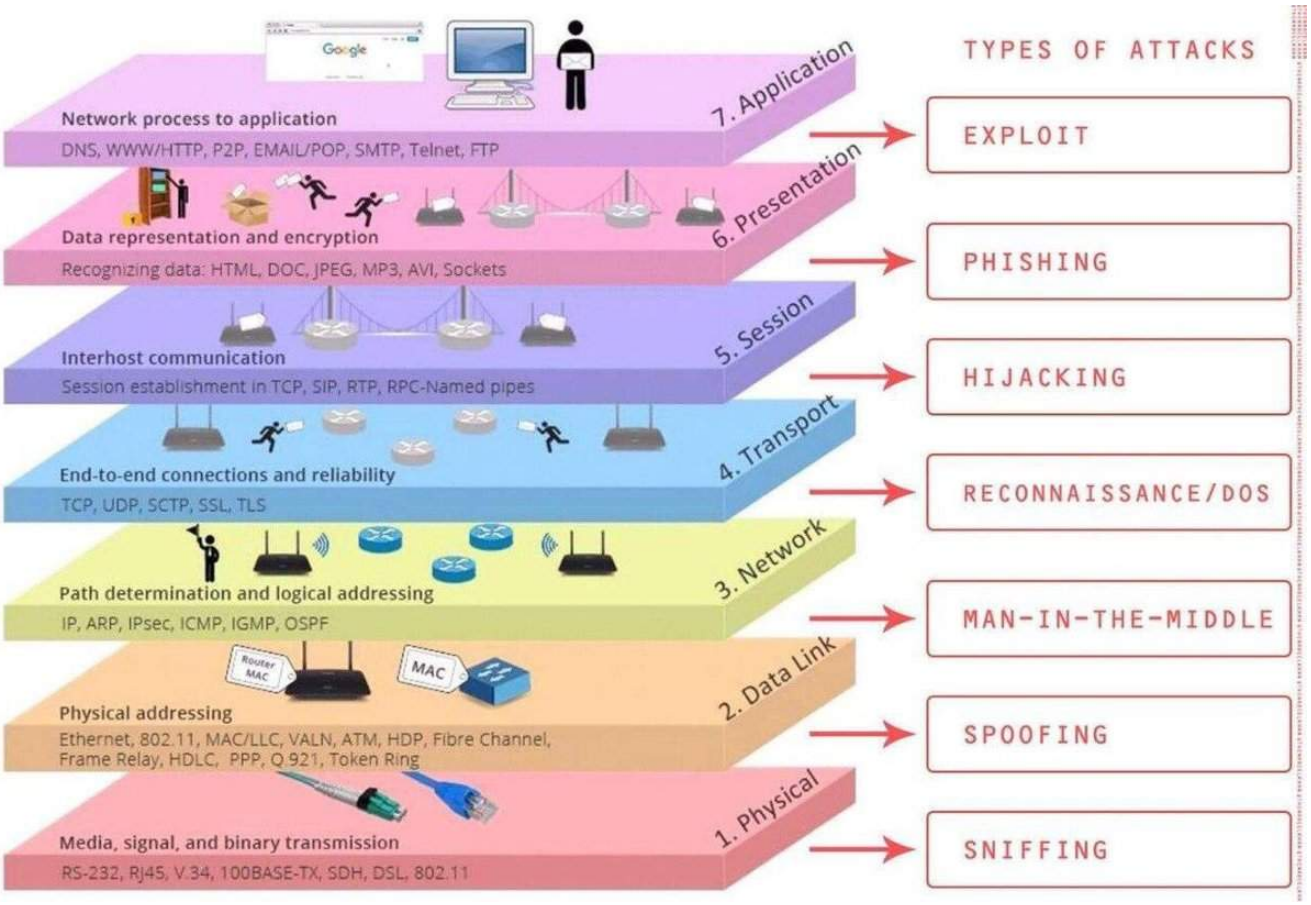
17 No hable fuera de la empresa temas concernientes a la tarea que se realiza dentro.

2. Tipos de ataques en el modelo OSI

2. Tipos de ataques en el modelo OSI

El modelo OSI presenta siete capas que demuestran los niveles que pueden ser afectados por algún tipo de *malware*.

Figura 5: Modelo OSI



Fuente: [imagen sin título sobre modelo OSI], s.f., https://n9.cl/rlil1.

Ciberataques

La creación de ciberataques organizados por los Estados marcó una irrupción en el tablero geopolítico y sentó las bases de un tipo de guerra diferente. Las nuevas armas se basan en la sofisticación tecnológica y en el ataque invisible y en muchos casos difíciles de detectar por los equipos forenses que tuvieron que adaptarse a las circunstancias.

Studnex es considerada la primera arma digital de la historia. "En enero de 2010, los inspectores de la Agencia Internacional de Energía Atómica que visitaban una planta nuclear en Natanz, Irán, notaron con desconcierto que las centrifugadoras usadas para enriquecer uranio estaban fallando. Curiosamente, los técnicos iraníes que reemplazaban las máquinas también parecían asombrados.

. . .

El 'gusano', ahora conocido como Stuxnet, tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse" (T13, 2015, https://n9.cl/19u38). Ciertos detalles técnicos del *malware* pueden leerse en el sitio de Panda Antivirus.

Flame: una nueva arma de ciberespionaje descubierta en Irán. Se trata de un malware altamente sofisticado que puede robar grandes cantidades de datos. Los detalles técnicos los puede encontrar en el sitio de f-secure. Uno de los módulos de Flame permite encender el micrófono de un equipo infectado para grabar conversaciones que ocurren alrededor del equipo, o a través de Skype. Las conversaciones son almacenadas y enviadas regularmente a los servidores de comando y control. También había un módulo que usaba tecnología Bluetooth para detectar otros equipos en las cercanías y robar nombres y números de los contactos.

Argentina: Desarrolla la primera ciberarma académica elaborada desde una tesis de maestría en Ingeniería del Software de la Universidad Nacional de San Luis y cuya

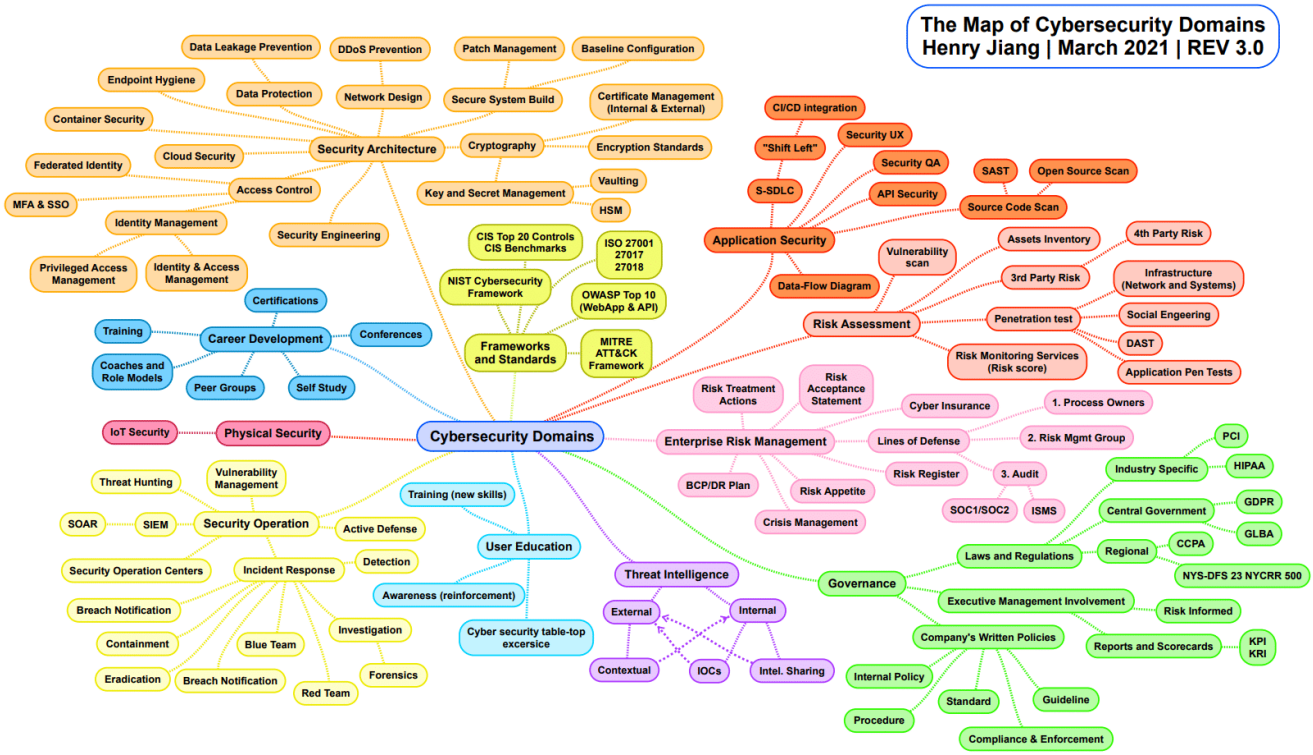
investigación se llevó a cabo en la Universidad Federal de Minas Gerais, Belo Horizonte, Brasil. En dicho trabajo se logró explicar de qué forma pudo elaborarse el módulo del *malware* Flame que robaba datos de dispositivos Bluetooth.

El descubrimiento de Studnex y Flame marca un hito en la historia de la seguridad informática mundial, donde el mundo pasó de combatir virus informáticos a denuncias por ciberataques entre naciones llevados a cabo mediante *software* con alta capacidad de desarrollo. El diario *New York Times* informaba que este *software* malicioso había sido patrocinado por Estados Unidos e Israel (Emergui, 2011). A partir de esto, los países aceleraron y otros empezaron a incursionar en la carrera armamentista digital del quinto dominio (ciberespacio). Otro hecho fundamental fue el comienzo de la discusión acerca de la gobernanza en Internet (UNESCO, s. f.).

Mapa de dominio

El mapa de dominio permite una mirada global de la ciberseguridad. En la siguiente figura se muestra este mapa.

Figura 6: Mapa de dominio



Fuente: Jiang, 2017, https://n9.cl/867de.

Lectura recomendada: Las siguientes lecturas permiten contextualizar la problemática que impulsó el fortalecimiento de las medidas de seguridad, el desarrollo de políticas específicas y la concientización sobre la necesidad de proteger las infraestructuras críticas. A través de estos casos y análisis, se evidencia el impacto real de las amenazas digitales y la importancia estratégica de la prevención y la protección en entornos críticos.

1 **BBC Mundo sobre Stuxnet**

BBC Mundo. (2015). *El virus que tomó control de mil máquinas y les ordenó autodestruirse*. https://bit.ly/3w9prqj

2 **Seguridad industrial y Stuxnet**

Lipovsky, R. (2017). *A siete años de Stuxnet, los sistemas industriales están nuevamente en la mira*. WeLiveSecurity. https://bit.ly/2GZOv57

3 **Stuxnet y sistemas SCADA en CNN**

Centro Criptológico Nacional (CCN-CERT). (2010). *El gusano Stuxnet que afecta a sistemas SCADA causa revuelo internacional*. https://bit.ly/3RSya6E

4 **Flame (*malware*)**

FayerWayer. (2012). *Descubren a "mini Flame", el hermano pequeño pero peligroso del virus Flame*. https://bit.ly/3PxdE9S

Escenarios reales de ciberataques

En esta instancia te proponemos ejecutar los mapas de detección de ciberataques en tiempo real enunciados en el apunte de la cátedra, así también leer sobre vulnerabilidades. Para entender cómo se comportan los ciberataques en un escenario real, analizarás los siguientes mapas:

- **Kaspersky**

Muestra por medio de líneas de colores los ciberataques que se llevan a cabo en tiempo real. Tiene también un apartado de "estadísticas": https://n9.cl/8qp94.

- **Fireeye**

Muestra las cinco industrias más amenazadas del último mes, lugar donde se están llevando los ataques y su nivel de seguridad: https://n9.cl/p047k.

- **Fortinet**

Muestra estadísticas de los ataques, tiene un mapa de día y otro de noche que se superponen a los ataques. Informa tipos de ataques, nivel de seguridad y ubicación: https://n9.cl/w3hf0.

- **Deteque**

"Muestra las ubicaciones de las IP de los servidores que se usan para controlar los *botnes* infectados con algún *malware*. También cuáles son los 10 países con más botnets y del número de bots activos en las últimas 24 horas" (LISA Institute, 2019, https://n9.cl/yr0s0). Acceder aquí: https://n9.cl/vdne8.

- **Threatbutt**

Tiene un diseño particular que incluye el sonido de videojuegos de los 80: https://n9.cl/twtiq.

- **Kaspersky**

Detección de ataques de *ransomware* en línea: https://n9.cl/z1k1ij.

Modelos y políticas de seguridad

La política de ciberseguridad en una empresa es un documento dinámico que debe actualizarse periódicamente para incluir cambios en la tecnología y en las regulaciones de cumplimiento que se establecieron. También deberá determinar cómo se autoevaluará la tarea.

¿Cómo redactar una política de seguridad de la información?

"ISO 27001 requiere que para redactar una política de Seguridad de la Información se sigan los siguientes pasos que se enuncian a continuación: Estudiar los requisitos, tener los resultados de su evaluación de riesgos, optimizar y alinear los documentos, estructurar el documento, narrar el documento, alcanzar la aprobación del documento, concientización y capacidad de sus trabajadores.

. . .

La Plataforma Tecnológica **ISOTools** ayuda a las organizaciones a llevar a cabo la redacción de una política de Seguridad de la Información según la norma **ISO 27001** y a implantarla en busca del éxito". (PMG, 2014, https://n9.cl/9sgrk)

Las políticas de seguridad para pymes elaboradas por INCIBE pueden ser útiles y guiar las planificaciones de seguridad o la creación de marcos de trabajo (*framework*). Estas normas se pueden encontrar en el sitio web de INCIBE (INCIBE, 2014) .

Seguridad del entorno

La seguridad física y lógica son componentes que deben planificarse cuidadosamente. Con el paso del tiempo, deben poder amoldarse a los dinámicos cambios que se presenten. Para garantizar que funcionen los procesos y el sistema, y que la información esté protegida, se suelen agrupar en cuatro áreas:

- Seguridad física
- Seguridad lógica

- Seguridad en la red
- Control de acceso adecuado, tanto físicos como lógicos

Existen diversos tipos de certificaciones en seguridad que ayudan a la protección de los datos:

- ISO 27001 / 9001: “Aplica a la gestión de la seguridad de la información de la empresa, enfocándose en la alineación de los objetivos de seguridad con los requisitos del negocio. Permite reducir el posible riesgo de fraude, pérdida y divulgación de la información” (IProfesional, 2010, https://n9.cl/ziype).
- Circular A 4609: Un *datacenter* apto para los bancos argentinos.
- CSA_CCM: (*cloud security alliance*): Versión v.3.0.1 - *threat and vulnerability management (cloud computing)*.
- También hay distintos tipos de certificación para los profesionales que certifican:
  - CISSP: IT Administration. Para gestionar y respaldar la postura y las políticas de seguridad generales de una organización.
  - CCSK: Cloud Security. Para adquirir, asegurar y administrar entornos en la nube o adquirir servicios en la nube.
  - MVP: Para diseñar, desarrollar y gestionar la postura de seguridad general de una

organización.

Seguridad física

Se refiere al conjunto de medidas, barreras y procedimientos destinados a proteger los activos y la información sensible mediante prevención y respuesta ante incidentes. Suele aplicarse especialmente en entornos de infraestructura crítica, donde deben contemplarse riesgos tanto intencionales (sabotaje, espionaje, robo de información) como accidentales o naturales (incendios, inundaciones u otros eventos).

Control de acceso

El control de acceso es un componente clave de la seguridad física y debe diseñarse pensando en amenazas externas e internas, además de posibles contingencias ambientales. No se limita a identificar a una persona: también implica autorizar o denegar el ingreso y vincular esa autorización con mecanismos físicos (apertura/cierre de puertas). Además, permite aplicar reglas según horarios, zonas o sectores específicos dentro de una organización. Algunos ejemplos de controles de acceso son:

- Lector biométrico.
- Detector de metales.
- Guardia de seguridad.
- Protección electrónica: circuito cerrado de televisión, detectores (aberturas, rotura vidrios, vibraciones), barreras infrarrojas.
- Seguridad con animales.
- Alternativas de potencia de corriente.
- UPS con batería.
- Generador eléctrico.

Seguridad lógica

“Existe un viejo dicho en la seguridad informática que dicta que ‘todo lo que no está permitido debe estar prohibido’ y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información”. (Zamenfeld, 2010, https://n9.cl/3hxk68).

En síntesis, la seguridad física es la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo. Por su parte, la seguridad lógica complementa la seguridad física e involucra medidas establecidas por la administración de recursos para

minimizar riesgos. No debemos olvidar que cada una de ellas deben conservar los principios estudiados al comienzo de la lectura: **confidencialidad, disponibilidad e integridad**.

Causantes de violaciones de acceso lógico

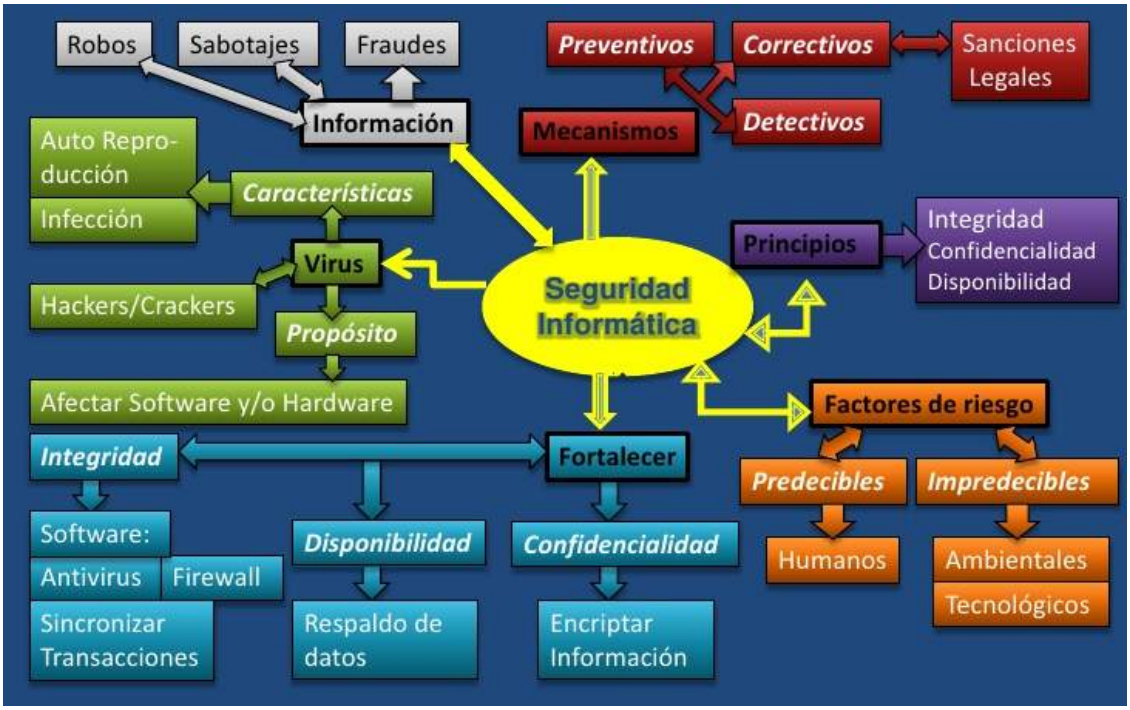
Los causantes de ataques pueden ser piratas informáticos (*hackers*), personal temporal o de tiempo parcial, exempleados, miembros de la competencia.

Lectura sugerida: Capítulo 2, 3 y 7 de Costas Santos (2011).

Resumen

La siguiente figura resume lo visto acerca de seguridad informática.

Figura 7: Resumen de seguridad informática



Fuente: [imagen sin título sobre resumen de seguridad informática], s.f., https://n9.cl/dsswlr .

CONTINUAR

Referencias

[Imagen sin título sobre modelo OSI] (s.f.). https://redess-locales-ocz-pjq.fandom.com/es/wiki/Modelo_OSI.

[Imagen sin título sobre resumen de seguridad informática] (s.f.). https://es.slideshare.net/slideshow/mapa-mental/4131760.

Avast (2020). *Malware frente a virus: ¿en qué se diferencian?* Avast. https://www.avast.com/es-es/c-malware-vs-virus

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria.

Bécares, B. (2020). *FireEye ofrece a las empresas herramientas para que puedan detectar si algún cracker los ataca con el software que le han robado*. Xataka. https://www.xataka.com/pro/fireeye-ofrece-herramientas-que-le-han-robado-a-empresas-estados-uno-grandes-problemas-seguridad-ano

Bejerano, P. G. (6 de 2 de 2014). *Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial*. El Diario.Es. https://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_1_5038272.html

Biontech (9 de 12 de 2020). *Statement Regarding Cyber Attack on European Medicines Agency*. Biontech. https://investors.biontech.de/news-releases/news-release-details/statement-regarding-cyber-attack-european-medicines-agency/

Contreras, B. (2019). *Marco NIST de Ciberseguridad: Un abordaje integral de la ciberseguridad*. LinkedIn. https://www.linkedin.com/pulse/marco-nist-de-ciberseguridad-un-abordaje-integral-

belisario-contreras/

Cortés, N. (2013). *El caso Snowden y nuestra indiferencia a la protección de datos*. Diario Rotativo. https://rotativo.com.mx/nacionales/el-caso-snowden-y-nuestra-indiferencia-a-la-proteccion-de-datos_160463_102.html

Costas Santos, J. (2011). *Seguridad y alta disponibilidad*. RA-MA.

digital, D. (13 de 07 de 2013). *BBC Londres*. Obtenido de https://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm

Emergui, S. (16 de enero de 2011). *Israel y EEUU crearon el virus que dañó el programa nuclear iraní*. El Mundo. https://www.elmundo.es/elmundo/2011/01/16/internacional/1295180388.html.

Gobierno de España (2012). *MAGERIT, versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I. Método*. Centro Criptológico Nacional, Ministerio de la Presidencia. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

González, A. (2019). *Significado de antivirus*. Significados. https://significado.com/antivirus-2/

INCIBE (2017). *Amenaza y Vulnerabilidad, ¿sabes en qué se diferencian?* INCIBE. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE (28 de 10 de 2014). *Centro Nacional de Ciberseguridad de España*. INCIBE https://files.incibe.es/incibe/politicas/politicas-pyme.zip

IProfesional (2010). *Telecom invierte $14 M en centros de datos para ofrecer nuevos servicios corporativos*. IProfesional. https://www.iprofesional.com/tecnologia/104911-telecom-invierte-14-m-en-centros-de-datos-para-ofrecer-nuevos-servicios-corporativos

Jiang, H. (10 de febrero de 2017). *The Map of Cybersecurity Domains (versión 2.0)*. LinkedIn. https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/.

Jonker, A., Lindemulder, G. y Kosinski, M. (s. f.). *¿Qué es la ciberseguridad?* IBM Think. https://www.ibm.com/mx-es/think/topics/cybersecurity

LISA Institute (2019). *Los 5 mapas de ciberataques más populares*. LISA Institute. https://www.lisainstitute.com/blogs/blog/los-5-mapas-de-ciberataques-mas-populares-en-2019

LISA Institute (s. f.). *Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación*. LISA Institute. https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas?srsltid=AfmBOop_FnWNwkQlNnBk3eRvjAFOIC6xw0tJmRxdx5UZUpRgQu_iFUda

Navarro Hidalgo, M. (2025). *Una breve historia de los virus informáticos y lo que nos deparará el futuro.* LinkedIn. https://www.linkedin.com/posts/manuelnavarrohidalgo_una-breve-historia-de-los-virus-inform%C3%A1ticos-activity-7352617090328989696-dJw4/?originalSubdomain=es

NIC Argentina (2018). *¿Qué es Ciberseguridad?* NIC Argentina. https://nic.ar/es/enterate/novedades/que-es-ciberseguridad

Omega Corp (s. f.). *Sistema de Gestión de Riesgos – ISO 31000*. OMEGA Corp. https://omegacorp-ec.com/sistema-de-gestion-de-riesgos-iso-31000/

Organización de los Estados Americanos (OEA) (2019). *Ciberseguridad: Marco NIST. Un abordaje integral de la ciberseguridad.* OEA y AWS. https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf.

Ortiz, J. (2011). *Colossus, la máquina que acortó la Segunda Guerra Mundial*. El Cajón de Grisom. http://www.elcajondegrisom.com/2011/05/el-coloso-la-maquina-que-descifro.html.

Pankov, N. (2020). *El impacto del coronavirus en la seguridad corporativa.* Kaspersky Lab. https://latam.kaspersky.com/blog/report-covid-wfh/18661/.

PMG (2014). *ISO 27001 ¿Cómo redactar una política de Seguridad de la Información?* PMG. https://www.pmg-ssi.com/2014/06/iso-27001-como-redactar-una-politica-de-seguridad-de-la-informacion/

PMG (2021). *Metodología NIST SP 800 – 30 para el análisis de Riesgos en SGSI*. PMG. https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/

Romero Castro, M., Figueroa Moran, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., Murillo Quimiz, Á., Castillo Merino, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Editorial Área de Innovación y Desarrollo, S.L.

Solarwinds (6 de 4 de 2021). *SolarWinds Security Advisory*. Solarwinds. https://www.solarwinds.com/sa-overview/securityadvisory#anchor1

T13 (2015). *El virus que tomó control de mil máquinas y les ordenó autodestruirse*. T13. https://www.t13.cl/noticia/tendencias/tecnologia/el-virus-tomo-control-mil-maquinas-y-les-ordeno-autodestruirse

Turton, W. y Bloomberg (15 de diciembre de 2020). *Hackers used a little-known IT vendor to attack U.S. agencies. Fortune* https://fortune.com/2020/12/15/solarwinds-hackers-u-s-agencies/

UNESCO (s.f.). *Gobernanza de Internet*. UNESCO. https://www.unesco.org/es/internet-governance.

Zamenfeld, S. (2010). *Recomendaciones en Seguridad Lógica*. Brain Labs. https://www.brainlabs.com/novedad/recomendaciones-en-seguridad-logica/

CONTINUAR

Descarga en PDF