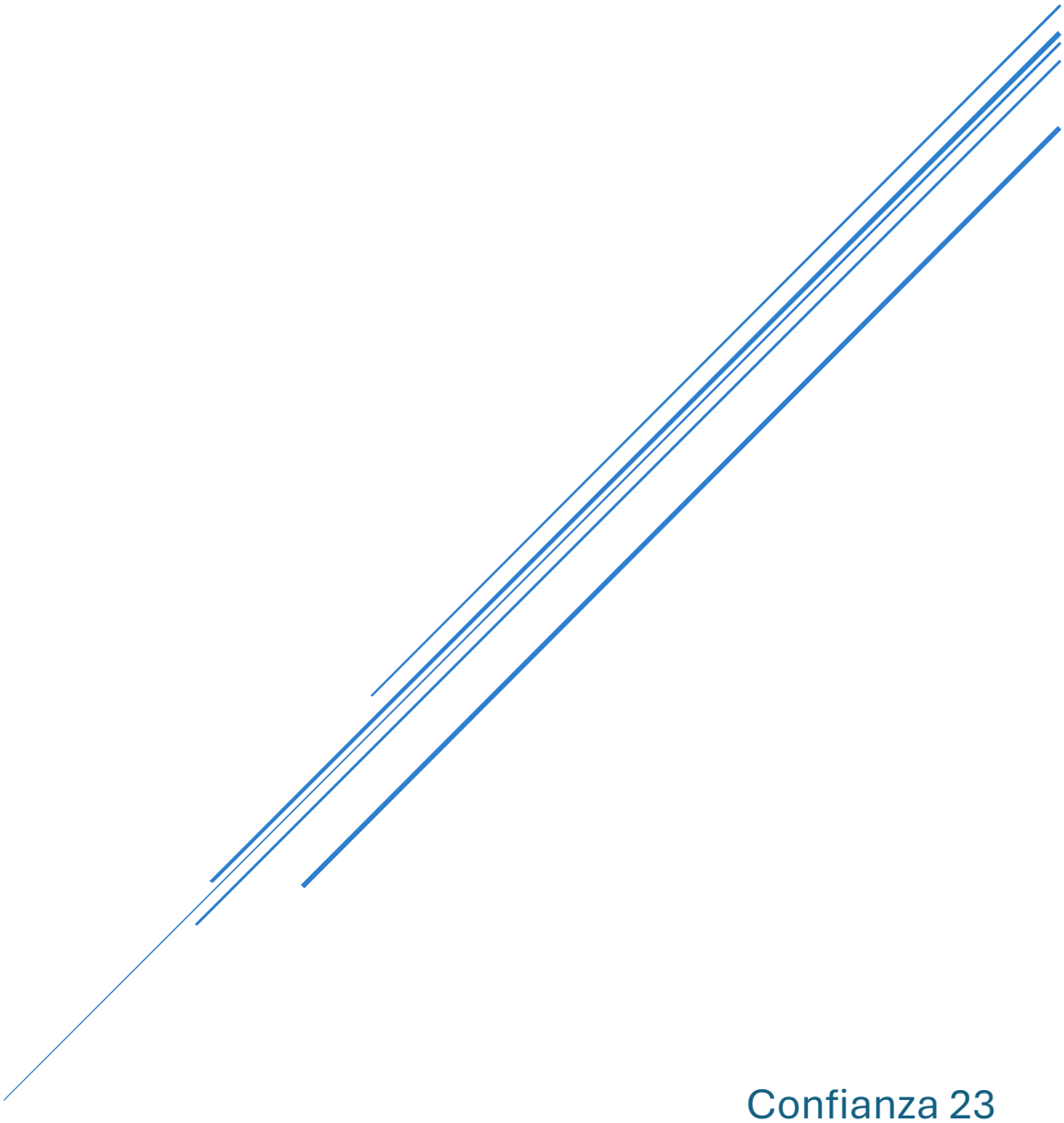
PROYECTO HAMMER

Documentación de investigación



Confianza 23

Programa de Prácticas 2025 Q2

Contents

Revisión conceptos e información teórica

La no familiaridad con algunos de los conceptos técnicos y normativos incluidos en el documento original se realizó una investigación detallada de los mismos para explorar y aprender sobre ellos. Por ello, en las siguientes secciones se analizan los estándares mencionados (como ISO 27001 y IEC 62443), los ámbitos de aplicación (IT, OT, IoT, etc.) y su impacto en la gestión de riesgos y ciberseguridad.

Ámbitos de Seguridad y Normativas Clave

1. **Seguridad de la Información y Ciberseguridad**:
    - **ISO 27001**: Norma internacional para la gestión de la seguridad de la información. Marco para proteger datos sensibles y gestionar riesgos de ciberseguridad.
    - **NIST Cybersecurity Framework v2**: Marco desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) que provee una guía para las industrias, gobiernos, agencias y otras organizaciones sobre cómo manejar los riesgos de ciberseguridad.
    - **NISTIR 8286**: Documento que integra la ciberseguridad con la gestión de riesgos empresariales. Brinda información para ayudar a las empresas a identificar, evaluar y manejar los riesgos de ciberseguridad en un contexto amplio.
2. **Seguridad Industrial**:
    - **ISA/IEC 62443**: Serie de estándares que define requerimientos y procesos en la implementación de ciberseguridad en sistemas de automatización y control industrial.
    - **NIST SP 1800-10**: Guía para proteger la integridad de los sistemas de control industrial en el sector manufacturero. Se centra en productos comerciales basados en estándares específicos y que representan algunas soluciones posibles relacionadas a la ciberseguridad en las empresas
3. **Inteligencia Estratégica y Competitiva**:
    - **UNE 166006:2018**: Norma para la gestión de sistemas de vigilancia e inteligencia en I+D+i, ayudando a anticipar cambios y reducir riesgos. Obligatoria para todas las organizaciones que establezcan sistemas de vigilancia

Un poco de información…

Ciberdelincuencia

La ciberdelincuencia es toda actividad ilegal que se realiza en entornos digitales, espacios digitales o a través de internet y dispositivos electrónicos. Implica cometer actividades delictivas como el robo de información personal, piratería o propagación de malware, entre otros.

Categorías

1. **Informática como objeto del delito** donde los ataques están dirigidos a dañar, comprometer o acceder ilegalmente a sistemas informáticos y datos digitales**.** Incluye ejemplos como sabotaje informático, crackeo, piratería informática, hackeo y DDNS (Denegación de servicio de nombres de dominio).

2. **Informática como medio del delito** donde los sistemas informáticos y las redes digitales se utilizan como herramientas para cometer delitos. Incluye falsificación de documentos electrónicos, cajeros automáticos y tarjetas de crédito, robo de identidad, fraudes electrónicos y pornografía infantil.

Ciberdelincuentes

Personas que cometen delitos informáticos convirtiéndose en amenazas para individuos, empresas y gobiernos involucrando a varias jurisdicciones, legislaciones, organizaciones, de todo el mundo.

Realizan delitos que suceden a diario, con tipificaciones penales, que ocurren de forma independiente, individual o grupal, sin encontrar elementos o indicios que nos permitan evaluar organización y regularidades en su conducta en sí.

Alcance de los ciberdelincuentes

Como el uso de dispositivos es cada vez es más común y todas las personas buscan comunicarse entre sí, el enviar información es algo inevitable sobre todo en casos en que las distancias son largas. Cualquier tipo de información enviada por medios electrónicos puede ser alcanzada por un ciberdelincuente, que no busca siempre beneficios económicos con su actividad delictiva, sino que en algunos casos busca poner a prueba su inteligencia, realizar extorciones o simplemente por el hecho de poder hacerlo. Por lo que, para la mayoría de ellos, no hay límites ni geográficos, ni éticos ni legales, ya que pueden operar desde cualquier parte del mundo y aprovechar la falta de regulaciones entre países para evadir la justicia.

Ciberamenaza

Acción o acto malicioso que busca comprometer, dañar o robar información digital con distintos objetivos como la irrupción de servicios, extorción, espionaje perjudicando así la seguridad digital de individuos, empresas o gobiernos.

Ataques Comunes

- **Malware:** Software malicioso diseñado para infiltrarse y dañar sistemas.
- **Troyanos:** Se hacen pasar por programas legítimos, pero ejecutan acciones maliciosas.
- **Virus y gusanos:** Código que se replica y se propaga sin el consentimiento del usuario.
- **Ransomware:** Cifra archivos y exige un pago para su recuperación.

- **Botnets:** Redes de dispositivos infectados controlados remotamente por atacantes.
- **Spyware:** Programa espía que recopila y roba información del usuario.
- **RATs (Troyanos de acceso remoto):** Permiten a un atacante tomar el control del sistema de manera remota.
- **Backdoors:** "Puertas traseras" que permiten el acceso no autorizado a un sistema.
- **Ataques DNS:** Manipulan el tráfico web para redirigir a los usuarios a sitios fraudulentos.
- **Ataques DDoS:** Sobrecargan servidores con tráfico masivo hasta colapsarlos.
- **Formjacking:** Inyecta código malicioso en formularios de pago para robar datos sensibles.

Delito cibernético

Actividad delictiva realizada por ciberdelincuentes con el objetivo de obtener fondos ilegales o causar daño a activos de información de una organización o institución. Los delitos ocurren en entornos digitales, donde los atacantes emplean diversas técnicas para infiltrarse en sistemas, acceder a datos confidenciales y cometer fraudes o extorsiones.

Los ciberdelitos representan una amenaza para la seguridad de individuos, empresas y gobiernos, ya que utilizan las computadoras tanto como medio como objetivo del crimen.

Características

Anónimos, desconocimiento de la identidad del delincuente, ya que su identidad puede estar oculta o distorsionada con la que realiza la acción delictiva. Tener conocimientos en la materia y habilidades necesarias permite cometer el delito y encubrirlo generando una difícil persecución del ciberdelito ya que se desconoce, en la mayoría de las ocasiones, quién es el autor real o desde qué red se ha cometido el delito.

Inexistencia de barreras geográficas, Con las TICs la comunicación puede ser en el momento sin importar las distancias, es decir, no se encuentran fronteras geográficas para que la comunicación se mantenga. Con las redes digitales, los ciberdelincuentes pueden operar desde cualquier parte del mundo, incluso desde países con escasa o nula regulación en la materia provocando los llamados “paraísos cibernéticos”, que son lugares donde la data de intervención judicial los hace más factibles para la cometer los delitos cibernéticos.

Instantáneos, se los puede efectuar en el mismo momento en el que el ciberdelincuente comienza la acción.

Masivos, Las TICs habilitan la difusión masiva de contenidos. Provocando que el ciberdelito se haga a mas personas al mismo tiempo y que la dimensión del mismo sea ilimitada.

Pluriofensivos, Pueden afectar a más de un bien jurídico protegido a la vez, pudiendo vulnerar la privacidad e integridad de la información, patrimonios y la seguridad tanto de individuos como de organizaciones o gobiernos.

Facilidad de comisión El delincuente no requiere de extensos recursos, medios o conocimiento para realizar el delito. Sino que, con tener un dispositivo electrónico al alcance y conexión a la red Internet, se puede fácilmente realizar la acción delictiva e incluso es posible encontrar personas que se ofrezcan a realizarlo.

Tipos de Delitos Cibernéticos

Según la ONU, Organización de Naciones Unidas, se reconocen los siguientes tipos de delitos informáticos:

1. **Fraudes cometidos mediante manipulación de computadoras;** Manipulación de datos, programas o transacciones financieras para obtener beneficios ilegales.

2. **Manipulación de datos de entrada;** como objetivo se alteran directamente los datos de una información computarizada o sistemas informáticos para cometer falsificaciones o fraudes.

3. **Daños o modificaciones de programas o datos computarizados;** entran tres formas de delitos: sabotaje informático elimina o modifica sin autorización funciones o datos de una computadora obstaculizando su funcionamiento. Acceso no autorizado a servicios y sistemas informáticos, espionaje o sabotaje

Otros tipos

1. **Hacking** Acceso ilegal y no autorizado a sistemas de información, redes o bases de datos. Los que destacan son:

    - **Etico:** Proceso de intrusión en sistemas o redes con el objetivo de identificar y reparar posibles puntos de ataque. Utilizan sus habilidades para mejorar la seguridad y proteger la información.

    - **Malicioso o cracker:** Tiene como objetivo causar daño, robar información o ganar acceso no autorizado a sistemas.

2. **Phishing:** Técnica de fraude en línea que utilizada para engañar a usuarios y hacer que revelen información personal y financiera. Los ciberdelincuentes simulan ser entidades de confianza y envían mensajes o correos electrónicos que instan al destinatario hacer clic en un link malicioso o descargar un archivo peligroso comprometiendo su seguridad y obteniendo la información necesaria para efectuar el ciberdelito. Siendo el método mas antiguo y efectivo para enganar a los usuarios

Tipos de Phishing

"Muchos ataques de ransomware se basan en este tipo de códigos maliciosos para apoderarse de los sistemas de una organización y cifrar sus datos. Según estimaciones de 2017, más de 9 de cada 10 correos electrónicos de phishing venían con archivos adjuntos que contenían código de ransomware." (*What is phishing? Definition, types, and prevention best practices*, 2025)

- **Spear phishing,** ataque a un individuo específico, como empleados de empresas sobre todo de IT, para obtener información confidencial
- **Whaling o whale phishing**, ataque a "peces muy gordos", como directores generales, administradores de red o altos ejecutivos.
- **Clon phishing,** se produce cuando un atacante crea una réplica formidable de un mensaje oficial o correo electrónico falso para engañar al usuario. A veces implica que el atacante «reenvíe» un mensaje momentos después de que el remitente legítimo haya enviado el mensaje original y oficial, simulando que reenvía el mensaje original por alguna razón, como haber insertado un enlace o un archivo adjunto incorrecto. Otra variante consiste en que el atacante crea un sitio web duplicado con un dominio falsificado.
- **Vishing,** combinación de «voice» (voz) y «phishing» (suplantación de identidad), se realiza a través de una llamada telefónica donde se le transmite un mensaje de voz supuestamente de un banco o una institución financiera y le pide a la victima que llame a otro número e introduzca su PIN u otra información de la cuenta con fines oficiales, como la verificación de la seguridad que luego pasan a ser del ciberdelincuente.
- **Snowshoeing,** Ataque de «golpear y correr» el agresor envía múltiples mensajes a través de diferentes direcciones IP y dominios. Cada uno está programado para enviar

unos pocos mensajes, por lo que los filtros de spam basados en el volumen o la reputación no bloquean estos mensajes inmediatamente.

Cibercrimen

Serie de delitos informáticos que ocurren de organizadamente, de forma profesional y su motivación es solo económica.

- Para el ciberdelincuente, los sujetos pasivos de estos delitos son elementos fungibles y sin interés, ya que el sólo busca optimizar sus ganancias.
- Según el **FBI**, las organizaciones cibercriminales operan como empresas, con expertos en cada tipo de trabajo y ocupación.

Blockchain o Cadena de bloques

Estructura de datos cuya información se agrupa en conjuntos llamados bloques con meainformacion relativa a otro u otros bloques, haciendo un seguimiento seguro de los mismos Gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques anteriores, propiedad que permite su aplicación en entornos distribuidos.

Principales características

- **Registro distribuido:** No depende de una única entidad certificadora.
- **Seguridad criptográfica:** Basado en criptografía asimétrica y funciones hash.
- **Inmutabilidad:** Una vez que un dato es registrado, no puede ser modificado sin alterar toda la cadena.
- **Descentralización:** Funciona en redes de pares (P2P).
- **Almacenamiento ordenado en el tiempo:** Se registran cambios de estado de manera secuencial.

Funcionamiento

Componentes esenciales

- **Almacenamiento de datos,** se logra mediante la replicación de información en los bloques de la red.
- **Transmisión de datos,** se realiza a través de redes P2P (peer-to-peer).
- **Confirmación de datos,** se obtiene mediante un proceso de consenso entre los nodos participantes.

Aplicaciones de la Blockchain

- **Dinero digital,** implementa registros contables distribuidos (ej. Bitcoin).
- **Autenticación y verificación de documentos,** estampillado de documentos para asegurar su integridad.
- **Contratos inteligentes (Smart Contracts),** ejecuciones de acuerdos automatizados sin intermediarios.

Piratería

Acceso no autorizado a servidores, redes, sistemas de información o aplicaciones de una organización con el objetivo de obtener información confidencial o crítica.

Hackers, personas externas que buscan penetrar en redes y servidores para robar datos sensibles como información estratégica o detalles de clientes, con la intención de exigir un rescate a cambio de su restauración.

Tipos de piratería informática

1. **Hurto de tiempo de máquina,** empleo de recursos de una empresa sin autorización
2. **Apropiación o hurto de hardware y datos, a**cceso ilegal a sistemas ajenos o sesiones de otros usuarios para robar información.

Piratería y derechos de autor

Abarca la violación ilegal del derecho de autor, definida en el **Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual (ADPIC)** que implica la copia similar a la original con la intensión de usarla como tal.

Existen dos modalidades principales:

- **Piratería técnica:** Copias de software o material digital para distribución ilegal.
- **Reproducción burda:** Imitaciones de productos originales con calidad inferior.

Malware

Software malintencionado diseñado para infiltrarse, dañar o hacer un uso no autorizado de un sistema informático sin el consentimiento del propietario. Herramienta utilizada mayormente en la ciberdelincuencia para lograr una variedad de fines. Describe a cualquier programa o archivo que tiene la intención de interrumpir o dañar un sistema o computadora, es decir infringe una red a través de vulnerabilidades.

- **Troyano**, forma de malware que se disfraza de software legítimo, pero realiza actividades maliciosas al ejecutarse.

Ciberseguridad

Práctica para proteger sistemas, computadoras portátiles, computadoras, redes, servidores, dispositivos electrónicos, información y datos de posibles ataques maliciosos por parte de piratas informáticos con el propósito de mantener la integridad y privacidad de los datos.

La ciberseguridad contiene los derechos y permisos de acceso a los datos del usuario para acceder a cualquier fuente de información. Además de cubrir el desarrollo y mantenimiento de uno o mas planes de recuperación de desastres y continuidad del negocio con la intensión de minimizar posibles efectos frente a incidentes de ciberataque. En estos planes se busca evitar la perdida o “fuga” de información, datos u operaciones.

Resumiendo, los objetivos principales son:

- Identificar y determinar el hecho denunciado y los posibles autores de acuerdo a la hipótesis del acusador.
- Resguardar la evidencia digital, ya que (a diferencia de la prueba física), se puede perder debido a su carácter volátil.
- Proyectar y realizar diferentes medidas de investigación para identificar al usuario sospechoso.

Características

- **Confidencialidad:** Garantizar que solo las personas autorizadas puedan acceder a la información.
- **Integridad**: Asegurar que los datos no sean alterados de manera malintencionada.

- **Disponibilidad**: Garantizar que los sistemas y la información estén accesibles cuando se necesiten.
- **Autenticación**: Verificar la identidad de los usuarios o dispositivos que acceden a los sistemas.
- **No repudio**: Evitar que un usuario o entidad pueda negar haber realizado una acción o transacción.

Tipos de ciberseguridad

- **Seguridad de la red:** Protección de la infraestructura de redes contra accesos no autorizados, ataques DDoS, malware, etc.
- **Seguridad de la información (InfoSec):** Protección de datos almacenados y en tránsito.
- **Seguridad en la nube:** Implementación de medidas de seguridad en entornos cloud.
- **Seguridad de dispositivos y endpoints:** Protección de dispositivos como computadoras, servidores y móviles.
- **Seguridad de aplicaciones:** Asegurar que el software esté libre de vulnerabilidades explotables.
- **Seguridad operativa:** Control de permisos de acceso y gestión de riesgos.
- **Resiliencia cibernética:** Capacidad de una organización para detectar, responder y recuperarse de ataques cibernéticos.

Inteligencia sobre ciberamenazas (CTI)

Proceso de recopilación, procesamiento y análisis de información relacionada con adversarios en el ciberespacio para difundir inteligencia sobre amenazas procesable. Busca comprender las motivaciones, el modus operandi y las capacidades de los atacantes para informar sobre las medidas de mitigación de la ciberseguridad a través de los equipos de seguridad de la empresa.

Permite a una empresa obtener información valiosa mediante el análisis de riesgos situacionales y contextuales, se adapta al panorama específico de amenazas en los mercados e industrias de las empresas. Esto permite a las empresas anticiparse a la mayoría de ciberamenazas o brechas planificadas antes de que se produzcan proporcionando alertas e indicadores específicos y así localizar y mitigar la amenaza. La inteligencia sobre amenazas también ofrece conocimiento de la situación del panorama de amenazas para permitir a los equipos de seguridad de las empresas comprender quién podría estar interesado en atacar su entorno

Búsqueda de ciberamenazas

La caza de amenazas implica ir proactivamente más allá de lo que ya sabemos o de lo que se nos ha alertado. Mientras que el software de seguridad nos alerta de los riesgos y comportamientos de ciberseguridad que sabemos que son maliciosos, la caza de amenazas se aventura en lo desconocido.

Ejercicio de seguridad activa con la intención de encontrar y erradicar atacantes desconocidos o nuevos que han penetrado en su entorno sin hacer saltar ninguna alarma. Esto contrasta con las investigaciones y respuestas tradicionales que se derivan de alertas que aparecen después de que se haya detectado la actividad potencialmente maliciosa.Los atacantes es pasar desapercibidos hasta que puedan acceder a la información más delicada, pero para detenerlos, primero hay que detectarlos. Ahí es donde la mentalidad de «asumir siempre una brecha» del equipo de caza de amenazas ayuda a descubrir IOA (indicios de ataque) que aún no se han detectado.

Vulnerabilidad de seguridad

Característica no intencionada de un componente informático o configuración del sistema que multiplica el riesgo de que ocurra un evento adverso o una pérdida, ya sea debido a una exposición accidental, un ataque deliberado o un conflicto con nuevos componentes del sistema.

Por su propia definición, una vulnerabilidad puede ser corregida mediante un parche de software, reconfiguración, capacitación de usuarios, actualización de firmware o reemplazo de hardware, a diferencia de un riesgo de seguridad que podría ser inevitable. A medida que los sistemas digitales evolucionan, surgen nuevas vulnerabilidades junto con ellos.

Se aconseja:

- Monitorear proactivamente las vulnerabilidades
- Priorizar las vulnerabilidades y corregirlas
- Divulgar vulnerabilidades de manera controlada para evitar riesgos de litigio
- Contribuir con datos de vulnerabilidades a fuentes de datos de inteligencia sobre amenazas de terceros para ayudar a la comunidad global de InfoSec a beneficiarse de su inteligencia colectiva.

Tipos de vulnerabilidades de seguridad

- **Vulnerabilidades en el código fuente**, Aparece en el momento del desarrollo del software. Puede haber errores lógicos que conducen a fallas de seguridad o configuraciones incorrectas.
- **Configuraciones de confianza,** concesiones que hace para el intercambio de datos hacia y desde sistemas de software y hardware
- **Prácticas de credenciales débiles,** vulnerabilidades en sistemas tanto de consumidores como de empresas. Los usuarios tienden a apegarse a prácticas de credenciales convenientes o cómodas, priorizando la facilidad de uso sobre la seguridad.
- **Falta de cifrado fuerte,** riesgo masivo que puede llevar a violaciones de datos severas. El cifrado de datos asegura que, si su plataforma de almacenamiento principal cae en manos equivocadas, alguien con malas intenciones no podrá descifrar o entender la información.
- **Amenaza interna,** van desde prácticas de reclutamiento y verificación de antecedentes mal pensadas hasta conflictos internos y fuerzas geopolíticas. Con la mayoría de los empleados trabajando desde casa, puede ser difícil detectar comportamientos anómalos que podrían indicar una amenaza interna en su organización.
- **Vulnerabilidad psicológica,** vulnerabilidades a través de ingeniería social. Convencer al usuario que necesita tomar medidas para desbloquear un beneficio o evitar una situación adversa.
- **Autenticación inadecuada,** surgen cuando no hay suficientes controles y equilibrios para restablecer contraseñas y credenciales.
- **Fallas de inyección,** aplicaciones web mal configuradas pueden ser propensas a fallas de inyección. Si la aplicación toma la entrada del usuario a través de un formulario en línea e inserta esa entrada en una base de datos de backend, comando o llamada de sistema de operaciones, dejaría la aplicación abierta a ataques de inyección como inyecciones SQL, XML o LDAP.
- **Exposición de datos sensibles**, no siempre hay una intención maliciosa detrás de estos escenarios. Errores humanos o configuraciones incorrectas del sistema hacen que datos sensibles (propiedad intelectual, credenciales de usuario, información personal identificable, detalles de pago, etc.) terminen en el lugar equivocado donde son vulnerables a la explotación.

- **Monitoreo y registros insuficientes,** análisis regular de registros y registros detallados son esenciales para frenar las vulnerabilidades de seguridad. De lo contrario, una entidad no autorizada puede obtener acceso a su paisaje informático sin que nadie se dé cuenta antes de que sea demasiado tarde.
- **Vulnerabilidades de tenencia compartida,** las soluciones de nube pública operan en un modelo de múltiples inquilinos donde un conjunto compartido de recursos se alquila a varias organizaciones en diferentes momentos, dependiendo de la escala de sus requisitos de recursos. Si un inquilino es comprometido, es posible que el ataque se propague a otras organizaciones en la nube aprovechando las vulnerabilidades de tenencia compartida. Por eso, las organizaciones que manejan información sensible, como bancos, escuelas y hospitales, eligen dividir sus cargas de trabajo entre inquilinos públicos y privados, manteniendo sus datos más valiosos compartimentados.

Evidencia digital

Es cualquier información en formato digital que puede usarse como prueba en una investigación judicial. Esta proviene de dispositivos electrónicos como computadoras, teléfonos móviles, servidores, cámaras de seguridad, discos duros, memorias USB, redes sociales, correos electrónicos, entre otros. Es fundamental para la investigación tanto aquellos aportados por el denunciante como de la víctima.

Características

- **Volátil,** se pierde o modifica fácilmente si no se manipula correctamente.
- **Reproducible,** se puede realizar copias sin alterar el original, lo cual es útil para análisis forenses.
- **Dependiente del contexto,** la interpretación de la información puede variar dependiendo del entorno tecnológico y legal.
- **Necesita herramientas especializadas,** su obtención, análisis y preservación requiere conocimientos técnicos y procedimientos forenses adecuados.
- **Intangible**, el dispositivo electrónico es el envase que soporta a los bits de información allí almacenada.
- **Posee metadatos**, esto es, dato del dato. Por ejemplo, la fecha de creación del documento.
- **Almacenamiento,** permite grandes volúmenes de información en contenedores de dimensiones reducidas, como un pendrive, por lo que exige una correcta identificación para no perder evidencia valiosa.

Concusiones

La ciberseguridad toma importancia día a día, a medida que más empresas e individuos confían en los dispositivos digitales e Internet convirtiéndolos en referentes para la comunicación, las transacciones y el almacenamiento de datos confidenciales. Po otro lado las amenazas de ciberseguridad provienen de varias fuentes, incluidos piratas informáticos, virus y malware, y se utilizan para causar daños financieros, de reputación y legales significativos.

El aumento constante del número de amenazas a la ciberseguridad y la creciente complejidad de los ataques, las empresas y los usuarios en general, tienen dificultades para mantenerse al día. Ayudar a detectar antes las amenazas y a responder con rapidez, es lo mas importante hoy en día, para así ahorrar a la empresa no sólo dinero o multas, sino también proteger su credibilidad y el valor de su marca.

Idealmente, todas estas vulnerabilidades deberían ser detectadas y corregidas durante las pruebas/QA, pero podrían filtrarse a la cadena de suministro y afectar a las empresas.

Por esto se recomienda:

- Realizar una auditoría de red
- Analizar datos de registros del sistema
- Utilizar un probador de penetración o hacker ético
- Aprovechar una base de datos de inteligencia sobre amenazas
- Simular un ataque de ingeniería social
- Utilizar minería de procesos para detectar fallas ocultas
- Revisar el código fuente
- Auditar la cadena de suministro de TI
- Documentar el paisaje de hardware

Bibliografías

Norma

Cybersecurity Framework | NIST (2025). https://www.nist.gov/cyberframework

Stine, K. *et al.* (2020) *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. https://doi.org/10.6028/nist.ir.8286

ISA/IEC 62443 Series of Standards - ISA (no date). https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Artículos

Administrador (2025) *CIBERDELITOS ¿Qué son y cómo investigarlos? - Revista At/pica*. https://revistaatipica.mjus.gba.gob.ar/ciberdelitos-que-son-y-como-investigarlos/#:~:text=La%20conducta%20antijur%C3%ADdica%20puede%20realizarse,conocidos%20como%20empresarios%20criminales%20individuales

Financial Crime Academy (2025) 'Descripción general de los delitos cibernéticos y la ciberseguridad: La importancia de la ciberseguridad en,' *Financial Crime Academy*, 1 April. https://financialcrimeacademy.org/es/descripcion-general-de-los-delitos-ciberneticos-y-la-ciberseguridad-la-importancia-de-la-ciberseguridad-en-la-lucha-contra-los-delitos-ciberneticos/#:~:text=El%20delito%20cibern%C3%A9tico%20se%20refiere,l%C3%ADnea%2C%20phishing%20y%20acoso%20cibern%C3%A9tico

What is a cyber threat? Definition, types, hunting, best practices, and examples (2025). https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat/

What is phishing? Definition, types, and prevention best practices (2025b). https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-phishing-definition-types-and-prevention-best-practices/

Páginas Web

colaboradores de Wikipedia (2025) *Delito informático*. https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

colaboradores de Wikipedia (2025a) *Cadena de bloques*. https://es.wikipedia.org/wiki/Cadena_de_bloques

Colaboradores de Wikipedia (2024) *Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio*. https://es.wikipedia.org/wiki/Acuerdo_sobre_los_Aspectos_de_los_Derechos_de_Propiedad_Intelectual_relacionados_con_el_Comercio