

Módulo 1: Introducción a la seguridad computacional

Lección 1: Panorama de la Ciberseguridad Moderna

Objetivos de la Lección

Al finalizar, el estudiante podrá:

1. **Definir** con precisión *seguridad computacional* y relacionarla con la tríada CIA (Confidencialidad-Integridad-Disponibilidad).
2. **Explicar** la importancia económica, social y legal de la ciberseguridad para individuos, organizaciones y gobiernos.
3. **Reconocer** y **analizar** tendencias actuales (Zero Trust, IA generativa, cadena de suministro, criptografía pos-cuántica y regulación) que configuran el panorama de la ciberseguridad.

Introducción a la Lección

Casi todas las actividades humanas dependen hoy de sistemas digitales: desde un pago sin contacto hasta la operación de infraestructuras críticas. A medida que el valor de los datos crece, también lo hacen las amenazas que buscan comprometerlos. Esta lección establece un fundamento común—definiciones, motivaciones y tendencias—sobre el que se construirán los módulos posteriores.

Desarrollo del Tema

Definición de Ciberseguridad y Seguridad Computacional

- **Ciberseguridad:** de acuerdo con Amazon Web Service (AWS), la ciberseguridad es una metodología o práctica de proteger equipos (ya sea a nivel de software o hardware), sistemas críticos y datos de posibles amenazas digitales. En la ciberseguridad se utilizan medidas y herramientas en el cual protegen datos confidenciales del acceso no autorizado o de intrusiones, así también como para evitar interrupciones de operaciones empresariales debido a actividades no deseadas.
- **Seguridad computacional:** disciplina que aplica controles físicos, técnicos y administrativos para proteger la **confidencialidad, integridad y disponibilidad** de los activos digitales y los sistemas que los procesan (Pfleeger & Pfleeger, 2023).
- **¿Qué es la Tríada CIA?**
(<https://www.fortinet.com/lat/resources/cyberglossary/cia-triad>)
 - **Confidencialidad** – la confidencialidad trata sobre los esfuerzo y desempeño que toma una compañía para que sus datos más sensibles no queden al ojo público o más bien queden totalmente privados. Esto implica, como componente clave, en que se tenga un sistema configurado con listas de control de acceso, en el cual permita que un grupo de usuario no puedan acceder a dichos datos o información privilegiada.
 - **Por ejemplo,** aquellos que trabajan con las finanzas de una organización deben poder acceder a las hojas de cálculo, cuentas bancarias y otra información relacionada con el flujo de dinero. Sin embargo, es posible que no se otorgue acceso a la gran mayoría de empleados, y quizás incluso a ciertos ejecutivos. Para garantizar que se sigan estas políticas, deben existir restricciones estrictas para limitar quién puede ver qué.
 - **Integridad** – La integridad trata en **asegurar** que los datos estén completamente seguros y **sin alteraciones**. La integridad de los datos se

mantienen solo si estos son auténticos, precisos y confiables. La integridad de los datos puede verse comprometida tanto de forma intencional como accidental. En algunos casos, un atacante logra evadir los sistemas de detección de intrusos (IDS), modifica archivos para abrir accesos no autorizados o manipula registros del sistema con el fin de encubrir su actividad y debilitar la seguridad de la información. Por otro lado, también pueden ocurrir errores involuntarios, como ingresar un código incorrecto o realizar acciones descuidadas. Incluso, si la organización no cuenta con políticas, controles y procedimientos adecuados, la integridad puede deteriorarse sin que haya una acción directa por parte de algún individuo.

- **Ejemplo:** si su empresa proporciona información sobre gerentes sénior en su sitio web, esta información debe tener integridad. Si es impreciso, las personas que visitan el sitio web para obtener información pueden sentir que su organización no es confiable.
- **Disponibilidad** - La disponibilidad es la capacidad de acceder a los datos y recursos cuando se necesitan. Aunque la confidencialidad y la integridad de la información se mantengan intactas, los datos resultan inservibles si no están disponibles para los usuarios autorizados en el momento adecuado. Esto implica que los sistemas, redes y aplicaciones deben operar correctamente y de manera continua. Además, quienes tienen permiso para acceder a cierta información deben poder consultarla sin demoras excesivas, garantizando así la eficiencia en las operaciones tanto internas como en el servicio al cliente.
 - **Por ejemplo,** si ocurre un apagón y no existe un **plan de recuperación ante desastres**, los usuarios podrían perder el acceso a sistemas esenciales, lo que pondría en peligro la disponibilidad. Asimismo, fenómenos naturales (Acts of God) como inundaciones o fuertes tormentas de nieve pueden impedir que los

empleados lleguen a sus lugares de trabajo, afectando el uso de estaciones y equipos necesarios para acceder a información o aplicaciones críticas. La disponibilidad también puede verse afectada por ataques intencionales, como los **ataques de denegación de servicio (DoS)** o **infecciones por ransomware**, que buscan interrumpir el acceso a los recursos.

- **Ejemplo práctico usando la Tríada Completa:** un sistema de salud que cifra historiales médicos (confidencialidad), utiliza firmas digitales en órdenes médicas (integridad) y mantiene servidores redundantes (disponibilidad).
- **Imagen CIA**

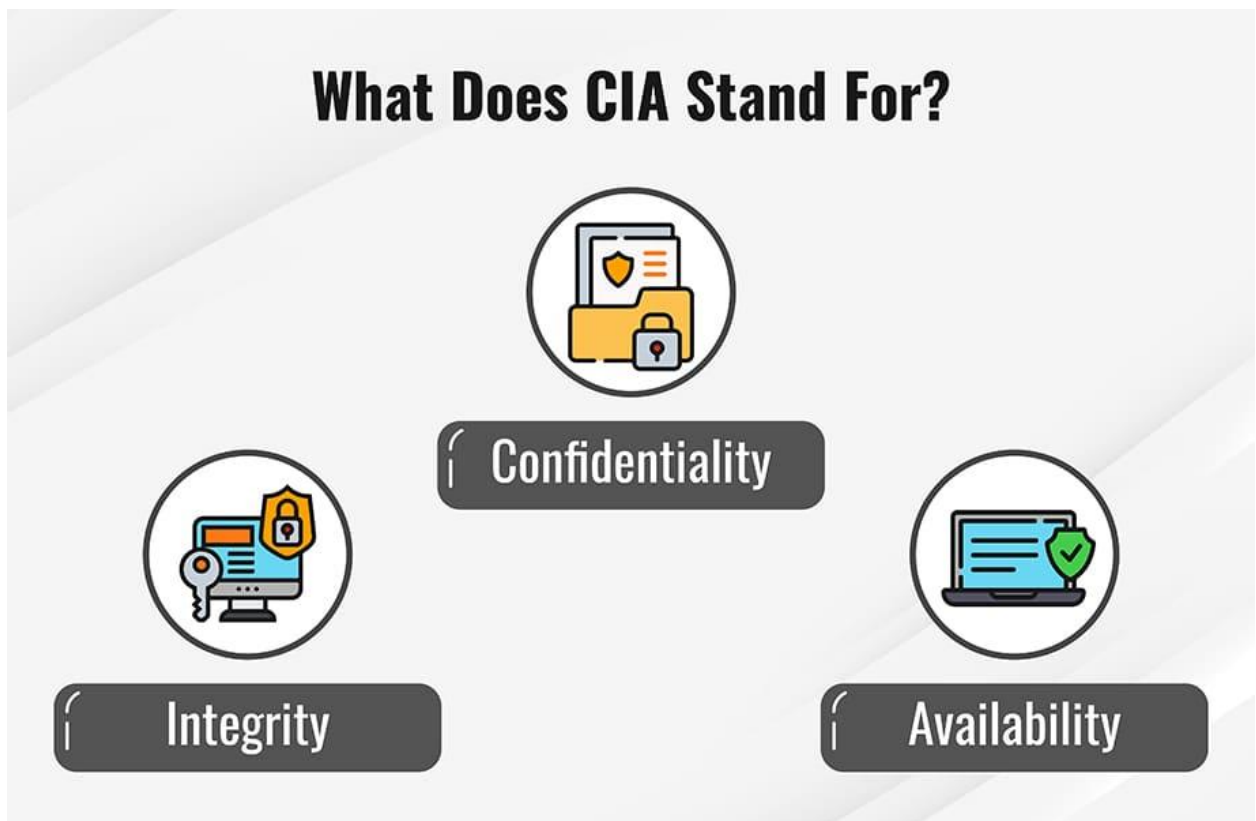


Imagen 1: Tríada CIA, <https://www.fortinet.com/lat/resources/cyberglossary/cia-triad>

Importancia de la seguridad computacional

La **seguridad computacional** se ha convertido en una necesidad fundamental ante los profundos cambios en los procesos productivos y en la forma en que la sociedad global interactúa, impulsada por la transformación digital. En este contexto, la información ha pasado a ser uno de los activos más valiosos tanto para organizaciones como para individuos. Para proteger estos datos, es indispensable invertir en mecanismos de seguridad adecuados. La seguridad computacional abarca la prevención, detección y respuesta ante accesos no autorizados a sistemas informáticos, y tiene como objetivo salvaguardar tanto los recursos digitales como los datos, frente a posibles intrusos que busquen usarlos de forma maliciosa o con fines ilícitos. Dicho esto la Seguridad Computacional puede ser trabajada por las siguientes 4 dimensiones:

1. **Económica:**

- a. El impacto económico del cibercrimen es monumental. De acuerdo con la revista CyberCrime Magazine (2023), se afirmó una estimación que en 2024, los costos asociados al delito cibernético superarían los US \$9 billones a nivel mundial, abarcando desde fraudes, robo de datos, hasta interrupciones operativas. Sin embargo, Reuter (2025) establece que de acuerdo con el informe del FBI, para el 2024 la suma total de pérdidas por cibercrímenes fueron de al menos \$16 billones, superando las estadísticas que plantearon en la revista CyberCrime.
 - i. Pequeñas y medianas empresas (pymes) son especialmente vulnerables, representando el 43 % de los objetivos de ataques, debido a la falta de recursos para implementar medidas robustas de ciberseguridad.
 - ii. Una sola violación de seguridad puede llevar a pérdidas económicas directas (robos, rescates) e indirectas (interrupciones de servicio, pérdida de clientes).

2. **Legal:**

- a. Normativas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Ley de Privacidad del Consumidor de California (CCPA) imponen sanciones severas por filtraciones o mal manejo de datos personales.
- b. Las multas pueden alcanzar hasta el 4 % de la facturación global anual, lo que representa una amenaza financiera considerable para empresas negligentes o desprevenidas.

3. **Reputacional:**

- a. Ejemplos notables incluyen ataques de ransomware a hospitales, los cuales han paralizado servicios médicos vitales y generado una pérdida masiva de confianza pública.
- b. Para las empresas, la pérdida de credibilidad ante clientes, socios y accionistas puede resultar más costosa que el daño económico inmediato.

4. **Personal:**

El usuario común también enfrenta riesgos significativos en el ámbito de la ciberseguridad.

- a. El robo de identidad y la exposición de datos personales se han vuelto frecuentes, especialmente con la proliferación de dispositivos conectados (IoT) como cámaras, asistentes virtuales o wearables (Dispositivos que los usuarios se ponen o llevan puestas y que procesan datos en tiempo real tales como Reloj y Gafas Inteligente, como los Apple Watch y demás.).
- b. Esta información puede ser usada para fraudes, chantajes, o suplantación de identidad, afectando la seguridad y privacidad de las personas

Caso ilustrativo: El ataque de *ransomware* a Colonial Pipeline comprometió disponibilidad y confidencialidad, implicó un pago de \$4.4 millones y afectó el suministro de combustible en la costa Este de EE. UU. ***Para más información:***

<https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

Uso de la seguridad computacional

La aplicación de la ciberseguridad varía según el contexto, pero siempre parte de la necesidad de proteger activos digitales frente a amenazas concretas:

1. Entornos corporativos.

Las empresas implementan copias de seguridad 3-2-1 (La regla 3-2-1 es dada por “**Conservar 3 copias de los datos**”, “**Guarde 2 copias de backups en distintos soportes de almacenamiento**”, “**Almacene 1 copia de BackUps externa**”), segmentación de red y controles de acceso basados en roles (RBAC). Estas medidas se alinean con marcos como el **NIST Cybersecurity Framework** y la norma **ISO 27001** para gestionar riesgos y cumplir requisitos regulatorios y contractuales.

2. Gobierno e infraestructuras críticas.

Las instituciones gubernamentales y las infraestructuras críticas (como plantas de energía, sistemas de agua, transporte y telecomunicaciones) dependen en gran medida de la seguridad computacional para mantener su funcionamiento seguro y continuo frente a amenazas cibernéticas cada vez más sofisticadas.

- **Centros de Operaciones de Seguridad (SOC)**

- Los gobiernos y agencias estatales trabajan SOC que funcionan las 24hrs del día los 7 días a la semana

1. Estos centros están encargados de monitorear, detectar, analizar y responder a incidentes de seguridad en tiempo real.
2. Utilizan tecnologías avanzadas como SIEM (Security Information and Event Management), inteligencia artificial y análisis de comportamiento para anticipar ataques o anomalías en las redes.


- **Criptografía Certificada – FIPS 140-3**

- **Criptografía:** es una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes (resultado de aplicar una función matemática (llamada función hash) que convierte una entrada de datos (texto, archivo, contraseña, etc.) en una cadena corta de caracteres alfanuméricos de longitud fija.) y firmas.
- Para proteger la confidencialidad e integridad de la información clasificada o sensible, se exige el uso de criptografía conforme al estándar FIPS 140-3 (Federal Information Processing Standard).
 1. Este estándar regula el uso de módulos criptográficos aprobados para proteger datos en tránsito y en reposo.
 2. Es obligatorio en agencias federales de EE. UU. y recomendado en organismos internacionales que manejan datos sensibles.
- **Controles de Seguridad – NIST SP 800-53**
 - Según secureframe (2024), el estándar NIST SP 800-53 es un estándar creado por los Estados Unidos por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) en el cual permite a organizaciones a diseñar y administrar sus sistemas de seguridad de la información, y, en adición, a cumplir con la Ley de Modernización de la Seguridad de la Información Federal (FISMA, por sus siglas en inglés).
 - El marco NIST SP 800-53 proporciona un catálogo completo de controles de seguridad y privacidad que deben aplicarse a sistemas de información federales, especialmente aquellos que manejan infraestructura crítica.
 - Dentro de los Controles NIST 800-53 se encuentran las siguientes 20 familias de controles (**Para más información:** <https://secureframe.com/es-es/blog/nist-800-53-compliance>):
 1. Control de acceso (**AC**)
 2. Conciencia y capacitación (**AT**)

3. Auditoría y responsabilidad **(AU)**
 4. Evaluación, autorización y monitoreo **(CA)**
 5. Gestión de configuración **(CM)**
 6. Planificación de continuidad **(CP)**
 7. Identificación y autenticación **(IA)**
 8. Respuesta a incidentes **(IR)**
 9. Mantenimiento **(MA)**
 10. Protección de medios **(MP)**
 11. Protección física y ambiental **(PE)**
 12. Planificación **(PL)**
 13. Gestión de programas **(PM)**
 14. Seguridad del personal **(PS)**
 15. Procesamiento y transparencia de datos **(PT)**
 16. Evaluación de riesgos **(RA)**
 17. Adquisición de sistemas y servicios **(SA)**
 18. Protección de sistemas y comunicaciones **(SC)**
 19. Integridad de sistemas e información **(SI)**
 20. Gestión de riesgos en la cadena de suministro **(SR)**
- **Protección de sistemas de control industrial (ICS)**
 - Las infraestructuras críticas dependen de sistemas de control industrial (ICS) y SCADA (Supervisory Control and Data Acquisition) para operar maquinaria, redes eléctricas, sistemas de agua, etc.
 - Estos sistemas, al estar más conectados a redes IP modernas, son ahora más vulnerables a ciberataques.
 - Por eso, se implementan firewalls industriales, segmentación de redes OT/IT (Operative Technology, Information Technology), autenticación robusta, y protocolos seguros para garantizar su disponibilidad, integridad y confidencialidad.

3. Consumidores y dispositivos personales.

- **Autenticación Multifactor (MFA)**

- **La MFA** es una de las herramientas más efectivas para proteger cuentas personales frente a accesos no autorizados.
- Requiere al menos dos o más factores: algo que el usuario sabe (contraseña), algo que tiene (código en app o token) o algo que es (huella, rostro).
- Está presente en plataformas como Google, Microsoft, redes sociales, servicios bancarios y tiendas en línea.
 -  **Beneficio:** Incluso si una contraseña es robada, el atacante no podrá acceder sin el segundo factor.

- **Gestores de Contraseñas**

- Muchos usuarios reutilizan contraseñas o usan combinaciones débiles. Los **gestores de contraseñas** ayudan a:
 - Generar contraseñas únicas y complejas.
 - Almacenar de forma segura múltiples credenciales.
 - Autocompletar accesos sin que el usuario tenga que recordarlas todas.
- Ejemplos: Bitwarden, 1Password, LastPass, KeePass.
- **Beneficio:** Reduce el riesgo de ataques por fuerza bruta y reutilización de contraseñas filtradas.

- **Buenas prácticas y recomendaciones OWASP**

- La OWASP (Open Worldwide Application Security Project) promueve buenas prácticas para mejorar la seguridad tanto en el

desarrollo como en el uso de aplicaciones. A nivel de consumidor, estas prácticas ayudan a evitar:

- Phishing: correos o mensajes falsos que buscan robar credenciales.
 - Malware móvil: apps maliciosas o falsificadas que capturan datos del usuario.
 - Explotación de vulnerabilidades: en aplicaciones móviles desactualizadas o mal diseñadas.
- Recomendaciones clave para usuarios:
- Descargar solo desde tiendas oficiales (App Store, Google Play).
 - Revisar permisos antes de instalar apps.
 - Mantener el sistema operativo y apps actualizadas.
 - No hacer clic en enlaces desconocidos o sospechosos.

Tendencias de la seguridad computacional

Tendencia	Descripción	Indicadores del mercado / regulación
Zero Trust & ZTNA	Zero Trust es un modelo de seguridad donde tiene como principio en que ninguna persona o dispositivo a nivel externo o fuera de la red de una organización puede tener acceso para conectarse a sistemas o cargas de	Mercado ZTNA crecerá de \$41,28 mil M (2024) a \$52,18 mil M (2025) finance.yahoo.com .

Tendencia	Descripción	Indicadores del mercado / regulación
	<p>TI a menos que sea necesario. En combinación con ZTNA (Zero Trust Network Access) este modelo contiene una cantidad de tecnologías y funcionalidades que van a permitir el acceso seguro de usuario remotos a aplicaciones internas, dentro del Enterprise. Mas información en:</p> <p>https://www.akamai.com/es/glossary/what-is-zero-trust y https://www.zscaler.com/es/resources/security-terms-glossary/what-is-zero-trust-network-access</p> <p>“Nunca confíes, siempre verifica”. Sustituye la confianza implícita de la red interna por autenticación continua.</p>	
IA Generativa (ofensiva y defensiva)	<p>En ciberseguridad esta es una herramienta tanto usada por defensores como por atacantes en el cual impulsa modelos de lenguajes grandes (LLM) que permiten a equipos de seguridad a mejorar lo que serían políticas, detección de amenazas, gestión de</p>	<p>93 % de las organizaciones usa IA generativa; 34 % carece de políticas formales splunk.com.</p>

Tendencia	Descripción	Indicadores del mercado / regulación
	<p>vulnerabilidades y esta el estado de la seguridad en general. En cambio, puede ayudar a atacantes e intrusos a lanzar ataques más peligrosos y rápidos. Para más Información:</p> <p>https://www.zscaler.com/es/zpedia/what-generative-ai-cybersecurity</p> <p>Herramientas de <i>deepfake</i>, <i>phishing</i> automatizado y código malicioso; también detección basada en ML y SOAR.</p>	
Seguridad de la cadena de suministro	Ataques a dependencias de software/hardware de terceros (ej. SolarWinds).	Requisitos SBOM (Software Bill of Materials) en contratos gubernamentales de EE. UU.
Criptografía pos-cuántica	La Criptografía post-cuántica (criptografía a prueba de cuántica) trata sobre algoritmos criptográficos (muchas veces algoritmos de clave pública) que permiten una seguridad robusta ante ataques criptoanalíticos por parte de un ordenador o una maquina cuántica.	Directivas gubernamentales de migración antes de 2030.

Tendencia	Descripción	Indicadores del mercado / regulación
	Algoritmos resistentes a la computación cuántica (NIST: CRYSTALS-Kyber, Dilithium).	
Regulación acelerada	<p>La directiva NIS2 de la UE exige notificar brechas <i>críticas</i> en < 72 h imperva.com. El incumplimiento de esta regulación podría costarles a compañías grandes un total de hasta 10,000,000 de euros o hasta el 2% del volumen del negocio anual.</p> <p>(¿Qué es NIS? NIS es una directiva que trabaja con sistemas de redes y sistemas de información en el cual tiene como propósito proporcionar medidas legales para aumentar el nivel de ciberseguridad en la Unión Europea, Mendoza (2016))</p>	

Relación con Otros Conceptos

- La **tríada CIA** se aplica tanto en el desarrollo seguro de sistemas —como el control de acceso, la validación de datos y los respaldos— como en hábitos personales del día a día, como el uso de contraseñas robustas y copias de seguridad.

- El modelo **Zero Trust** orienta tanto la programación segura —por ejemplo, validando cada entrada del usuario— como nuestras prácticas digitales cotidianas, al usar autenticación multifactor y limitar el acceso innecesario.
- Las regulaciones como **GDPR** y **NIS2** demandan una responsabilidad ética y técnica que afecta tanto a los desarrolladores —al diseñar sistemas que protejan la privacidad— como a los usuarios, quienes tienen derecho a saber cómo se manejan sus datos.
- Las **tendencias actuales**, como la inteligencia artificial generativa, la criptografía pos-cuántica y los ataques a la cadena de suministro, influyen directamente en la forma en que se programa, se prueban los sistemas y se toman decisiones sobre qué tecnología usamos y cómo la protegemos.

Resumen de la Lección

Definimos la seguridad computacional como la protección sistemática de la confidencialidad, integridad y disponibilidad de los activos digitales. Su relevancia abarca pérdidas financieras multimillonarias, riesgos regulatorios y repercusiones sociales. La ciberseguridad se aplica desde dispositivos personales hasta infraestructuras críticas, guiada por marcos como NIST CSF. Finalmente, tendencias como Zero Trust, IA generativa, seguridad de la cadena de suministro, criptografía pos-cuántica y nuevas regulaciones moldean un panorama dinámico que exige adaptación continua.

Actividad de la Lección

Taller Amenaza–Control (30 min en clase + 1 h fuera):

1. Forme equipos de tres estudiantes y elija un escenario (p. ej., *e-commerce*, *smart-home*, *hospital*).
2. Identifique una amenaza emergente ligada a una tendencia (p. ej., deepfake + phishing).

3. Modele el impacto sobre CIA y proponga al menos dos controles alineados con Zero Trust o IA defensiva.
4. Entregue un resumen (infografía o diapositiva) con amenaza, impacto, controles y referencias.

Entrega: PDF o PPT subido al LMS antes de la próxima clase.

Referencias Adicionales

- Pfleeger, C. P., Pfleeger, S. L., & Coles-Kemp, L. (2023). *Security in Computing* (6.^a ed.). Addison-Wesley.
- Bishop, M. (2018). *Computer Security: Art and Science* (2.^a ed.). Addison-Wesley.
- Statista. "Expected Cost of Cybercrime until 2028" (2024).
- GlobeNewswire. "Zero Trust Network Access (ZTNA) Industry Report 2025" (19 jun 2025).
- Splunk & ESG. *State of Security 2024: The Race to Harness AI* (30 abr 2024).
- Imperva. *Understanding NIS2 Reporting Requirements* (19 abr 2024).
- ¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS. (n.d.). Amazon Web Services, Inc. <https://aws.amazon.com/es/what-is/cybersecurity/>
- ¿Qué es la criptografía? - Explicación sobre la criptografía - AWS. (n.d.). Amazon Web Services, Inc. <https://aws.amazon.com/es/what-is/cryptography/>