CIBERSEGURIDAD

Elaborado por: Orea Juárez Daniel y Licea Trujeque Valentina
CFLB: TIC
Instituto de la Veracruz
Orizaba, Ver. A 04 de julio del 2025

Introducción

Vivimos en una era digital, caracterizada por una interconectividad sin precedentes. Prácticamente todas nuestras actividades cotidianas, dependen directa o indirectamente del acceso a internet y al uso de tecnologías digitales. Esta dependencia tecnológica ha revolucionado la forma en que vivimos, facilitando múltiples procesos, aumentando la productividad y permitiendo un acceso casi instantáneo a la información. Sin embargo, junto con estos avances, han surgido nuevas vulnerabilidades y amenazas que afectan tanto a individuos como a organizaciones e incluso a gobiernos.

En este escenario, la ciberseguridad emerge como una disciplina clave para la protección de la información, los sistemas informáticos y las redes digitales. Su función principal es prevenir, detectar y responder a incidentes que comprometan la confidencialidad, integridad o disponibilidad de los datos. La ciberseguridad no solo busca evitar ataques maliciosos, sino también garantizar la privacidad, el buen funcionamiento de los servicios digitales y la confianza del usuario en el entorno digital.

El auge de los delitos cibernéticos, ha puesto de manifiesto la urgente necesidad de fortalecer la seguridad digital en todos los niveles. Ya no se trata de un problema exclusivo de los expertos en tecnología; hoy en día, la ciberseguridad nos involucra a todos: estudiantes, trabajadores, empresarios, funcionarios públicos y cualquier persona que utilice un dispositivo con conexión a internet.

Desarrollo

La ciberseguridad, también conocida como seguridad informática, se define como el conjunto de técnicas, prácticas, herramientas y políticas destinadas a proteger los sistemas digitales, redes de comunicación y datos frente a accesos no autorizados, ataques maliciosos o pérdidas accidentales. Su principal objetivo es salvaguardar tres principios fundamentales de la información: la confidencialidad (que solo las personas autorizadas accedan a los datos), la integridad (que los datos no sean alterados o manipulados sin autorización) y la disponibilidad (que los datos y servicios estén accesibles cuando se necesiten).

Hoy en día, las amenazas cibernéticas evolucionan constantemente. Algunas de las más comunes son:

- Malware: software malicioso diseñado para dañar o controlar dispositivos.
- Phishing: correos o sitios falsos que suplantan identidades para robar información confidencial.
- Ransomware: secuestra datos mediante cifrado y exige un rescate económico para liberarlos.
- DDoS: ataques de denegación de servicio que sobrecargan servidores hasta inutilizarlos.

Estas amenazas no solo afectan a grandes empresas o instituciones, sino también a usuarios comunes que, sin saberlo, pueden convertirse en víctimas de ataques. La educación digital es clave para reconocer los riesgos y adoptar medidas básicas de protección, como utilizar contraseñas fuertes y únicas, activar la autenticación en dos pasos, mantener actualizado el

software, no descargar archivos sospechosos y ser cuidadoso con los enlaces que se reciben por correo o redes sociales.

En el ámbito corporativo e industrial, la ciberseguridad adquiere una dimensión aún más compleja. Con la expansión de la Industria 4.0, las empresas deben proteger no solo su información financiera, sino también sus sistemas de control y producción. Un ataque en este entorno puede paralizar una planta entera, generar enormes pérdidas económicas o, incluso, poner en riesgo la seguridad de las personas.

La ciberseguridad, entonces, se convierte en un componente esencial del funcionamiento moderno. No se trata solo de instalar un antivirus, sino de implementar una cultura de seguridad donde todos los usuarios estén capacitados, informados y preparados para prevenir o responder ante posibles amenazas digitales.

Conclusión

En la actualidad, la ciberseguridad se ha consolidado como un pilar esencial para la vida digital. La enorme cantidad de datos que generamos, compartimos y almacenamos diariamente nos convierte en blancos potenciales de diversos tipos de ataques cibernéticos. En este contexto, proteger nuestra información personal, laboral, financiera y social se ha vuelto una necesidad urgente que requiere compromiso, conciencia y acción tanto individual como colectiva.

Ya no basta con confiar únicamente en las herramientas tecnológicas; es necesario que cada persona desarrolle una actitud crítica y preventiva frente al uso de internet. La educación en seguridad digital debe formar parte de la formación básica desde edades tempranas, igual que otras competencias clave para la vida moderna. Solo una sociedad informada podrá resistir y responder adecuadamente ante las amenazas emergentes en el ciberespacio. Asimismo, las organizaciones, instituciones educativas, empresas y gobiernos tienen la responsabilidad de implementar políticas de ciberseguridad sólidas y actualizadas, que incluyan auditorías periódicas, planes de contingencia y protocolos de respuesta ante incidentes. La protección de infraestructuras críticas, servicios públicos y sistemas financieros depende en gran parte de estos esfuerzos.

Por otro lado, el desarrollo económico y tecnológico de un país también está vinculado a su capacidad para garantizar la seguridad digital de sus ciudadanos y empresas. Sin confianza en los sistemas digitales, difícilmente puede haber inversión, innovación ni progreso. Por ello, la ciberseguridad es también una cuestión de soberanía, competitividad y bienestar social. Construir un entorno digital más seguro es tarea de todos.

Referencias:

 Instituto Nacional de Ciberseguridad (INCIBE). (2023). *Guía de ciberseguridad para ciudadanos*. Gobierno de España. https://www.incibe.es/protege-tu-empresa/guias/ciudadanos

 Organización de los Estados Americanos (OEA). (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://www.oas.org/es/sms/cicte/docs/Informe-Ciberseguridad-ESP.pdf

 Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). (2022). *Consejos de ciberseguridad para evitar fraudes electrónicos*. Gobierno de México. https://www.gob.mx/condusef/articulos/consejos-de-ciberseguridad

 Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI). (2021). *Ciberseguridad en la era digital: Retos y recomendaciones*. https://www.canieti.org/

 Universidad Nacional Autónoma de México (UNAM), Instituto de Investigaciones Jurídicas. (2022). *Protección de datos personales y ciberseguridad en México*. https://archivos.juridicas.unam.mx/www/bjv/libros/14/6629/11.pdf

 Deloitte México. (2023). *Tendencias en ciberseguridad 2023*. https://www2.deloitte.com/mx/es/pages/risk/articles/tendencias-en-ciberseguridad.html