

## **Rangkuman**

### **Webinar Minggu 2 – Pengantar Teknologi Informasi**

Nama: Harsya Brahmantyo Wibowo

NIM: 103032430021

Kelas: IT-48-02

Webinar ini membuka gambaran besar tentang bagaimana teknologi berkembang dari era mekanisasi hingga kolaborasi manusia dan AI pada Industri 5.0. Komputasi dipahami sebagai aktivitas berorientasi tujuan untuk mencipta dan memanfaatkan komputer dalam memecahkan masalah nyata. Dari sini, TI (Information Technology) diposisikan bukan sekadar “payung” teknologi, melainkan fungsi strategis yang memilih, mengintegrasikan, dan mengelola solusi-mulai dari perangkat keras dan lunak, jaringan, hingga layanan-agar proses bisnis menjadi lebih cepat, paralel, dan akurat.

Materi kemudian mengurai komponen sistem TI: hardware, software, firmware, infoware (prosedur, pedoman, regulasi), dan brainware (pengguna akhir, spesialis TI, manajer). Pemisahan ini menegaskan bahwa keberhasilan implementasi tidak hanya bertumpu pada alat, tetapi juga pada tata kelola dan kompetensi manusia. Perbedaan data dan informasi turut ditegaskan: data adalah bahan mentah, sementara informasi adalah data yang sudah diproses sehingga bermakna dan bernilai untuk pengambilan keputusan-dalam beragam wujud seperti teks, audio, visual, hingga bentuk elektronik yang ditransmisikan.

Bagian keamanan informasi menjadi sorotan melalui kerangka CIA: Confidentiality, Integrity, dan Availability. Kerahasiaan memastikan hanya pihak berwenang yang dapat mengakses; integritas menjamin data tetap utuh, akurat, dan terlindungi dari perubahan tidak sah; ketersediaan memastikan sistem dan informasi siap digunakan saat dibutuhkan. Ketiganya tidak boleh dilihat secara terpisah: praktik yang baik menyeimbangkan kontrol akses, enkripsi, audit trail, ketahanan infrastruktur, dan rencana respons insiden. Kerangka People–Process–Technology melengkapi perspektif ini-edukasi pengguna, proses yang jelas (identifikasi, proteksi, deteksi, respons, pemulihan), serta teknologi perlindungan (firewall, anti-malware, keamanan email/DNS, logging) harus berjalan serempak.

Terakhir, topik Internet of Things (IoT) mengaitkan otomasi dan konektivitas dengan tantangan keamanan. Karena banyak perangkat IoT beroperasi tanpa interaksi manusia dan sering terhubung langsung ke internet, permukaan serangannya meluas. Pendekatan “secure-by-design” direkomendasikan: hardening perangkat, segmentasi jaringan, autentikasi kuat, enkripsi ujung-ke-ujung, pemantauan berkelanjutan, serta pembaruan

berkala. Keseluruhan materi menegaskan bahwa informasi adalah aset organisasi; keberhasilan transformasi digital menuntut fondasi komputasi yang kuat, tata kelola TI yang matang, dan budaya keamanan yang konsisten dari manusia, proses, hingga teknologi.