

La Rivoluzione Digitale: Trasformazione e Sfide nell'Era 4.0

Nel 1985, Porter e Millar profetizzavano come l'Information Technology stesse permeando ogni punto della catena del valore, trasformando radicalmente i processi lavorativi. Oggi, la Digital Revolution trova le sue radici nella terza rivoluzione industriale, ma ne amplifica portata e impatto in modo drammatico.

La digitalizzazione ha reso necessario un ripensamento completo di tecnologie, processi e governance aziendale. Il cambiamento non riguarda solo i processi operativi, ma si estende all'invenzione di nuovi modelli di business digitali che ridefiniscono il modo in cui le aziende creano e forniscono valore ai clienti.

Le Cinque Diretrici dell'Industria 4.0



Gestione Dati e Connettività

Sensori, Internet of Things, tecnologia cloud e blockchain per potenza di calcolo e connettività avanzata



Analisi e Intelligenza Artificiale

Big data, analisi avanzate, intelligenza artificiale e automazione del lavoro della conoscenza



Interazione Uomo-Macchina

Realtà virtuale e aumentata, robotica avanzata e sistemi di automazione intelligente



Produzione Avanzata

Manifattura additiva, stampa 3D e utilizzo di energie rinnovabili nei processi produttivi



BIM e Digital Twin

Miglioramento della fase di progettazione, realizzazione e manutenzione. Building Information Modeling, CIM, digital-twin, droni e nanotecnologie per progettazione e manutenzione

Modello di Business

Il modello di business (in inglese business model) in sintesi, rappresenta il modo in cui un'organizzazione crea, distribuisce e cattura valore.

Secondo la letteratura, un modello di business descrive la logica attraverso cui un'impresa opera, ovvero come:

- Crea valore (offerta di prodotti o servizi utili per il cliente);
- Lo distribuisce (canali, relazioni con clienti e partner);
- Ne cattura una parte (ricavi e profitti);

Principali definizioni secondo gli autori

(Autore, Definizione, Fonte)

Peter Drucker (1954), **Il modello di business definisce come un'azienda "si guadagna da vivere".**, The Practice of Management

Timmers (1998), **Un'architettura per il prodotto, il servizio e i flussi di informazione, che descrive gli attori coinvolti e i benefici economici derivanti.**

Amit e Zott (2001), **La struttura dei contenuti, la governance e i flussi di transazione progettati per creare valore attraverso opportunità di business.**

Magretta (2002), **Il modello di business racconta la storia di come un'impresa funziona: chi è il cliente, cosa valuta, e come l'azienda può offrire valore a costi appropriati.**

Osterwalder e Pigneur (2010), **Una rappresentazione logica di come un'organizzazione crea, distribuisce e cattura valore.**

Modello di Canvas

Uno dei modelli più noti è il Business Model Canvas (Osterwalder & Pigneur, 2010), che individua 9 blocchi fondamentali:

- Segmenti di clientela
- Proposta di valore
- Canali di distribuzione
- Relazioni con i clienti
- Flussi di ricavi
- Risorse chiave
- Attività chiave
- Partner chiave
- Struttura dei costi

Internet of Things e Robotica nelle Costruzioni

Internet of Things (IoT)

L'IoT comprende dispositivi con capacità di autoidentificazione, localizzazione, diagnosi, acquisizione ed elaborazione dati. Nei grandi progetti infrastrutturali, queste tecnologie trovano applicazione in:

- Monitoraggio continuo di manufatti e strutture
- Sistemi di sicurezza avanzati
- Monitoraggio ambientale in tempo reale
- Gestione predittiva della manutenzione



Robotica Applicata

La robotica estende l'utilità della tecnologia alla fase di costruzione attraverso:

1. Droni per sorveglianza, rilevamento topografico e ispezione strutturale
2. Robot da costruzione per muratura, pittura, carico e operazioni di bulldozer
3. Camion autonomi per gestione magazzino, forniture e materiali
4. Escavatori a guida autonoma per scavi e movimentazione terra



Tecnologie Emergenti: Stampa 3D ed E-Commerce

Stampe 3D nel Settore Costruzioni

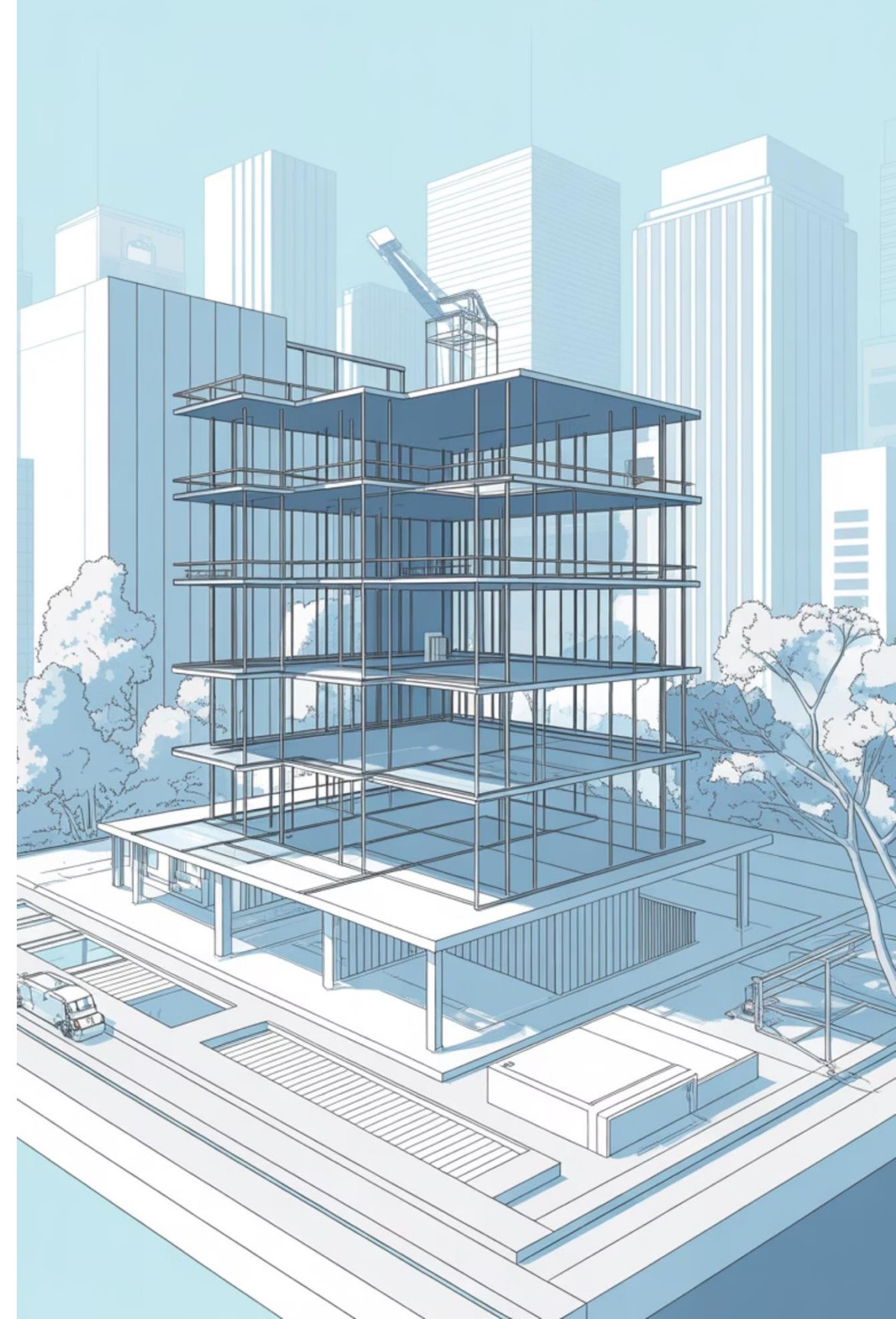
Le tecnologie di stampa 3D si utilizzano diffusamente per prototipare e produrre componenti singoli, rivoluzionando i processi di costruzione:

- Realizzazione rapida di strumenti e prodotti da cantiere
- Prototipazione di elementi architettonici complessi
- Produzione on-demand di componenti personalizzati
- Riduzione degli sprechi di materiale
- Accelerazione dei tempi di produzione

E-Commerce B2B

Le transazioni virtuali trasformano l'approvvigionamento:

- Acquisto e vendita online di materiali
- Ordini attraverso piattaforme dedicate
- Pagamenti digitali sicuri
- Consegna tramite canali tradizionali o elettronici



Cloud Computing e Blockchain: Nuovi Paradigmi

Cloud Computing

Servizi IT online su richiesta che includono archiviazione e gestione dati utilizzando risorse fisiche e virtuali condivise. Gli utenti accedono ai servizi da qualsiasi dispositivo e posizione, garantendo flessibilità e scalabilità senza precedenti.

Blockchain

Tecnologia che garantisce immutabilità del registro, tracciabilità delle transazioni e sicurezza crittografica. Applicazioni emergenti includono criptovalute, smart-contract per pagamenti automatici, e piattaforme che creano fiducia attraverso trasparenza e sicurezza.

Intelligenza Artificiale

Disciplina che integra filosofia, matematica, psicologia e scienze cognitive. Collegata ai big data nel cloud, elabora informazioni in tempo reale tramite algoritmi avanzati per controllo, monitoraggio continuo e capacità predittive nei diversi ambiti applicativi.

BIM: Building Information Modeling

Il BIM rappresenta la rappresentazione digitale di caratteristiche fisiche e funzionali di un oggetto, nato dalla volontà di promuovere collaborazione tra progettisti, interoperabilità dei software, integrazione tra processi e sostenibilità.

01

Progettazione Collaborativa

Integrazione in un unico modello delle informazioni architettoniche, strutturali, impiantistiche, energetiche e gestionali

02

Utilizzo Multidisciplinare

Impiantisti, ingegneri strutturisti, architetti, costruttori, montatori e collaudatori lavorano sullo stesso modello

03

Modello Tridimensionale Integrato

Racchiude informazioni su volume, dimensioni, materiali, aspetto e caratteristiche tecniche senza perdite nella comunicazione

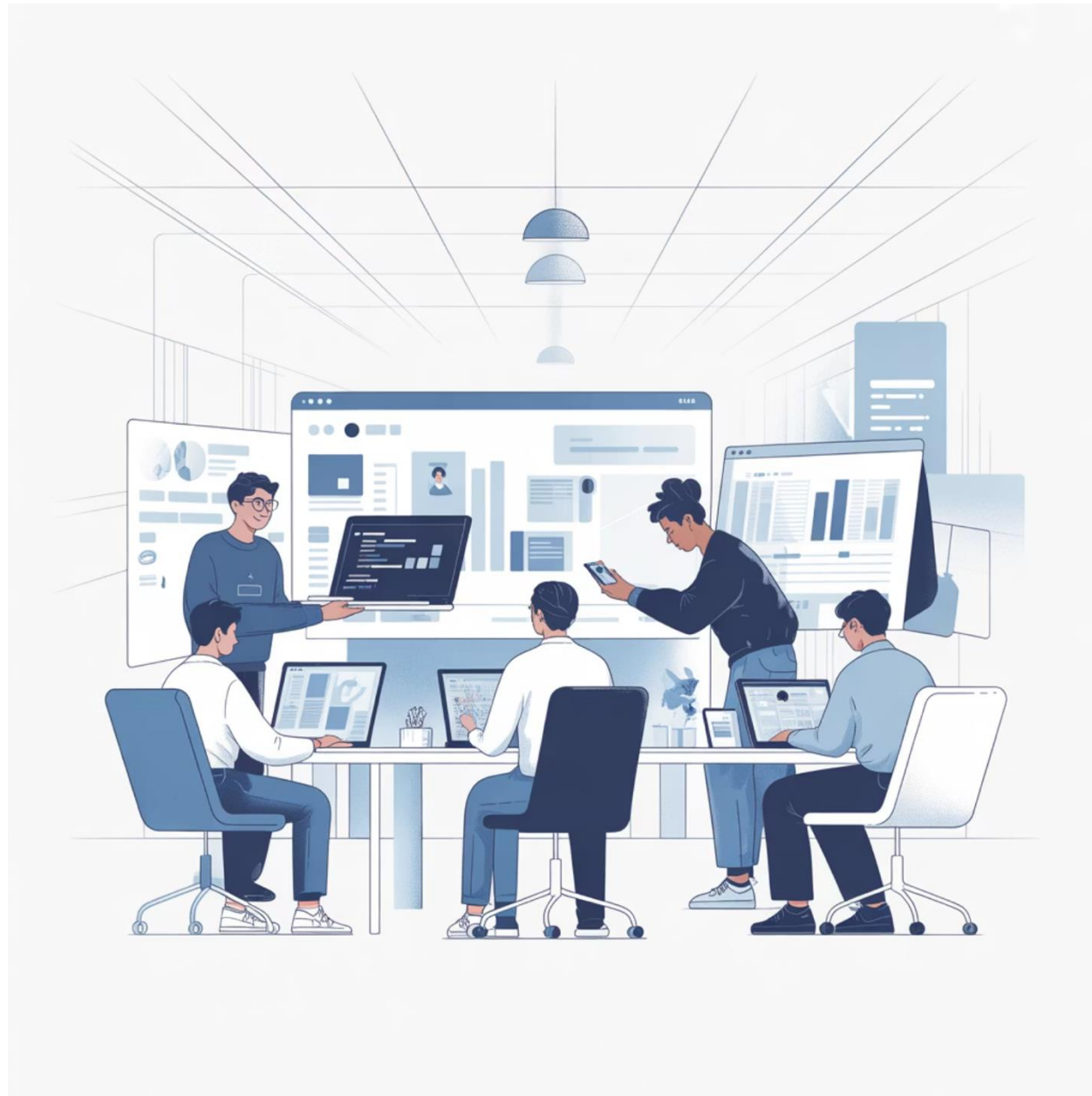
04

Vantaggi Operativi

Maggiore efficienza, meno errori, riduzione tempi morti e costi, massima condivisione informazioni e controllo puntuale del progetto



Il Digital Mismatch: Sfida delle Competenze



Il Divario Crescente

Il disallineamento tra domanda e offerta di competenze digitali (*digital mismatch*) è in ulteriore crescita rispetto agli anni precedenti e rappresenta la maggiore criticità nella realizzazione dei piani di innovazione delle imprese.

A tutte le professioni, anche quelle meno apparentemente coinvolte nello sviluppo tecnologico, sarà richiesta una riconversione in chiave tecnologica delle competenze. L'emergenza pandemica ha ulteriormente aumentato questo divario, anche fra Paesi con diversi livelli di sviluppo economico e di accesso alle nuove tecnologie.

Nuove Figure Professionali

L'innovazione tecnologica richiede l'inserimento di figure professionali emergenti:

- **AI Expert:** specialisti in intelligenza artificiale
- **Data Scientist:** analisti di big data
- **AI Business Development Manager:** gestori dello sviluppo business basato su IA
- **Digital Transformation Manager:** responsabili della trasformazione digitale

Le Cinque Insidie della Digitalizzazione secondo Porter

Porter e Heppelmann hanno evidenziato cinque insidie critiche da evitare quando si sviluppano offerte avanzate basate su tecnologie emergenti:



Caratteristiche Non Richieste

Offerta di prodotti con funzionalità opzionali che i clienti non percepiscono come valore reale e non sono disposti a pagare



Sottovalutazione Rischi Sicurezza

Tendenza a minimizzare i rischi per la sicurezza e la privacy. I prodotti intelligenti e connessi rappresentano vie di accesso ai sistemi aziendali e dati sensibili



Ritardo Tecnologico

Incapacità di tenere il passo con i progressi tecnologici rispetto ai concorrenti "maturi" digitalmente



Entrata Tardiva

Late entry che riduce il vantaggio competitivo rispetto ai concorrenti che acquisiscono e analizzano dati in anticipo



Sopravvalutazione Capacità Interne

Sottovalutazione delle nuove tecnologie, abilità e competenze richieste per comprendere pienamente la trasformazione digitale

Digital ERM: Enterprise Risk Management nell'Era Digitale

La nozione di ERM si evolve in Digital ERM (D-ERM), richiedendo un esame sistematico dei rischi emergenti che impattano su temi strategici, operativi, finanziari e di compliance.

1. Rischi di Informazione

- Cybersecurity e privacy
- Gestione emergenze
- Data life-cycle management
- Data quality and assurance
- Normative e compliance

Riguardano danni da perdita di dati o uso improprio: sicurezza tecnica, gestione identità, controlli accessi, sicurezza di rete.

2. Rischi Tecnologici

- Project-delivery risk
- Resilienza sistemi e infrastrutture
- Data management
- Integrazione tecnologica

Attengono al rischio di interruzione o guasto dei sistemi. Richiedono progettazione di resilienza e gestione operazioni quotidiane per prevenire perdite.

3. Rischi Protezione Clienti

- Trasparenza utilizzo dati
- Errori identificazione clienti
- Comunicazione multicanale
- Vendita attraverso canali diversificati

Danni ai clienti attraverso cattiva comunicazione o prodotti inappropriati danneggiano gravemente la reputazione aziendale.

Rischi Emergenti Globali secondo il WEF

1

Esiti Avversi Progressi Tecnologici

Conseguenze negative intenzionali o non intenzionali dei progressi tecnologici su individui, imprese, ecosistemi ed economie per improprio utilizzo di intelligenza artificiale

2

Danneggiamento Infrastrutture Informatiche

Deterioramento, saturazione o chiusura di infrastrutture fisiche e digitali critiche come risultato di dipendenza sistemica da reti e tecnologie informatiche

3

Disuguaglianza Digitale

Accesso frammentato e diseguale a reti e tecnologie digitali critiche, tra e all'interno dei paesi, per capacità di investimento ineguali e mancanza di competenze

4

Concentrazione Potere Digitale

Concentrazione di risorse, capacità e conoscenze digitali critiche da parte di un numero ridotto di individui, aziende o stati

5

Fallimento Sicurezza Informatica

Crimini informatici sempre più sofisticati e frequenti, con perturbazioni economiche, perdite finanziarie, tensioni geopolitiche e instabilità sociale

6

Fallimento Governance Tecnologica

Mancanza di normative, istituzioni o regolamenti accettati globalmente per l'uso di reti e tecnologie digitali critiche

Cyberspazio e Cybersecurity: Il Quinto Dominio

Nel settembre 2010, il vice-segretario della Difesa americano William J. Lynn III ha pubblicamente qualificato il cyber-spazio come il **quinto dominio della conflittualità** dopo terra, mare, aria e spazio.

L'Attacco all'Estonia (2007)

Nell'aprile 2007, l'Estonia fu oggetto di una serie di attacchi DDoS (Distributed Denial of Service) capaci di paralizzare quasi completamente l'intera infrastruttura informatica del Paese. Questo evento ha acceso i riflettori internazionali sulle tematiche di:

- **Cyber-crime:** criminalità informatica organizzata
- **Cyber-intelligence:** spionaggio elettronico
- **Cyber-warfare:** guerra informatica tra stati

Stuxnet: La Prima Cyber-Arma

Il malware Stuxnet rappresenta l'unica vera cyber-armata attualmente conosciuta: un software capace di danneggiare fisicamente l'infrastruttura critica di una nazione sfruttando i sistemi informatici che la governano.

Procurement Tradizionale vs Digitale

Approccio Tradizionale: Limitazioni Critiche

Il processo tradizionale di procurement, gestito ante digitalizzazione, presenta notevoli limitazioni che impattano negativamente sull'efficienza operativa:

Carente Governo della Spesa

Visibilità della spesa focalizzata per singola funzione, senza una visione integrata e complessiva

Processi Seriali Prolungati

Approvazioni seriali e frammentazione delle responsabilità che rallentano le decisioni

Scarso Coinvolgimento Fornitori

Limitata condivisione e collaborazione con i fornitori nella catena del valore

Attività Manuali e Errori

Verifiche manuali con elevato rischio di errori e costi amministrativi significativi

Scarsa Tracciabilità

Difficoltà nel tracciare il processo in tutte le sue fasi e nell'identificare criticità

Digital Procurement: Source-to-Pay (S2P)

Il D-Procurement rivoluziona le modalità di gestione attraverso un sistema integrato che copre l'intero ciclo dalla identificazione delle fonti al pagamento.

1

Source-to-Contract (S2C)

Upstream - Strategico

- Monitoraggio e analisi della spesa
- Governance processo negoziale
- Analisi e valutazione fornitori
- Gestione rischi e performance
- D-sourcing e D-Catalog

2

Procure-to-Pay (P2P)

Downstream - Operativo

- Selezione da cataloghi online
- Emissione ordini automatica
- Gestione entrata merce
- Ricezione fatture elettroniche
- Pagamento fornitori

3

Integrazione ERP

Sistema Unificato

- Contabilità integrata
- Controllo di gestione
- Gestione magazzini
- MRP e produzione
- Vendite e distribuzione



Vantaggi del Digital Procurement



Multicanalità e Accessibilità

Informazioni fruibili in multicanalità e via web browser da qualsiasi dispositivo e posizione, garantendo flessibilità operativa senza precedenti



Tracciabilità Completa

Tracciabilità di tutte le attività svolte dall'acquirente e dal fornitore, garantendo trasparenza totale in caso di controversie e audit



Disponibilità Persistente

Continua e persistente disponibilità dei dati e delle informazioni gestite, rilevante per disaster recovery e business continuity

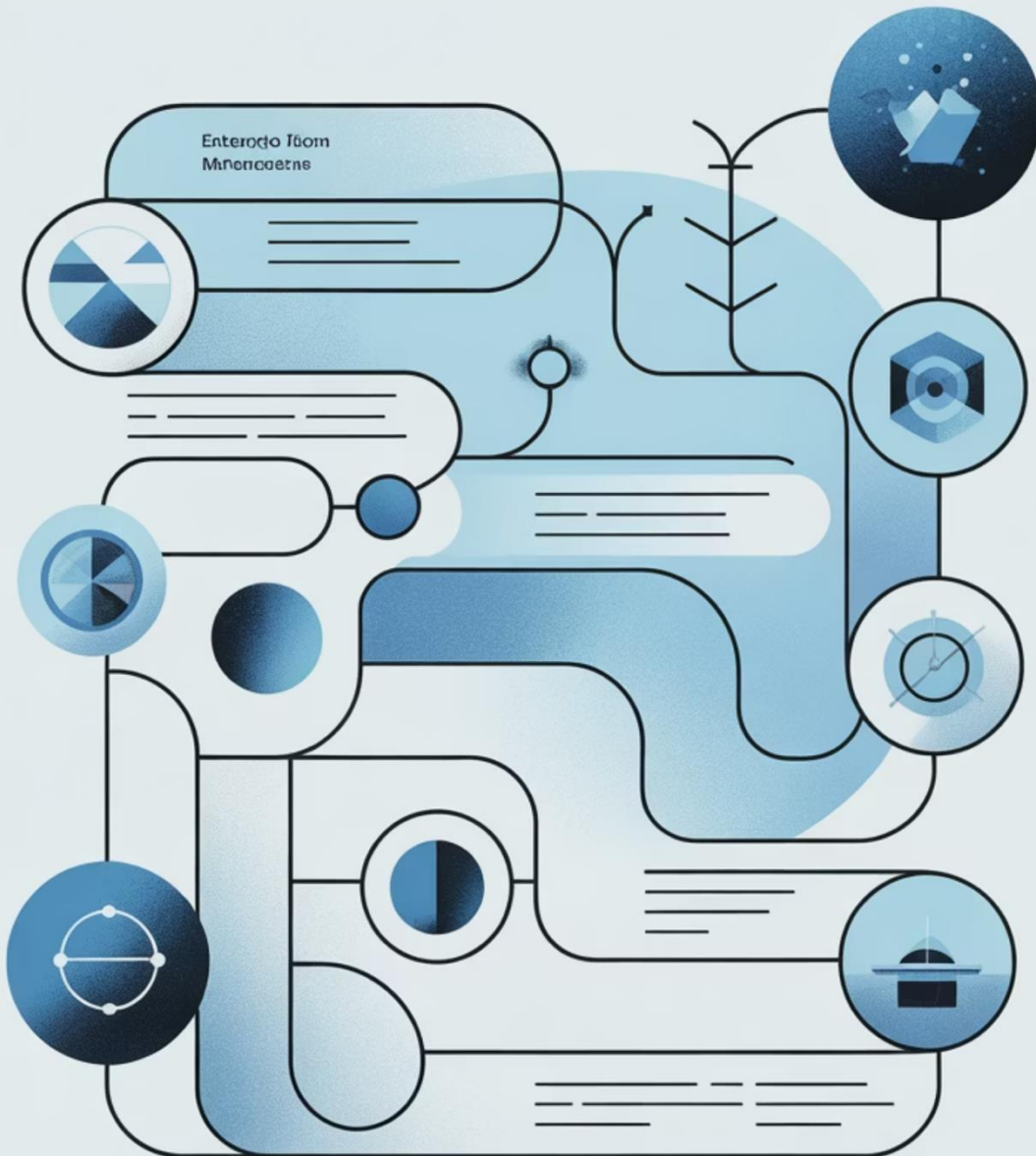


Sicurezza e Continuità

Garanzie di sicurezza informatica, tracciabilità delle operazioni, trasparenza nei processi e continuità operativa del business

📌 **Nota Importante:** A forti opportunità si accompagnano rischi emergenti. È necessario che le funzioni di controllo interno adattino i loro modelli di riferimento e si dotino di strumenti adeguati a fronteggiare le sfide dell'era digitale.

Enterprise Risk Management Framework



Framework di Controllo: IC 2013 ed ERM 2004/2017

Approccio Integrato ai Rischi Tecnologici

L'Internal Control-Integrated Framework (IC 2013) e l'Enterprise Risk Management-Integrated Framework (ERM 2004/2017) costituiscono la base per valutare e gestire efficacemente i rischi tecnologici.

I rischi tecnologici **non possono essere gestiti per "silos"** come problema di esclusiva pertinenza della funzione IT, ma richiedono la diffusione di una corretta cultura della information technology e della digitalizzazione in tutta l'organizzazione.

Componenti Essenziali

01

Informazione e Comunicazione

Base per svolgere il controllo interno sull'organizzazione

02

Monitoraggio Continuo

Valutazioni continue sul corretto funzionamento del sistema

03

Data Analytics

Utilizzo di sistemi avanzati di analisi dei dati per controllo e reporting

Cyber Resilience: I 6 Principi del WEF per il Board

Il World Economic Forum ha delineato sei principi-cardine che i Board devono seguire per supportare le organizzazioni nella Cyber-Resilienza:

1

Sicurezza come Strumento Strategico

Considerare la sicurezza informatica come enabler per la strategia aziendale, non solo come problema IT o compliance formale. Contribuisce al mantenimento del business e crea nuove opportunità di valore.

2

Comprendere i Driver Economici

Il processo decisionale richiede analisi delle tematiche economiche connesse ai cyber-rischi. Usare strumenti di analisi e pianificazione di scenario per considerare potenziali guadagni e perdite.

3

Allineare CR alle Esigenze Aziendali

Management e Board devono valutare come gestire efficacemente i cyber-rischi attraverso le leve del risk management: eliminazione, riduzione, accettazione, mitigazione o trasferimento.

4

Progettazione Organizzativa Adeguata

Garantire una governance interna che affronti la sicurezza informatica in logica di sistema integrato, con chiari KPI e integrazione delle pratiche di sicurezza.

5

Competenze ed Esperienze nel Board

Avvalersi di advisor esterni e competenze interne, aumentare la conoscenza di base degli amministratori mediante formazione, audit periodici e benchmarking indipendenti.

6

Resilienza Sistemica e Collaborazione

La cyber-resilienza richiede azione collettiva e partnership. Garantire piani efficaci di collaborazione con il settore pubblico e partecipazione a piattaforme di condivisione informazioni.

Continuous Auditing e Monitoring: Tecnologie Abilitanti

La trasformazione digitale implica cambiamenti radicali negli strumenti, modalità di lavoro e competenze richieste per il controllo interno. L'approccio vincente è di tipo preventivo: intercettare per tempo i rischi dotandosi di strumenti adeguati.

Audit Analytics

Procedure analitiche realizzate attraverso soluzioni informatiche per estrarre indicatori e statistiche dall'analisi di dati elettronici, gestionali e contabili. Impiegati in specifici audit limitati al singolo incarico.

Continuous Auditing

Raccolta di evidenze di audit e statistiche su processi, transazioni, controlli e sistemi informativi su base continuativa o con frequenza prestabilita. Test automatici incorporati nei sistemi che gestiscono le transazioni.

Continuous Monitoring

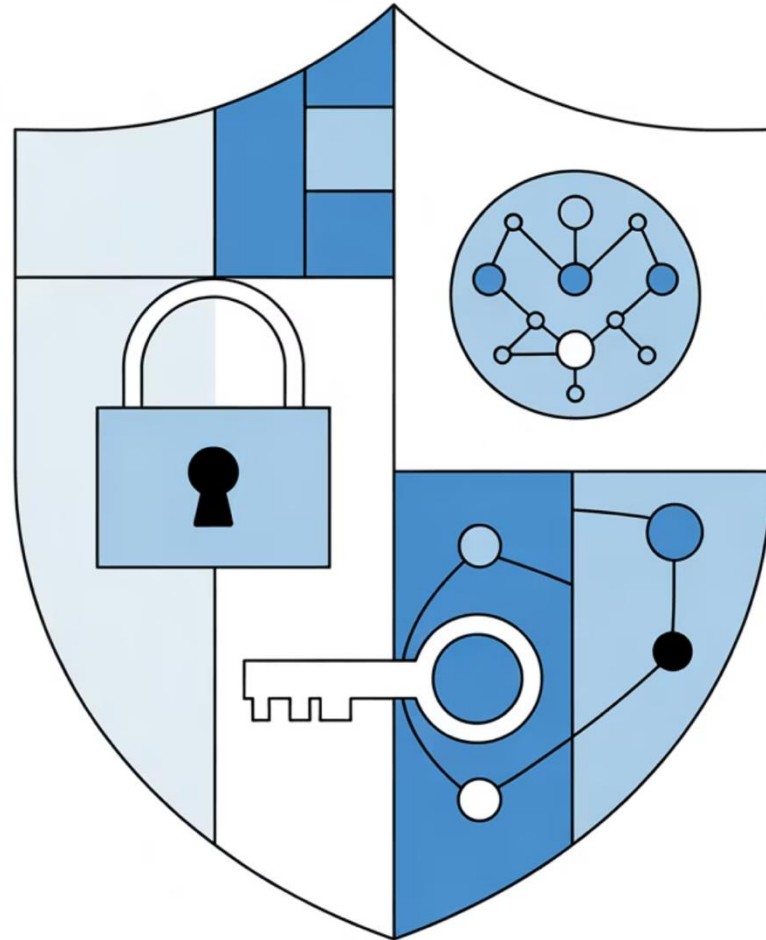
A cura del management attraverso sistemi di reporting del controllo di gestione, contabile e industriale. Fornisce feedback continuo sull'andamento delle attività e su specifici rischi per l'assunzione di decisioni.

Data Analytics per il Procurement: Esempi Pratici

L'utilizzo di sistemi avanzati di analisi consente di implementare significativamente le capacità predittive e di controllo. Gli auditor definiscono come incrociare banche dati su parametri specifici per intercettare tempestivamente possibili aree di rischio.

Validità Pagamenti	Pagamenti duplicati	Verifica identità/similarità: vendor, invoice, amount, account, data
Validità Fatture	Fatture duplicate	Verifica identità/similarità: vendor, invoice, type, amount, products, data
Esistenza Controparti	Pagamenti fraudolenti	Match dipendente-fornitore: name, address, phone, email, SSN/TaxID, bank account
Autorizzazione Acquisti	Frazionamento ordini	Identifica transazioni sotto soglia o verso stesso vendor che oltrepassano limiti
Modifiche Autorizzate	Modifiche non autorizzate	Audit trail modifiche vendor master, verifica autorizzazioni, monitoraggio key fields
Segregazione Funzioni	Conflitto di interessi	Verifica SOD tra chi crea OdA e chi approva, identifica eccezioni

GDPR e Protezione dei Dati Personali



Autorità Garante e DPO

L'Autorità Garante per la protezione dei Dati Personali controlla che i trattamenti siano conformi al Regolamento e prescrive le misure necessarie per svolgere correttamente il trattamento nel rispetto dei diritti fondamentali.

Particolare rilievo assumono i **Data Protection Officer (DPO)**, responsabili della protezione dei dati nel nuovo sistema basato su trasparenza e accountability.

Misure di Mitigazione

Per cautelarsi da violazioni di sicurezza dei dati personali (**data breach**) vanno poste in essere misure adeguate sia tecniche che organizzative.

General Data Protection Regulation

Il tema della protezione dei dati personali è divenuto sempre più importante con l'affermarsi delle tecnologie di trattamento e digitalizzazione. Ha notevoli valenze etiche per il rispetto dei principi di correttezza e trasparenza.

La legge sulla privacy (675/1996), poi disciplinata dal Codice (d.lgs. 196/2003), con il d.lgs. 101/2018 ha reso applicabile il **GDPR** europeo.

Reati Informatici e D.Lgs. 231/2001

L'articolo 24-bis del decreto 231 ha esteso la responsabilità amministrativa delle persone giuridiche agli enti per i delitti informatici commessi nel loro interesse o a loro vantaggio.

Falsità Documenti Informatici

Falsificazione di documenti informatici, detenzione e diffusione abusiva di codici di accesso

Danneggiamento Dati

Danneggiamento di informazioni, dati e programmi informatici con finalità illecite



Diffusione Programmi Dannosi

Distribuzione di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere sistemi informativi

Accesso Abusivo

Accesso non autorizzato a sistemi telematici o informatici per danneggiare informazioni, dati e programmi

📄 **Impatto della Digitalizzazione:** La trasformazione digitale ha fortemente amplificato la rischiosità dei reati informatici sia in termini di frequenza (ampliamento della platea dei potenziali autori) sia di gravità delle conseguenze. Le organizzazioni devono dotarsi di adeguati Modelli di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001.