MAPS
SHARING KNOWLEDGE

I QUADERNI DI **6MEMES**

ICT, INNOVAZIONE E GDPR.
Un punto di equilibrio tra la rapida evoluzione del mondo digitale e la protezione dei dati.

di Giulio Destri

INDICE DEI CONTENUTI

Introduzione

ICT è l'acronimo di Information Communication Technology, ossia **l'insieme delle nuove tecnologie in ambito informatico ed elettronico che consente di trattare e scambiare le informazioni in formato digitale**.

Esse sono alla base di una vera e propria rivoluzione tecnologica odierna non solo nel settore economico ed industriale ma anche nella vita di tutti i giorni, dove **l'ICT sta trasformando il modo in cui lavoriamo, viaggiamo, comunichiamo e viviamo.**

Un nuovo studio Assintel sulla digital transformation mondiale ed europea ha confermato, entro il 2020, una spesa in tale ambito in aumento del 60% e, in Iatalia, un aumento del 2% circa nei prossimi tre anni del settore IC.

La spinta innovativa, nel mercato, della digital transformation ha prodotto nuovi servizi decretando la nascita di profili professionali in grado di interpretare i

potenziali di sviluppo e di cambiamento. Nel 2016: *"sono stati più di 62.000 i posti di lavoro vacanti nel campo dell'Ict, un dato in aumento del 30% rispetto al 2015".*

Proprio nella richiesta di figure professionali, **una proiezione di Confindustria ha identificato cinque settori cruciali in cui l'occupazione offerta sarà probabilmente maggiore rispetto al numero di giovani preparati per quelle professioni: oltre all'industria meccanica, alimentare e chimica, ed al settore tessile, compare anche l'Information and Communication technology**.

La rapida evoluzione delle tecnologie correlate a internet e lo sviluppo dei servizi ICT ha avuto un profondo impatto non solo sulle nostre vite ma anche in ambito economico e politico. Tuttavia **collegarsi alla rete rende PC, smartphone e ogni wereables devices** (ossia dispositivo indossabile, come per esmpio lo smartwatch), con tutti i dati che essi contengono, **potenzialmente vulnerabili e soggetti ad attacchi di pirateria informatica.**

Le problematiche di sicurezza, diretta ed indiretta, legate agli strumenti IT, rende necessaria la prevenzione di tutto questo che si può

attuare solo a livello progettuale di un servizio IT, diretto o parte di un sistema industriale, domotico o di internet delle cose. **Questa sicurezza** non può essere solo basata sui componenti tecnici, ma **deve essere parte di un processo**, dal momento in cui il servizio viene ideato (inception), passando per la progettazione, sino al momento in cui il servizio deve funzionare in modo sicuro.

E, strettamente **connessa al concetto di sicurezza, è la privacy dei dati.** A tale riguardo, **la nuova norma europea che entrerà in vigore nel maggio 2018, nota come General Data Protection Regulation o GDPR stabilisce nuovi doveri e responsabilità del titolare del trattamento dati**. Il regolamento è stato sviluppato per adeguarlo alla veloce evoluzione digitale caratterizzata dalla crescente diffusione dei social network, dall'Internet of Things e dalla gestione di Big Data.

Oltre ad essere obbligatorio, il nuovo regolamento Europeo sulla Data Protection garantisce i diritti di chi quei dati li ha forniti, incentrandosi su doveri e responsabilità del titolare del trattamento dei dati. Una svolta che richiede lungimiranza e molta attenzione e che, per Imprese e PA, potrebbe essere facilitata

introducendo piattaforme tecnologiche impostate per garantire la compliance normativa.

Grazie al pertinente contributo del Prof. Giulio Destri attraverso questo White Paper **cercheremo di guardare al futuro per prepararci a sfruttare in pieno le opportunità fornite dall'ICT, nuova ma già essenziale risorsa.**

01. Il ruolo dell'ICT oggi.

Cosa rappresenta l'Information e Communication Technology (ICT) oggi, nelle aziende e, soprattutto, nella nostra vita di tutti i giorni? Un buon modo per rispondere a questa domanda è analizzare una "normale" giornata della nostra vita.

La vita di tutti i giorni…

La sveglia che ci desta è, molto probabilmente, data da una app entro un cellulare o un tablet che è, sostanzialmente, un computer. Mentre in auto ci spostiamo verso il luogo di lavoro siamo guidati da un navigatore, molto probabilmente connesso ad Internet o anche esso realizzato da una app entro un cellulare o tablet. L'auto su cui ci muoviamo è un concentrato di elettronica, probabilmente ospita un sistema di informazione ed intrattenimento (infotainment) attraverso cui riceviamo informazioni sul mondo. Se ci spostiamo su un mezzo pubblico come un

autobus o un treno, la **pianificazione degli orari di questo è ottenuta attraverso sistemi informatici**. In alcuni casi, come per esempio la linea 5 della metropolitana milanese, **il mezzo stesso è guidato da computer**. Magari durante il tragitto osserviamo comunicazioni dirette al nostro profilo Facebook o di un altro social network, **grazie ad una complessa infrastruttura ICT che gestisce le piattaforme social e le comunicazioni** verso il nostro cellulare/tablet.

Giungiamo nel nostro luogo di lavoro e – qualunque esso sia – **abbiamo a che fare con dei computer** e il software in essi operante. Se abbiamo bisogno di cercare qualcosa **accediamo a enormi banche dati su Internet**, dove è concentrato l'intero scibile umano. Le comunicazioni di lavoro con clienti, fornitori e anche con nostri colleghi che, magari, lavorano in una sede estera della nostra azienda e non abbiamo mai incontrato di persona, sono principalmente basate sulla posta elettronica.

Anche molte delle nostre attività professionali sono realizzate attraverso

sistemi informatici, per esempio la registrazione della fattura di un fornitore o la verifica della pratica di un cliente.

Se la nostra è un'azienda manifatturiera, **buona parte delle operazioni nei reparti di produzione sono pianificate e realizzate da sistemi di automazione** industriale controllati da computer. La logistica di approvvigionamento e trasporto dei prodotti finiti è pianificata attraverso sistemi informatici. I camion che trasportano le merci **sono controllati tramite sensori connessi ai satelliti**.

Se dobbiamo pianificare un viaggio scegliamo e prenotiamo alberghi e mezzi di trasporto, e **spesso scegliamo anche dove andare, tramite Internet**. Possiamo poi andare in un centro sportivo e, mentre usiamo un attrezzo, possiamo controllare il nostro stato di forma fisica attraverso uno smart watch o un altro strumento simile. **I dati raccolti sono un utile ausilio per controllare il nostro stato di salute**. Durante ogni visita medica sarà usato uno strumento elettromedicale come ad esempio un ecografo, che esporterà i nostri dati clinici in un formato

digitale. Queste stesse informazioni saranno disponibili presso una banca dati medica e accessibili tramite Internet.

Ma non finisce qui… **Accanto agli interventi "diretti" di così tanti strumenti ICT nella nostra vita quotidiana, esistono anche tanti altri indiretti**, non meno importanti.

Il nostro stesso modo di vivere è infatti basato su grandi reti infrastrutturali che trasportano l'energia elettrica, l'acqua, il gas… Accanto ad esse ci sono le infrastrutture di trasporto (strade, ferrovie, porti ed aeroporti), le già citate infrastrutture sanitarie, di pubblica sicurezza, della pubblica amministrazione, ecc… **Tutte queste infrastrutture sono, più o meno direttamente, controllate attraverso grandi sistemi informatici**.

In conclusione possiamo affermare che, oggi, **è l'ICT a fare funzionare tutto il nostro mondo** e a rendere possibile il nostro modo di vivere. Quindi la nostra vita è basata sulla tecnologia? Sì. E **l'ICT è soltanto la tecnologia? No, perché per rendere possibile il funzionamento dell'ICT sono necessarie tante componenti**.

Persone e tecnologie alla base dell'ICT

Andiamo con ordine: **si definisce sistema informativo un insieme di persone, procedure, prodotti tecnologici che ha il compito di raccogliere, archiviare, gestire e rendere disponibili le informazioni e i servizi che esse abilitano entro un'azienda, una pubblica amministrazione o anche tutta una nazione**.

Quindi, partendo ciò che lo standard ITIL definisce per l'interno delle aziende, possiamo affermare che, dietro ad uno qualsiasi dei servizi sopra indicati che compaiono nella nostra vita quotidiana, ci sono almeno 4 componenti:

1. ***La tecnologia stessa***, ossia i prodotti tecnologici, ulteriormente suddivisibili in varie categorie, come i terminali finali (cellulari, smartphone, tablet, PC…), componenti server, software, infrastrutture di rete etc.
2. ***Le persone che producono l'hardware***, quelle che lo installano/vendono, quelle che

realizzano il software, quelle che gestiscono i sistemi e li fanno funzionare etc.

3. ***Le procedure, le leggi ed i regolamenti* che governano (o dovrebbero governare) il funzionamento dei servizi** esistenti e la pianificazione di servizi futuri.
4. ***Le relazioni e le partnership fra le varie entità giuridiche*** la cui collaborazione rende possibili i servizi per l'utente finale, ad esempio i fornitori di servizi di connettività ad Internet (Telecom Italia, Vodafone, 3, Fastweb…), i fornitori di servizi Internet (Google, Facebook, Trivago…), i fornitori di terminali (Apple, Samsung, HP, Dell…), i fornitori di software (Microsoft, IBM, SAP…) etc.

Accanto a questi 4 pilastri, ci sono poi altre componenti che completano il quadro che rende possibili i nostri servizi:

- *Per realizzare procedure e processi e impostare le relazioni fra le varie entità giuridiche* ***servono strutture organizzative, composte di persone****.*

- ***Le procedure vanno impostate in base a leggi fatte con consapevolezza****, da persone che, direttamente o indirettamente, possono basarsi sulle opportune conoscenze.*
- *Per operare a qualsiasi livello entro le organizzazioni che realizzano i servizi* ***servono opportune conoscenze.***

  Ecco quindi che il quadro prende forma:

- ***diventa fondamentale il ruolo delle persone che lavorano entro l'ICT****, a vari livelli;*
- ***diventano fondamentali le conoscenze e le capacità che tali persone devono avere e saper usare****. Conoscenze e capacità che non sono solo tecniche ma devono anche essere manageriali, organizzative, relazionali interne ai team e verso utenti, clienti e fornitori…*

Oggi siamo immersi in una grande trasformazione e ancora non sappiamo dove ci condurrà. Accanto ai servizi sopra descritti, che già fanno parte della nostra realtà quotidiana, ne stanno nascendo altri. I Big Data, l'Internet delle Cose e la collegata rivoluzione industriale

4.0 trasformeranno ancora il nostro modo di vivere. L'economia di paesi industriali come il nostro ne sarà dipendente. Chi non riuscirà a cavalcare le trasformazioni corre il rischio di esserne travolto e di dover affrontare una pesante decadenza economica.

Questa rubrica è dedicata alla IT Governance**, intesa come capacità di governare e guidare le profonde trasformazioni rese possibili dalla tecnologia nel nostro mondo.**

Nei prossimi articoli parleremo:

- ***di formazione per l'ICT****, di singole figure professionali vecchie e nuove e delle collegate prospettive di carriera per chi è già dentro l'ICT o chi vuole entrare in questo settore;*
- ***di conseguenze sociali ed economiche delle trasformazioni in corso****, nonché delle scelte che gli IT Manager delle aziende si trovano o si troveranno presto a dover compiere.*

E della più che mai indispensabile necessità di una consapevolezza diffusa riguardante causa ed effetto in merito a strumenti e servizi che tutti,

anche i non addetti ai lavori, utilizzano continuamente magari senza farci caso.

02 L'IT nel XXI secolo: il compromesso tra velocità di evoluzione ed equilibrio.

Buon compleanno IT.

L'Information Technology (IT o, in termini più completi, ICT, comprendendo anche il fattore legato alle Comunicazioni), come visto nell'articolo precedente, oggi è un pilastro fondamentale per la nostra società e per la nostra vita.

Si considera data di nascita dell'IT l'anno 1946, quando furono realizzati i primi calcolatori elettronici programmabili, come evoluzione dei sistemi precedenti. Quindi **nel 2016 l'IT ha compiuto 70 anni** e, in questi decenni, ha subito una grande evoluzione, incomparabile con altri settori dell'attività umana.

L'inizio dell'uso dell'IT nelle aziende è stato alla fine degli anni '50 negli USA e nei primi anni '60 in Italia, anche se da noi **la vera diffusione dell'IT nelle piccole e medie imprese e nella pubblica amministrazione locale avvenne solo con l'avvento dei PC nei primi anni '80**,

soprattutto per problemi di costo delle tecnologie precedenti. Infine, con l'avvento di Internet aperta a tutti negli anni '90 sono apparsi servizi per il grande pubblico, come ad esempio i negozi virtuali come Amazon.

Nel corso della evoluzione, dopo i primi momenti di "fai da te", **sono stati creati standard internazionali (come, ad esempio, ITIL) che hanno definito buone pratiche per realizzare (e mantenere nel tempo) i sistemi informatici**, sia interni alle aziende, sia diretti verso i clienti delle aziende. In particolare viene riconosciuto in questi standard l'importanza dei sistemi informatici ed il valore (anche monetario) da essi procurato al business. **In questo articolo vedremo:**

1. **gli aspetti fondamentali del ciclo di vita dei sistemi IT**;
2. **il loro legame con il business** e con il valore che essi procurano ai propri clienti/utenti, interni od esterni all'azienda cui appartengono.

Le buone pratiche non valgono solo in un contesto aziendale, ma possono essere applicate anche al libero professionista od al privato.

Il concetto di servizio IT.

Per servizio IT s'intende **una unità funzionale, composta di software, hardware e reti, che eroga un valore per i suoi utenti** e che, spesso, nasce come soluzione ad una specifica esigenza e poi si evolve nel tempo.

All'interno di una azienda alcuni servizi IT sono:

- ***la posta elettronica aziendale****,*
- ***un software ERP come SAP*** *(o, più precisamente, i moduli che lo formano),*
- *un sistema di gestione relazioni coi clienti (CRM),*
- *l****a singola postazione di lavoro*** *composta dal PC e da una suite Office, o software specifici come il CAD.*

Se l'azienda ha un reparto di produzione allora **entrano in gioco le Operation Technology (OT)**, ossia le tecnologie di automazione basate sull'IT, alla base della Industry 4.0.

Quindi sono servizi IT anche **un sistema di supervisione e controllo di una catena di**

montaggio, un magazzino automatico o i software per un terminale logistico.

Orientati verso il grande pubblico, sono servizi IT anche:

- ***un sistema di Home Banking****,*
- ***un social media*** *come Facebook,*
- ***un servzio mail*** *come GMail,*
- *un software come la suite Office di Microsoft usato in casa,*
- ***una app*** *come quella per pagare un parcheggio (o meglio, tutto il sistema con tale app connesso e di cui la app è soltanto la interfaccia utente), ecc…*

Nell'ambito interno dell'azienda è quasi immediato il valore che tali servizi erogano, anche se non sempre è calcolabile con precisione il contributo che essi danno al business. Anche per i clienti esterni è chiaro il valore: pensiamo al tempo risparmiato svolgendo le pratiche di pagamento attraverso gli strumenti di home banking, o alla possibilità di acquistare prodotti o altro su Internet senza recarsi presso un negozio

(attività che per molte persone, soggette ai frequenti ritmi frenetici del mondo di oggi, diventa quasi un lusso…).

Le buone pratiche per un servizio IT efficiente.

Le buone pratiche riconoscono **la necessità di strutturare un piano di business, in cui inserire il progetto di un servizio IT**, dal suo concepimento, alla sua realizzazione, alla sua entrata in servizio, alle sue evoluzioni successive, sino alla sua dismissione. **Questo concetto è applicabile sia ad un grande servizio interno ad un'azienda, sia ad un servizio rivolto al grande pubblico**, sia ad un servizio interno ad una famiglia, come per esempio il PC di casa.

Nella figura è mostrato il ciclo di vita di un servizio IT, versione semplificata del ciclo standard presente in ITIL.

Un servizio IT viene ideato per rispondere ad una precisa esigenza, come per esempio automatizzare una determinata funzione aziendale o renderla più veloce, e nasce entro una strategia

legata agli obiettivi del business. **Il suo processo di creazione, realizzazione e mantenumento può essere suddiviso nelle seguenti fasi**:

- ***Service Strategy*** *(insieme di obiettivi, parametri di misurazione e budget da dedicare).*
- ***Service Design*** *(insieme dei requisiti legati agli obiettivi e i criteri di garanzia del servizio).*
- ***Service Transition*** *(insieme dei passaggi necessari alla realizzazione effettiva del servizio).*
- ***Service Operation*** *(realizzazione effettiva del servizio e sua messa in opera).*
- ***Continual Service Improuvement*** *(insieme delle valutazioni periodiche sulla necessità di evoluzione del servizio e il conseguente avvio di un nuovo ciclo evolutivo).*

Service Strategy.

La parte detta Service Strategy deve quindi definire per il servizio obiettivi, parametri di misurazione e budget da dedicare. E' in questa fase che, attraverso uno studio di fattibilità, si può decidere se il servizio deve essere effettivamente

costruito, quali esigenze deve soddisfare e in che tempi deve diventare operativo.

Service Design.

Nella fase successiva, detta Service Design devono essere:

1. **individuati con precisione tutti i requisiti legati agli obiettivi definiti nella fase precedente** che il servizio deve realizzare (attività che fa parte della Business Analysis che viene chiamata anche Requirement Engineering);
2. **definiti i criteri di garanzia del servizio,** come per esempio la sua disponibilità temporale (il servizio deve essere disponibile 24 ore per tutti i giorni della settimana? Oppure soltanto in orario di ufficio?), **oppure la capacità del servizio** (ad esempio numero di utenti che si possono collegare simultaneamente al servizio o numero di documenti che possono essere memorizzati in formato elettronico dal servizio).

In base a tali criteri il servizio viene progettato in modo da fornire ad essi soluzione. E, in base alla

struttura dell'azienda ed alla convenienza economica, si decide se:

- ***il servizio viene realizzato in toto entro l'azienda stessa*** *(make),*
- ***il servizio viene acquistato completamente*** *all'esterno, ovvero la sua realizzazione è completamente appaltata all'esterno (buy) o,*
- ***la realizzazione è ibrida*** *(customize).*

La gestione del progetto di realizzazione e messa in opera dovrà essere svolta secondo i criteri dell'IT Project Management.

Service Transition.

Nella fase di Service Transition vengono svolti tutti i passaggi necessari alla realizzazione effettiva del servizio ed alla sua messa in opera entro il contesto dove dovrà operare. Il punto fondamentale di questa fase è la installazione dei componenti del servizio stesso e la gestione opportuna del cambiamento relativo in modo tale da minimizzare gli impatti su altri servizi che stanno funzionando.

Service Operation.

La fase di Service Operation è la più importante di tutte: in questa fase il servizio IT è installato, funziona e svolge il compito per cui è stato creato, erogando ai suoi utenti il valore associato a tale compito. Problemi di funzionamento, guasti ed errori devono essere corretti nel minor tempo possibile per ripristinare le normali condizioni di esercizio del servizio stesso, con una apposita organizzazione.

Continual Service Improuvement.

Le esigenze di business che cambiano nel tempo, vincoli di legislazione, o anche esigenze operative come il numero di utenti che aumenta possono richiedere che il servizio si evolva. **Per mantenersi adeguato in un mondo mutevole, il servizio deve essere "vivo", deve evolvere in base al bisogno. La fase di Continual Service Improuvement** (ogni riferimento del risultante acronimo CSI alla omonima serie televisiva è, a mio parere, tutto meno che

casuale…) **prevede proprio valutazioni periodiche sulla necessità di evolvere il servizio e il conseguente avvio di un nuovo ciclo evolutivo**, che, se gli obiettivi di business del servizio non cambiano, non parte dal Service Strategy, ma direttamente da Service Design o, se la modifica è piccola, dal Service Transition.

Qualche esempio di applicazione del ciclo di vita di un servizio IT.

In un contesto aziendale un servizio IT potrebbe essere un sistema di CRM analitico, che viene disegnato in base agli obiettivi di business di migliorare la penetrazione in un segmento di mercato, che viene comprato in Cloud da un fornitore, che viene attivato per un numero di utenti dell'azienda e che, dopo un anno, viene arricchito di funzionalità di cui è emersa la necessità in base all'esperienza fatta.

In un contesto di servizio verso il pubblico pensiamo ad un portale di servizi turistici, che nasce per permettere agli utenti di prenotare alberghi e viaggi e che viene continuamente

arricchito di funzionalità per rimanere competitivo sul mercato.

In un contesto domestico, pensiamo al PC di casa: nostro figlio o nostra figlia arriva in una nuova scuola per cui è necessario l'acquisto di un PC più potente, che durerà alcuni anni e per il quale acquisteremo nuovi software man mano che se ne presenta la necessità. Eventualmente stipuleremo un contratto di garanzia ed assistenza con il fornitore per potere avere il PC sempre funzionante. Un discorso analogo vale per lo smartphone, o anche altri elettrodomestici come la smart TV.

Servizio IT: che lezioni traiamo da questi esempi?

Per la reralizzazione di un servizio IT diventa necessario mettere in atto e gestire efficientemente progetti anche complessi, con tante professionalità coinvolte. Questo perchè:

1. **Ogni strumento/servizio IT ha uno scopo o più di uno e può essere evoluto o sostituito in base all'evoluzione dello scopo**; questa

cosa vale anche per altri strumenti, come per esempio l'automobile che dobbiamo sostituire quando in famiglia si cresce di numero; non scordiamo anche le operazioni di passaggio: se nel nostro smartphone è una rubrica con 1000 contatti, essa è un patrimonio che dobbiamo trasferire in un nuovo strumento, senza dover ribattere tutti i contatti;

2. Quando pianifichiamo l'acquisto o la costruzione di uno strumento/servizio IT, ricordiamo che **esso dovrà evolvere nel tempo a seguire il bisogno, ma che dovrà anche funzionare in modo sufficiente per il bisogno per un certo tempo**;
3. Nel contesto di servizi grandi, interni all'azienda o per il pubblico/cliente, **sono necessarie analisi strategiche, analisi dei rischi, analisi di requisiti, design tecnico, pianificazioni, realizzazioni, integrazioni**, ossia una serie di azioni molto diverse, **che coinvolgono professionalità diverse**.

Nel prossimo articolo tratteremo **delle caratteristiche e il riconoscimento dei profili professionali del mondo IT.**


01
01
01
01

03. Le figure professionali dell'ICT: come riconoscerle.

Capita spesso che chi lavora nel settore IT o ICT abbia qualche difficoltà a spiegare in poche parole il proprio lavoro a chi non conosce bene il settore. Questo è anche dovuto all'enorme evoluzione che c'è stata nel corso degli anni. Vediamo di fare chiarezza ed esplorare le competenze di queste figure professionali.

Breve biografia istituzionale dell'ICT.

L'ICT che, come visto nell'articolo precedente, *"è oggi un pilastro fondamentale per la nostra società e per la nostra vita"* ha ormai decenni di attività alle spalle e h**a subito una evoluzione non comparabile con quella di altri settori tecnologici umani.**

In particolare, negli ultimi 15 anni **si sono verificati tanti cambiamenti per i profili professionali operanti nel campo ICT**, con

una moltiplicazione enorme di titoli e job description, c**he ha portato contestualmente a un grande disordine** e alla non effettiva comprensione di chi fa che cosa all'interno della definizione di l'ICT. Situazione, questa, in comune comunque con diversi altri settori professionali, all'interno dei quali sono nate nel corso degli anni professioni del tutto nuove.

In questo quadro, **il 14 gennaio 2013 in Italia è stata emanata la Legge n. 4 recante "Disposizioni in materia di professioni non organizzate", norma di particolare interesse per chi svolge professioni appunto non organizzate in ordini o collegi**, a esclusione delle attività artigianali, commerciali e in generale di tutto ciò che è già normato o disciplinato.

Sulla base di questo mandato UNINFO, la sezione dedicata alla regolamentazione ICT di UNI, l'Ente Italiano di Normazione, ha emanato la norma UNI 11506:2013 dal titolo **"Attività professionali non regolamentate – Figure professionali operanti nel settore ICT – Definizione dei requisiti di conoscenza, abilità e competenze"**, in vigore dal 26 settembre 2013.

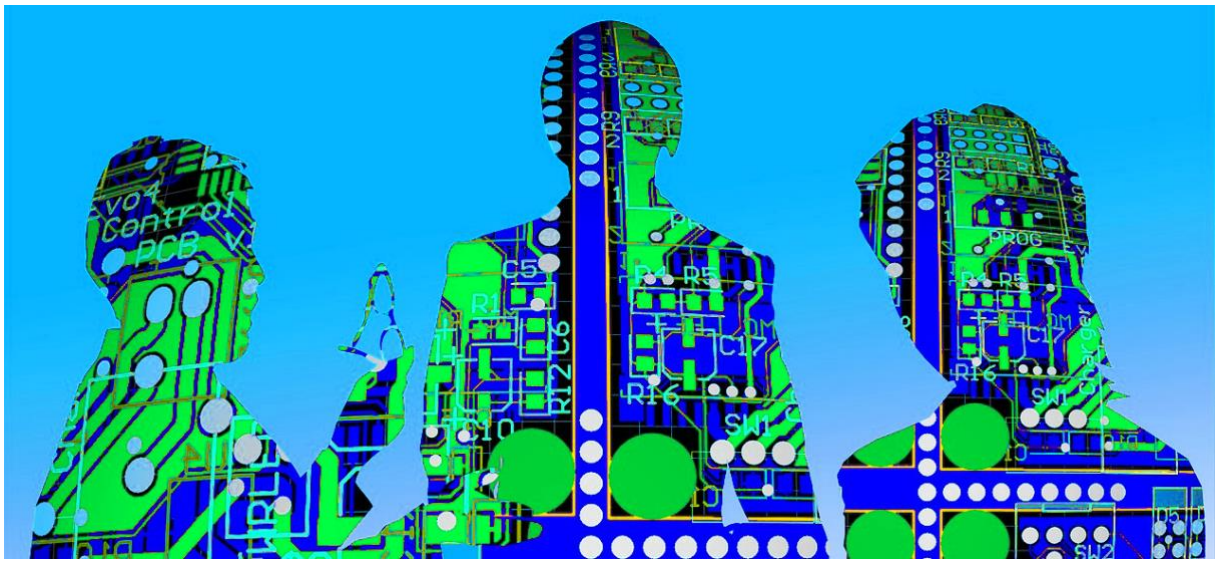
Questa norma definisce i criteri generali delle figure professionali operanti nel settore ICT stabilendo i requisiti fondamentali per l'insieme di conoscenze, abilità e competenze che le contraddistinguono, e si applica alle figure professionali indipendentemente dalle modalità lavorative e dalla tipologia del rapporto di lavoro (dipendente, freelance o libero professionista iscritto a un Ordine professionale).

La norma UNI 11506 è stata redatta a partire dal quadro europeo di riferimento delle competenze e dei relativi skill "eCompetence Framework (e-CF)", trasferendolo al contesto italiano. **L'Italia, con la norma UNI 11506, è stata la prima nazione a livello europeo a dotarsi di uno standard per le competenze ICT, diventando per la prima volta anche propositore** e anticipando altre nazioni: l'organo di normazione della Unione Europea, il CEN, ha rilasciato nella primavera 2016 **la nuova norma EN 16458-1**, basata sulla nostra UNI11506, con tanto di traduzione italiana già pronta.

La continua crescita e la necessità di costruire un sistema evolvibile ha infine portato alla normativa completa attualmente in essere dal 2016, la UNI 11506-11621, norma "multi-parte" che definisce:

- ***Livello 1: le 6 famiglie fondamentali di profili****, legate alle specifiche funzioni necessarie per tutto il ciclo di vita di un servizio ICT, e le regole per costruire un profilo professionale ad esse legato.*
- ***Livello 2: entro una (o più) di queste funzioni i 23 profili professionali fondamentali dell'ICT****, detti anche profili di "seconda generazione".*
- ***Livello 3 e successivi: profili di "terza generazione"****, definiti seguendo le regole del livello 1 e collegati con i profili di seconda generazione.*

I fornitori del servizio ICT: famiglie e profili.



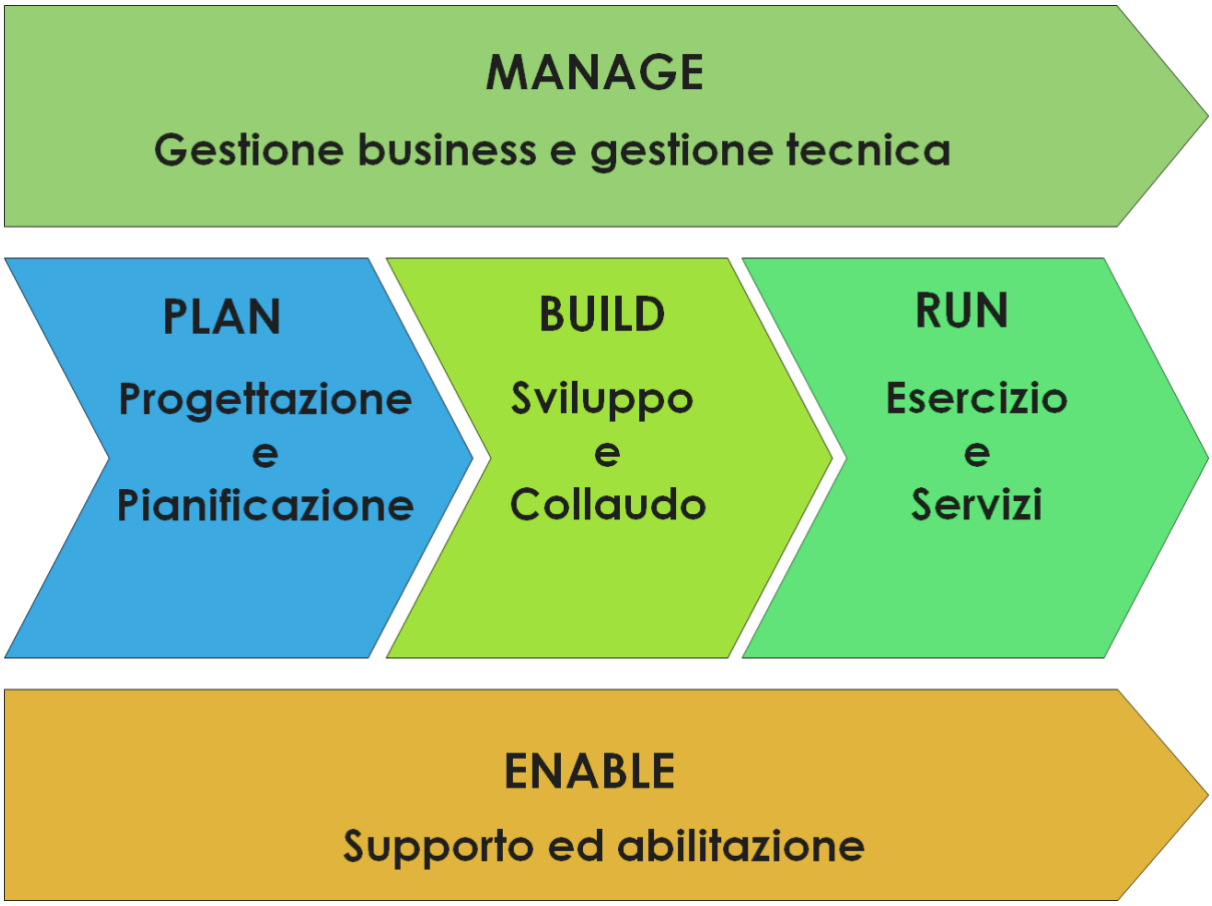
Vediamo ora le "famiglie" fondamentali in cui sono suddivisi i profili, tenendo presente che viene riconosciuta la necessità di strutturare un piano di business in cui inserire il progetto di un servizio ICT, dal suo concepimento alla sua entrata in servizio, sino alla sua dismissione. Ricordiamo inoltre che per servizio ICT si intende una unità funzionale, composta di software, hardware e reti, che eroga un valore per i suoi utenti. **Esempi di servizi ICT possono essere un social media come Facebook, un servzio mail come GMail, un software ERP come SAP, un software come la suite Office di**

Microsoft o una app come quella per pagare un parcheggio.

Diventano quindi necessari gli ambiti:

- ***Business Management****: gestione dal punto di vista business ed economico, deve garantire un ROI per il servizio.*
- ***Technical Management****: gestione metodologica e tecnica, presuppone l'uso delle tecniche di Project Management applicate al contesto ICT.*
- ***Design e Plan: progettazione tecnica ed architetturale****, dove è compresa la raccolta dei requisiti e la definizione delle esigenze funzionali cui il progetto pone una risposta.*
- ***Build: costruzione tecnica del servizio*** *obiettivo del progetto, quindi sviluppo, integrazione e collaudi.*
- ***Run: parte di esercizio, in cui il servizio deve svolgere il compito per cui è stato creato*** *rispettando i parametri di funzionamento stabiliti durante le fasi precedenti.*

- ***Enable: tutto l'insieme delle attività di supporto*** *che abilitano il funzionamento del servizio, che comprendono anche le relazioni commerciali tra entità giuridiche diverse (ad esempio clienti-fornitori).*

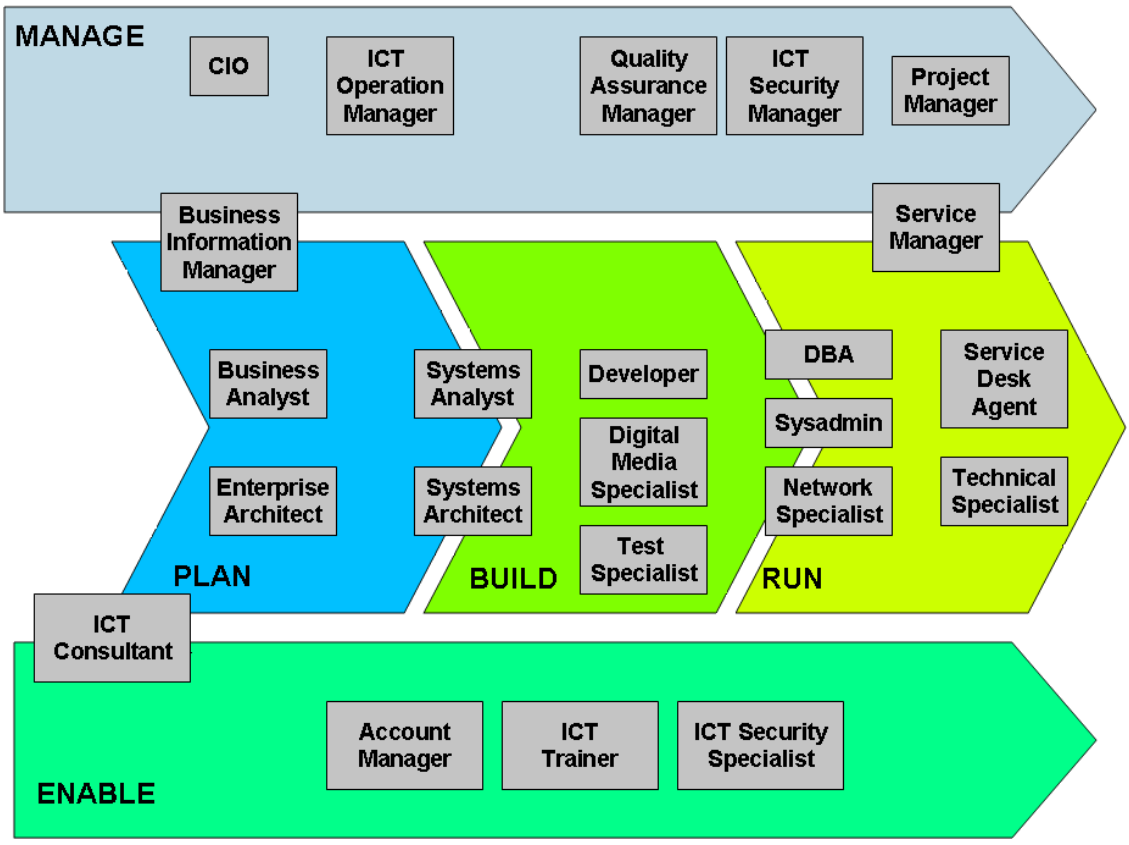


Il quadro va pensato in termini temporali: **tutti i servizi sopra citati non sono entità statiche**, che una volta realizzate rimangono costanti, **ma strumenti che evolvono nel tempo, seguendo le mutevoli esigenze funzionali di chi le usa**. Pensiamo, ad esempio, a come nel

tempo si sono evoluti Facebook o GMail. Ne deriva che, in realtà, il ciclo plan-build-run si ripete continuamente nel tempo, con l'aggiunta di funzionalità sempre nuove e la correzione di errori e imprecisioni.

Altri profili e prossime sfide.

Nel diagramma sottostante sono invece rappresentati, inquadrandoli nei 6 ambiti fondamentali, **i ruoli di seconda generazione, che devono svolgere le funzioni degli ambiti fondamentali**.



Tra di essi sono riconoscibili alcuni ruoli "storici" come il developer o sviluppatore, il CIO – evoluzione dell'EDP/IT Manager, l'IT Project Manager, il Business Analyst o analista funzionale, il Sysadmin o sistemista [2].

Alcuni ruoli sono di collocazione "varia", come l'ICT Consultant, che è a cavallo fra diversi ambiti. O il Service Manager, che si colloca fra la gestione tecnica ed il run. Altri ruoli sono nati con le nuove tecnologie, come il Business Information Manager, responsabile, fra l'altro, delle informazioni e della conoscenza in un'azienda e figura funzionale che dovrà un domani dirigere chi si occupa materialmente di Big Data.

In ogni caso è stabilita una nomenclatura standard, che identifica ruoli precisi e gli associati compiti e definisce ordine nel mare magnum dell'ICT, finora molto anarchico. Il quadro sicuramente si evolverà nel tempo al procedere della evoluzione dell'ICT e nuovi profili dovranno essere creati.

La certificazione professionale, disponibile per profili come il Security Specialist, l'IT Project Manager ed il Business Analyst, aggiunge valore

alla figura del professionista che la possiede, in quanto riconosciuta da Accredia, l'Ente Italiano di Accreditamento.

Inquadrato il discorso in ambito generale, proviamo ora a entrare più nello specifico.

- ✓ **Un'azienda di informatica italiana, come ad esempio il Gruppo Maps, di che profili ha bisogno?**

  Senz'altro di molti Developer, Test Specialist e Digital Media Specialist, di alcuni sysadmin, DBA, network specialist e technical specialist, di diversi Business Analyst, System Analyst e Systems Architect, di diversi Project Manager e Account Manager, di almeno un Quality Assurance Manager. Il tutto tenendo conto del fatto che più ruoli possono essere ricoperti dalla stessa persona, magari in diversi progetti, purché essa abbia gli skill necessari e il tempo uomo sufficiente a disposizione.

- ✓ ***Un'azienda non di informatica, invece, di che profili ha la necessità?***

  Sicuramente di un CIO, di un Security Manager, di diversi sysadmin, network specialist e DBA, di service desk agent. Inoltre di ICT Consultant e Technical Specialist, questi ultimi tipicamente esterni. Se è presente un settore di sviluppo interno saranno necessari anche diversi developer.

- ✓ ***Un'ultima questione: chi si affaccia per la prima volta al mondo dell'ICT può, da subito, aspirare a ricoprire uno qualsiasi di questi profili?***

  Nella maggior parte dei casi no, perché i ruoli più manageriali richiedono sicuramente anche esperienza operativa sul campo.

Nel prossimo articolo vedremo **come l'Università prepara** le persone che diventeranno **i professionisti ICT** di domani.

04. La formazione accademica: come si diventa professionista ICT.

Negli ultimi anni **le aziende spesso lamentano carenze nella preparazione che scuole ed università danno ai nuovi professionisti del settore ICT**. E, talvolta, le stesse lamentele giungono anche dagli allievi. Ciò comunque **non impedisce ai neolaureati in Informatica ed Ingegneria Informatica di trovare rapidamente lavoro**, almeno in molte zone d'Italia. E le stime di agenzie internazionali come Modis, confermate dall'AgID (Agenzia per l'Italia Digitale), indicano in alcune decine di migliaia i posti di lavoro nel settore ICT destinati a non essere coperti per mancanza di figure professionali adeguate, da qui al 2020.

Quale è l'obiettivo della formazione accademica "tecnica"?

Una domanda che sorge spontanea è questa: **quale è l'obiettivo della formazione accademica "tecnica"? O, in altri termini, quale deve essere la preparazione di un laureato in informatica/ingegneria informatica?** Per rispondere devo fare riferimento sia alle mie esperienze accademiche come professore a contratto dal 2003 presso il corso di Laurea in Informatica e, per alcuni periodi, anche presso quello di Ingegneria Informatica a Parma, sia alle mie esperienze come formatore aziendale nel comparto ICT.

Nell'articolo precedente ho trattato il tema dei profili professionali dell'ICT definiti nella normativa UNI11506-11621 e riconosciuti a livello di Unione Europea. **Alcuni di tali profili richiedono, oltre alla preparazione teorica, un certo livello di esperienza sul campo e quindi non possono essere rivestiti subito da neolaureati.** Ma possono ovviamente esserlo dopo alcuni anni di esperienza lavorativa.

Cosa significa questo?

Chi affronta lo studio di un corso di laurea orientato verso il settore ICT, come Informatica o Ingegneria Informatica, deve essere consapevole che **dovrà dedicare una parte del proprio tempo lavorativo** (o anche del proprio tempo libero) **al continuo aggiornamento**, ovvero che lo studio non termina con l'Università, ma prosegue per sempre.

D'altronde **l'Università** non deve solo formare per i primi ruoli che le persone incontreranno nel mondo del lavoro, ma **deve invece formare professionisti, abili e consapevoli, che possano poi crescere gradualmente, integrando lo studio e l'aggiornamento autonomo con l'esperienza sul campo.**

Per questo possiamo riassumere le competenze che l'Università deve trasmettere in alcune grandi aree:

AREA TECNICA – per la quale **occorrono competenze tecniche di programmazione,**

sistemiche e metodologie sistemiche. In pratica il neolaureato:

- ***deve essere in grado di disegnare e realizzare programmi*** *secondo i paradigmi moderni di programmazione e, soprattutto,* ***deve essere in grado di apprendere rapidamente anche nuovi linguaggi di programmazione****; non c'è spazio nel mercato futuro per persone solo abituate al copia e incolla di codice;*
- ***deve conoscere bene almeno un sistema operativo*** *come Windows o Linux;*
- ***deve essere consapevole dell'"ecosistema digitale" in cui si troverà ad operare*** *e dei pericoli che si corrono al suo interno e, soprattutto,* ***deve essere consapevole che il software o i sistemi su cui lavorerà sono parte di un enorme intrico di sistemi connessi*** *fra loro in rete.*

AREA CULTURALE – per la quale **occorrono competenze di cultura scientifica generale e**

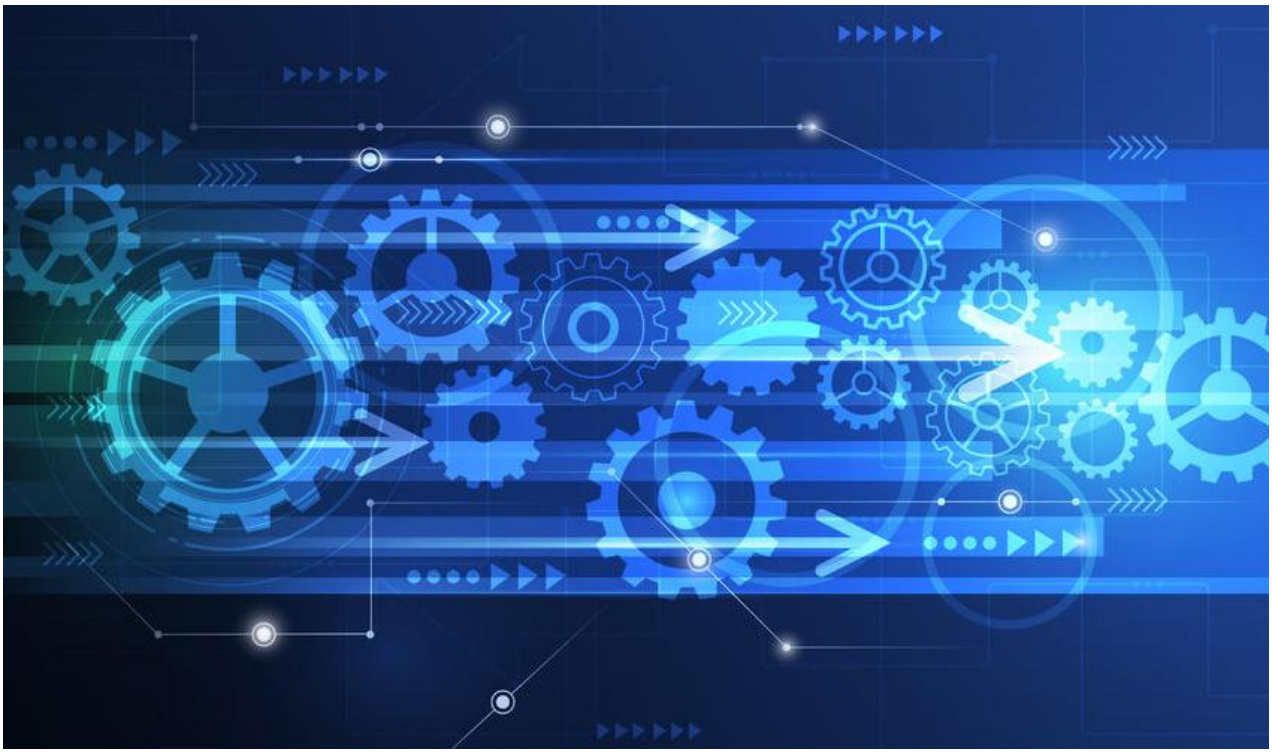
competenze linguistiche, normalmente sottostimate:

- ***una cultura scientifica generale è invece importante, in primis per tutti coloro che operano in settori collaterali all'ICT****, come l'automazione industriale e la robotica (ovvero le Operation Technologies o OT) mentre;*
- ***le competenze linguistiche*** *sono* ***di fondamentale importanza per la comunicazione, sia nella stesura di documenti tecnici, sia nella creazione di presentazioni a clienti e testi commerciali chiari.*** *Non sono tollerabili errori grossolani di italiano in una tesi di laurea o in un report, meno che mai durante un colloquio con un cliente; ovviamente è necessaria anche la buona conoscenza della lingua inglese.*

AREA LAVORATIVA – per la quale occorrono **competenze econometriche e competenze relazionali e di lavoro in team.**

In pratica, il neolaureato:

- ***deve essere consapevole di come è organizzato normalmente il lavoro entro le aziende*** *in cui entrerà a lavorare e di come inserirsi proficuamente in un team;*
- ***deve essere consapevole sia dello scopo ultimo dell'ICT****(uno strumento di supporto al business e per fare business)* ***sia, soprattutto, degli aspetti economici di un progetto ICT****; questo aspetto diventerà fondamentale qualora il neolaureato divenga poi capo progetto o voglia intraprendere una carriera da libero professionista o imprenditore.*



Sono sempre necessarie tutte queste competenze? Alcune possono essere create, a fatica, durante il lavoro. Ma in ogni caso se già in possesso del neolaureato, esse sono un plus.

Un altro aspetto che il neolaureato deve ricordare è: **essere orgoglioso delle proprie conoscenze e delle proprie potenzialità, ma allo stesso tempo essere consapevole delle proprie carenze e disposto all'apprendimento** sul campo. Infatti in alcuni casi i neolaureati si comportano da primedonne, arrivando in aziende e gruppi di lavoro con anni (o decenni) di esperienza alle spalle, e generando un rifiuto da parte degli altri membri del gruppo e la conseguente progressiva emarginazione dall'organizzazione, di solito seguita dalle loro dimissioni o dalla non conferma dopo il periodo di prova.

Ovviamente il neolaureato inserito bene potrebbe, dopo un po' di tempo, preferire un'altra azienda a quella in cui si trova, per svariati motivi. Così come esistono aziende in cui il lavoro è particolarmente impegnativo e di conseguenza

il turn-over è molto alto, con un basso tempo di permanenza delle persone.

In sostanza quale è il punto?

Le aziende italiane del mondo ICT, nonostante molte non usino le metodologie tecniche ed organizzative di ultima generazione, **hanno un patrimonio umano di esperienze molto vasto e ricco. Se adeguatamente integrate da una nuova generazione di professionisti e modernizzate con le apposite metodologie** (come, per esempio, la organizzazione agile) le aziende italiane si **possono proporre sul mercato internazionale**. Le aziende italiane possono entrare in competizione con le aziende indiane, meno flessibili, e quelle dell'Europa orientale, i cui costi stanno rapidamente crescendo.

L'Italia può e deve approfittare di questa opportunità di portare lavoro tecnologico in casa nostra. Ma, **per sfruttare questa opportunità, è necessario:**

- ***che ci sia presto sul mercato una nuova generazione di professionisti ICT ben preparati****. Non ha senso che per aumentare il numero si abbassi la qualità della preparazione. Ciò significa quindi che* ***i giovani che intraprendono la carriera nel settore ICT devono essere disposti all'investimento in uno studio molto intenso durante il periodo accademico,***
- ***che le aziende devono essere disposte a modernizzarsi*** *per fare rendere il nuovo capitale umano, anche con retribuzioni adeguate.*

Nel prossimo articolo porremo attenzione su una delle questioni più rilevanti del mondo ICT, ovvero la sicurezza dei dati.

05. ICT ed effetti indiretti di sicurezza: la cybersecurity sulla scena politico-economica mondiale.

IT Security e CyberSecurity.

Nel primo articolo della serie è stato spiegato il ruolo centrale che l'Information e Communication Technology (ICT), o semplicemente IT, ha oggi nella nostra vita di tutti i giorni, sia professionale, sia personale.

Partendo ora dal ruolo dell'ICT nel nostro mondo, **spieghiamo il concetto di sicurezza diretta ed indiretta dei sistemi ICT:**

1. **Per sicurezza diretta intendiamo tutto ciò che riguarda la prevenzione di attacchi diretti** ai sistemi ICT, come ad esempio l'effetto di virus informatici sul nostro PC di casa o sul server aziendale contenente i dati della contabilità. **E questo è ciò che viene chiamato IT Security o ICT Security**.
2. **Per sicurezza indiretta** intendiamo:

– ***la prevenzione dell'uso di sistemi ICT*** *come strumento ponte per condurre un attacco verso altri apparati che sono connessi a tali sistemi e anche (almeno in parte),*

– ***la prevenzione che problemi nei sistemi ICT,*** *dovuti magari ad eventi casuali,* ***possano estendersi agli altri apparati connessi****. E questo è ciò che viene chiamato* ***CyberSecurity****.*

Quindi IT Security e CyberSecurity, pur strettamente connesse tra loro, **non sono sinonimi**.

La CyberSecurity è estremamente più vasta della IT Security, perché ormai l'IT pervade quasi ogni aspetto della nostra vita. E, siccome tendiamo a dimenticare questa pervasività, spesso siamo consapevoli della IT Security elementare (ad esempio, sappiamo o dovremmo sapere che è rischioso aprire un allegato di una mail proveniente da sconosciuti), mentre **siamo molto meno consapevoli degli innumerevoli aspetti della CyberSecurity**, destinati ad

aumentare ulteriormente nei prossimi anni, per l'avvento di sempre nuove tecnologie.

Lo scenario della CyberSecurity.

Per spiegare meglio il concetto è utile un esempio tratto dalla storia: **nel 2014 la grande banca americana J.P. Morgan ammise che dei pirati informatici erano penetrati nei suoi sistemi ed avevano rubato i dati di circa 80 milioni di clienti**. Il punto interessante è come erano riusciti questi pirati a penetrare.

Furono necessari molti mesi di indagine per scoprire che **i pirati informatici non avevano attaccato direttamente i sistemi informatici della banca, ma avevano percorso un'altra strada, aggirando le protezioni.**

In pratica, il sistema di climatizzazione dell'enorme edificio in cui il quartier generale della banca si trova, insieme ai sistemi informatici centrali, era governato da un computer, accessibile dall'esterno, per consentire all'azienda che gestiva l'impianto di climatizzazione di controllare l'impianto stesso. Questo computer non avrebbe dovuto essere collegato nella stessa rete degli altri (esistono infatti protocolli precisi per situazioni del genere), ma lo era stato. I pirati lo avevano usato quindi come ponte, per attaccare i sistemi informatici della banca con molta maggiore facilità rispetto ad un attacco diretto.

Proviamo ad espandere lo scenario, considerando le grandi infrastrutture come gli elettrodotti e gli acquedotti. Nei sistemi odierni, **praticamente ogni centrale elettrica, così come ogni stazione di pompaggio, contiene uno o più computer**, collegati ai sistemi di controllo degli apparati con opportune interfacce. In molti casi le centrali e le stazioni **non sono presidiati da personale umano ed i computer sono connessi a reti per**

permettere il telecontrollo attraverso l'accesso remoto. **Un attacco a questi computer potrebbe provocare il blocco degli apparati** lasciando, ad esempio, un'area geografica più o meno vasta senza acqua o senza energia elettrica.

Lo stesso principio vale per altre infrastrutture, come i gasdotti o come le reti di trasporto. **Nel mese di giugno 2017 un guasto informatico ha praticamente bloccato i voli di British Airways** per molte ore, con le devastanti conseguenze sul traffico aereo. In base alle indagini sembra che **la causa non sia stata un attacco deliberato, ma semplicemente un errore di un tecnico.**

Considerando le infrastrutture critiche di una nazione, diventa p**ossibile pensare ad una serie di attacchi informatici generalizzati rivolti a tali strutture come arma di guerra?**

La risposta è sì e **questo approccio si chiama CyberWar o CyberWarfare** (talvolta tradotto in italiano come guerra cibernetica o guerra informatica). **Nel 2007 si registrò in Estonia il primo scenario di attacchi generalizzati alle**

infrastrutture, dalla rete gorvernativa alla Borsa che, per diverse settimane, furono sottoposti ad assalti massicci e coordinati, provenienti soprattutto dalla Russia e, molto probabilmente comandati dal governo russo, dato il clima di tensione politica fra i due Paesi in quell'anno.

Il coinvolgimento del governo russo non fu mai dimostrato, almeno ufficialmente, e i danni economici furono ingentissimi. **L'episodio, considerato il primo caso riconosciuto di guerra cibernetica, dimostrò l'estrema vulnerabilità delle infrastrutture delle nazioni. Da allora la NATO ha organizzato una divisione di guerra cibernetica. Tutte le grandi potenze sono oggi impegnate attivamente nella difesa da CyberWar** (e anche nella offesa, come diversi fatti hanno dimostrato, non ultimo il caso, non ancora chiarito completamente, della interferenza russa nelle ultime elezioni presidenziali americane).

Restringendo lo scenario ad una casa, **possiamo pensare al ruolo di dispositivi "smart" come elettrodomestici allacciati alla rete, SmartTV**

e sistemi domotici. Questi dispositivi consentono il controllo remoto della casa e, se attaccati, potrebbero consentire violazioni della privacy o anche l'ingresso non autorizzato nella casa stessa.

Computer e smart device non sono "semplici" elettrodomestici.

Uno dei fattori che **sta incrementando i possibili attacchi cibernetici è la considerazione che, mediamente, le persone hanno dei nuovi dispositivi presenti da pochi anni sul mercato**. Nella accezione comune un computer è considerato qualcosa di diverso da uno smartphone, da una smart TV, da una interfaccia di sistema di informazione ed intrattenimento (infotainment) presente nel cruscotto di un'automobile o da un frigorifero intelligente. Dopo anni di problematiche legate a virus informatici ed attacchi diretti le persone hanno iniziato a considerare il PC come qualcosa "da usarsi con una certa attenzione" (comunque spesso insufficiente, come dimostrano i tantissimi casi di attacchi informatici diretti causati da

imprudenze di operatori umani). Mentre lo stesso discorso non vale per smartphone ed altri device, che nell'accezione comune sono equivalenti agli elettrodomestici delle generazioni precedenti. Non è così.

Oggi uno smartphone è a tutti gli effetti un computer, spesso con potenza di calcolo superiore a quella di PC di pochi anni fa. **Ha la complessità di un computer e le vulnerabilità di un computer**. È dunque soggetto al furto di informazioni ed alla azione di virus e software malevoli, come un computer.

Il discorso è, in alcuni casi, **ancora peggiore per gli smart devices. Un frigorifero intelligente o una smartTV ospita di solito un sistema operativo completo**, privato di alcune parti non necessarie, **ma con tutta la connettività di rete presente. Connettività che può essere usata da pirati informatici per entrare nel sistema del dispositivo** ed usarlo per scopi malevoli vari, come dimostrato nel celebre caso di invio di mail indesiderata da parte di smart device di pochi anni fa. Spesso, **il problema è nella configurazione**

dell'ingresso via rete, impostata in fabbrica a valori di default e non personalizzabili dall'utente, ma sfruttabili da pirati informatici.

Cosa significa questo? Che sia da parte dei produttori, sia da parte degli utenti, devono essere applicate apposite procedure di sicurezza:

- ***I produttori devono realizzare dispositivi più sicuri****,*
- ***gli utenti devono essere informati su quali precauzioni prendere*** *per ridurre al minimo i rischi.*

L'Internet delle Cose e le auto sempre connesse.

Lo scenario è in continuo sviluppo: l'**Internet delle Cose è un mercato enorme**. Una ricerca IDC stima che nel 2020 ci saranno centinaia di miliardi di oggetti connessi alla rete, per un mercato di circa 1.300 miliardi di dollari. Quindi bisogna affrontare le cose in modo tale che tutto questo rimanga opportunità di business, sviluppo e miglioramento e non conduca a rischi giganteschi.

Prendiamo, ad esempio, l**e nuove funzionalità offerte da una smart car**. La smart car:

1. **analizza i propri sistemi fornendo una diagnostica preventiva** che segnala le riparazioni da fare prima ancora che i guasti si manifestino;
2. **i dispositivi hardware come lo sterzo ed i freni sono controllati dalla centralina che è, a tutti gli effetti, un piccolo computer** consentendo, ad esempio, la frenata di emergenza in rischio di collisione, tanto pubblicizzata in vari spot;
3. comunicando con altre auto o interagendo con sistemi come Google Maps **l'auto può segnalare ingorghi e suggerire strade alternative al pilota**;
4. **raccoglie le abitudini di guida che comunica al costruttore,** consentendo di personalizzare sempre più le caratteristiche dei futuri modelli.

Ma c'è anche il rovescio della medaglia. **In un articolo su Wired del 2015 veniva**

dimostrato come fosse possibile prendere il controllo completo di una smart car entrando nel sistema attraverso la connessione di rete, sfruttando una vulnerabilità del software. Di qui al furto d'auto c'è poca strada: negli USA ormai si contano moltissimi casi di furti d'auto perpetrati attraverso attacchi informatici ai sistemi di bordo.

In sostanza quindi occorre tenere presente che un **dato sistema informatico, quando diviene parte di un contesto più ampio, come un frigorifero intelligente o il controllo di un impianto industriale, deve essere adatto al nuovo ambiente in cui si trova**. Sistemi sviluppati per funzionare in modo non connesso in rete e, quindi, non progettati o non adeguatamente testati per operare in rete, non possono essere semplicemente collegati senza rischi per la sicurezza.

Da Insecurity by Design a Security from Inception.

Nel corso della cena di un evento ufficiale del 2015, insieme ad un amico che lavora all'ENISA, coniammo (o meglio riscoprimmo) il termine **"Insecurity by Design", intendendo con questo che in moltissimi sistemi informatici o di smart device di oggi la sicurezza è talmente poco considerata da far quasi pensare che siano progettati apposta per essere insicuri**.

I casi sopra presentati ci inducono a pensare che l'insicurezza rende anche possibili scenari inquietanti, in cui, per esempio, un attacco al sistema informatico di un impianto di riciclaggio rifiuti può portare all'alterazione dei livelli di

inquinanti rilasciati nell'ambiente e al conseguente blocco dell'impianto stesso, mandando in crisi la nettezza urbana di una grande città.

È necessaria prevenzione di tutto questo. E la prevenzione parte dalla consapevolezza. La consapevolezza che la sicurezza è qualcosa da prevedere fin dagli inizi di un servizio IT, diretto o parte di un sistema industriale, domotico o di internet delle cose. La sicurezza deve quindi essere spostata da un rimedio apposto dopo i primi incidenti a una prevenzione applicata a livello di progetto, in una visione di insieme. Questo è anche quello che standard internazionali riconosciuti come ITIL, COBIT, ISO27001… raccomandano o impongono.

La sicurezza non può essere solo basata sui componenti tecnici, ma deve essere progettata come processo, dal momento in cui il servizio viene ideato (inception), passando per la progettazione, sino al momento in cui il servizio deve funzionare in modo sicuro.

È necessario quindi:

- ***che il legislatore intervenga, a tutti i livelli, per imporre ai produttori la sicurezza*** *in sede di progettazione e per imporre alle aziende utilizzatrici l'uso della sicurezza entro i propri processi;*
- ***educare il grande pubblico per evitare che comportamenti imprudenti o imperizia possano portare a rischi di sicurezza****, nel mondo aziendale (come nel caso del blocco dei sistemi di British Airways sopra citato), nel mondo della pubblica amministrazione e nella nostra vita di tutti i giorni.*

Il GDPR (General Data Privacy Regulation), regolamento europeo della privacy che entrerà in vigore nel 2018, **è una legge che va in questa direzione e sarà oggetto del prossimo articolo.**

07. Come cambiano le normative: arriva il GDPR.

GDPR: il "Gran Decreto Privacy"?

Nel precedente articolo abbiamo visto alcune delle problematiche di sicurezza, diretta ed indiretta, legate agli strumenti IT.

In questo articolo **concentriamo invece l'attenzione sulla privacy dei dati**, connessa in modo molto stretto con la sicurezza, **e sulla nuova norma europea** che entrerà in vigore nel maggio 2018, il Regolamento UE 679/2016, meglio noto come **General Data Protection Regulation o GDPR**.

In Italia esistono già norme sulla privacy: la Legge n. 675 del 31/12/1996, sostituita poi dal D.lvo 196/2003 noto anche come "Decreto Privacy", che ha contribuito a fare crescere la consapevolezza della necessità di sicurezza dei dati, anche se i suoi obblighi, come il documento programmatico di sicurezza informatica sono stati

spesso disattesi e alcuni hanno cessato di essere obbligatori nel 2012.

Il nuovo regolamento europeo viene a sostituire le normative precedenti in tutti i paesi della UE e, per come è stato strutturato, **diviene legge nei vari paesi direttamente, senza alcun bisogno di ratifica da parte dei parlamenti nazionali**. Per questo, essendo il successore del Decreto Privacy di cui amplia aspetti e regole, durante la riunione di un comitato tecnico di cui faccio parte il GDPR è stato soprannominato scherzosamente "Gran Decreto Privacy" :-).

Ad un primo esame, il nuovo regolamento si presenta come estremamente rigoroso, intransigente e, soprattutto, sanzionatorio. Infatti introduce sanzioni molto pesanti per i trasgressori, che possono giungere a multe pari a milioni di euro o al 4% del fatturato globale di un'azienda. In realtà **un esame più approfondito rileva gli indubbi aspetti positivi** del nuovo regolamento, accompagnati comunque anche da caratteristiche negative.

Come molte norme europee **il regolamento è suddiviso fra principi (173 elementi definiti "considerando") e 99 articoli (che definiscono la norma effettiva)** il cui ruolo, senza una precedente lettura dei considerando, non apparirebbe altrettanto chiaro.

Definiamo ora l'ambito di azione del GDPR.

Il GDPR stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Per "dato personale", come specificato nell'articolo 4 dello stesso GDPR, si intende:

> *"(…) qualsiasi informazione riguardante una persona fisica identificata o identificabile", definita subito dopo col termine "interessato".*

Inoltre:

> *"(…) si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di*

identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Quindi **il GDPR si preoccupa della protezione dei dati personali**, immagazzinati con strumenti fisici (es. archivi cartacei) e/o elettronici e **di regolamentare i trattamenti che essi possono subire**. Per "trattamento", sempre nell'articolo 4, il GDPR intende:

"(…) qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Ne consegue che i**l GDPR regolamenta anche i trattamenti di dati che sono alla base del web e social media marketing** e, in generale, anche molti dei trattamenti che hanno luogo grazie ai Big Data (si veda questo articolo del 2015 relativo alla convergenza digitale).
Potremmo dire che lo stesso potere delle più grandi aziende dei nostri tempi viene toccato, almeno sul territorio dell'Unione Europea!

Nello svolgere questo fondamentale compito, però, il GDPR introduce una serie di principi fondamentali e di direttive che vanno ad integrarsi profondamente con molteplici aspetti organizzativi, tecnologici e operativi della vita delle aziende e **ha quindi un impatto ampio. Vediamo di seguito come.**

Aspetti fondamentali della norma sono:

- **Il consenso informato (trasparenza) per gli interessati ai trattamenti**, che devono ricevere in modo chiaro ed esaustivo tutte le informazioni relative ai trattamenti che i propri dati personali possono subire per qualsiasi motivo (ad esempio, analisi mediche, oppure

la gestione della garanzia di un elettrodomestico); non sono più ammessi scenari di consenso "per default": il consenso deve essere sempre espresso direttamente. Come dice il GDPR "i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

- **Il diritto a ricevere informazioni se i trattamenti dei dati cambiano da parte degli interessati e il diritto dei medesimi ad opporsi** al nuovo uso dei dati nei nuovi trattamenti. I dati "sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità". Quindi non è più possibile, ad esempio, travasare i dati raccolti per una certa finalità in un nuovo archivio dove saranno usati per tutt'altro, senza l'esplicito ed informato consenso degli interessati.
- **Minimizzazione dei dati:** i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali i dati sono trattati; quindi se in un certo

processo di trattamento dei dati certe informazioni non sono necessarie, è bene che non siano nemmeno presenti.

- **I dati devono essere esatti e, se necessario, aggiornati**: devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; a questo proposito esistono purtroppo tantissimi casi, recenti e meno recenti, di persone che hanno subito danni per errori nei dati che li riguardavano.
- **I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati; quindi non è più possibile conservare certi dati a tempo indefinito, solo a titolo di esempio, a molti di noi ancora capita di ricevere lettere pubblicitarie indirizzate a propri cari defunti da anni.
- **I dati devono essere trattati in maniera da garantire un'adeguata sicurezza** dei dati

personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). In caso di danni o altro i titolari dei trattamenti sono tenuti a informare gli interessati. In altre parole i dati devono essere protetti da danni accidentali, da furti o danneggiamenti volontari, da abusi. E, in caso questi accadano, sia gli interessati, sia il Garante della Privacy ne devono essere informati (con rischi enormi sulla reputazione della organizzazione). Questo prosegue ed amplia principi e compiti già stabiliti nel DPR del 2003.

- **Principio di "responsabilizzazione"**: i titolari del trattamento, ossia le aziende che gestiscono e trattano i dati, ovvero i loro rappresentanti legali, sono competenti per il rispetto di tutti gli obblighi suddetti e devono essere in grado di dimostrare tale rispetto.

Il punto 7 rappresenta una rivoluzione rispetto a molte situazioni oggi esistenti, da

cui discendono tutta una serie di conseguenze, non ultime le minacce delle sanzioni. Il dover essere in grado di dimostrare che si sta "lavorando in modo lecito, corretto, esatto, sicuro e responsabile" con i dati significa in sostanza:

1. **Dover conoscere tutti i trattamenti di dati in corso presso la propria organizzazione e quindi conoscere e poter dimostrare a richiesta**:

   a. *quali dati vengono trattati e in che modo sono rappresentati;*

   b. *per quale finalità sono trattati;*

   c. *entro quali processi aziendali sono trattati;*

   d. *con quali strumenti, informatici e non, sono trattati;*

   e. *chi (quali persone entro l'organizzazione) li trattano, con quale ruolo;*

   f. *quali strumenti di sicurezza sono posti a garantire la riservatezza, la esattezza e la disponibilità di tali dati.*

2. **Mettere in atto (o avere in atto se si è già provveduto) tutte le misure necessarie**

per poter dimostrare tutte le informazioni del punto precedente e per poterle gestire ed aggiornare, mantenendole coerenti con i trattamenti esistenti man mano che essi si evolvono.

3. **Mettere in atto tutte le misure necessarie per fornire il consenso informato** agli interessati e per raccogliere la loro autorizzazione esplicita.
4. **Impostare i processi necessari per tenere i dati aggiornati ed esatti** o per integrarli o per cancellarli in base alla eventuale richiesta degli interessati.

Questi ed altri compiti vengono esplicitati nel GDPR, ad esempio, attraverso l'introduzione nell'articolo 30 del Registro del Trattamento. Questo è molto di più del documento programmatico di sicurezza del vecchio Decreto Privacy, in quanto:

1. **Deve tenere traccia in modo adeguato di tutte le operazioni di trattamento** effettuate all'interno della singola organizzazione (come definito sopra).

2. **Deve costituire uno strumento operativo di lavoro**, per censire le raccolte di dati esistenti in azienda e che deve tenersi sincronizzato con la evoluzione di queste.
3. **Rappresenta anche un documento probatorio** con il quale il titolare dei dati può dimostrare, ad esempio, in caso di ispezione, di avere adempiuto alle prescrizioni del GDPR.

Inoltre, ad esempio **nell'articolo 25, il GDPR regolamenta anche i nuovi trattamenti**, successivi alla sua adozione in azienda, esprimendo alcuni principi come:

1. **La privacy sin dalla progettazione e per impostazione predefinita**: in tutti i nuovi progetti di trattamenti di dati la privacy deve fare parte dei requisiti obbligatori e deve essere il caso di default; in pratica quindi tutto deve essere pensato partendo dalla privacy e sono eccezioni da giustificare i casi in cui la riservatezza dei dati è meno importante di altre caratteristiche.
2. **La protezione dei dati sin dalla progettazione e per impostazione**

predefinita: in tutti i nuovi progetti devono essere tenuti presente obbligatoriamente i principi di protezione e conservazione dei dati, complemento indispensabile della privacy.

3. **Deve essere svolta una adeguata analisi dei rischi**.

Questi principi rappresentano una rivoluzione del modo di progettare i trattamenti dei dati, anche se sono conformi pienamente ai principi espressi da normative internazionali come ISO27001 (la sicurezza informatica) e ISO31000 (la gestione del rischio) e, in generale, ai temi della qualità espressi dalla normativa ISO9001 nella nuova versione del 2015.

In pratica quindi tutto questo significa che la piena conformità al GDPR non può essere svolta attraverso la mera scrittura di documenti fini a se stessi, ma richiede una serie di interventi di adattamento che agiscono a livello di processi (organizzazione aziendale), di risorse umane, di gestione dei rapporti con clienti e fornitori, oltre che di IT. Il progetto di adeguamento deve

essere gestito con tutti i principi del buon Project Management (ad esempio la ISO21500).

A partire da tali presupposti, possiamo ignorare il GDPR?

Si, certo, possiamo farlo, ma **correndo il rischio di multe salate e danni di immagine molto ampi**, oltre che il fatto che fornitori o clienti di altri paesi europei, che si stanno già adeguando al GDPR, possano farci causa in caso di incidenti coi dati, o di usare la loro conformità come fattore competitivo.

In sostanza il GDPR deve essere visto più come una opportunità per migliorare il proprio modo di lavorare e per rendere più sicura la propria IT (**si ricordi l'articolo precedente**), **più che non come l'ennesimo "male necessario".**

Alcuni aspetti citati del GDPR sono profondamente legati ad altre caratteristiche della Governance dei Sistemi e della Progettazione IT e

saranno oggetto di approfondimento in successivi articoli.


DATA PROTECTION & IT

O7. GDPR e requisiti nei progetti IT: il quadro della situazione.

Nei precedenti articoli abbiamo visto alcune delle problematiche di sicurezza, diretta ed indiretta, legate agli strumenti IT e introdotto il regolamento europeo GDPR (General Data Protection Regulation), soprannominato anche "Gran Decreto Privacy".

In questo articolo **concentriamo l'attenzione su alcune delle richieste che il GDPR pone per i nuovi trattamenti di dati successivi alla sua definitiva entrata in vigore: la privacy e la data protection by design e by default**.

La privacy e la protezione dei dati diventano parte integrante di ogni trattamento sin dalla progettazione e per impostazione predefinita. E deve essere svolta una adeguata analisi dei rischi. Ciò è conforme pienamente ai principi espressi da normative internazionali come ISO27001 (la sicurezza informatica) e ISO31000 (la gestione del rischio) e, in generale, ai temi della qualità espressi dalla normativa ISO9001

nella nuova versione del 2015. E rientra nelle buone pratiche suggerite dai framework come ITIL e COBIT e dai principi degli standard di Project Management come PMBoK, Prince2, ISO21500 etc.

Le conseguenze e i vincoli introdotti.

In un progetto di servizio IT che automatizza un trattamento di dati e considerando anche eventuali fasi manuali al suo interno **occorre inserire fra i requisiti essenziali la data protection e la privacy.**

Per capire meglio cosa questo significa **partiamo dalle premesse**: un progetto IT, in questo caso di nuovo trattamento dei dati, **parte necessariamente da una serie di requisiti da soddisfare**, legati alle ragioni di business aziendale cui è associato l'obiettivo del processo. **Questi requisiti**, integrando quanto il GDPR chiede negli standard di Business Analysis, **possono essere suddivisi nelle seguenti categorie:**

- ✓ ***Requisiti funzionali espliciti:*** sono le esigenze funzionali che il servizio IT deve soddisfare per generare valore per chi lo usa; un esempio, in un servizio web e-commerce, è descrizione della form di iscrizione al sito stesso.
- ✓ ***Requisiti funzionali impliciti:*** sono esigenze funzionali che tendiamo spesso a dare per scontate, ma che sono comunque molto importanti; un esempio sono le regole di profilazione degli utenti che accedono ad un sistema, che definiscono i diritti di accesso alle varie categorie di dati per i singoli profili degli utenti.
- ✓ ***Requisiti non-funzionali:*** sono caratteristiche tecniche ed organizzative che il servizio IT dovrà rispettare; un esempio sono le piattaforme su cui una app deve operare (iOS, Android, Windows Phone…).
- ✓ ***Requisiti di qualità***, fra cui includere anche quelli di sicurezza: sono la parte che ITIL definisce come "garanzia" di un serv**izio e rappresentano la qualità del servizio stesso. Tra questi i più importanti sono:**

– ***la disponibilità (availability) di un servizio***, ossia l'intervallo in cui il servizio è disponibile per gli utenti, che può essere, per esempio, orario di ufficio oppure 24x7x365 (tutto il tempo dell'anno);

– ***la capacità (capacity) di un servizio***, ad esempio il numero massimo di utenti che possono collegarsi simultaneamente, il numero massimo di documenti memorizzabili etc.;

– ***l'affidabilità (reliability), ossia la capacità di un servizio di funzionare rispettando tutte le specifiche*** che lo definiscono in modo costante nel tempo (ad esempio, il tempo di esecuzione di una data funzione dovrebbe mantenersi ragionevolmente costante anche al crescere del numero di utenti collegati);

– ***la sicurezza (security) del servizio***, sia rispetto ad eventi accidentali (ad esempio, guasti di componenti hardware) ed attacchi deliberati (azione di pirati informatici, virus etc).

Affidabilità e sicurezza sono in sostanza quanto richiesto dal privacy e data protection by default.

In particolare queste due caratteristiche si traducono nelle seguenti qualità da mantenere per i dati:

- ✓ ***disponibilità del dato:*** il dato è fruibile per gli utenti attraverso il servizio IT che lo tratta, se questo non sta funzionando, il dato è inaccessibile; anche se il dato è salvato nel backup, occorre tempo per ripristinare il funzionamento del servizio IT e ri-immettervi il dato rendendolo nuovamente disponibile per gli utenti; si pensi, ad esempio, ad un contesto sanitario dove la cartella clinica di un paziente deve essere disponibile per tutti quanti sono coinvolti nella cura del paziente stesso;
- ✓ ***riservatezza del dato:*** il dato deve essere accessibile solo alle persone il cui ruolo prevede l'accesso al dato stesso; ovviamente possono esistere ruoli abilitati ad accedere a una quantità maggiore di dati rispetto ad altri; ad esempio, in un archivio del personale l'ufficio HR ha accesso a tutti i dati delle

persone memorizzate, mentre altre funzioni non possono vedere indirizzi e stipendi;

- ✓ ***integrità del dato:*** il dato deve essere protetto rispetto a modifiche del contenuto, accidentali (involontarie) oppure effettuate volontariamente in modo non autorizzato (ad esempio, si pensi all'azione di virus, dai cripto-locker come WannaCry ai virus subdoli che scambiano tra loro in modo casuale le righe di testo dei documenti che attaccano, oppure all'azione di un pirata informatico che modifica i voti di un concorso pubblico);
- ✓ ***esattezza del dato:*** il dato deve essere esatto (ossia contenere dati personali corretti) ed aggiornato; pensiamo per esempio a tutte le problematiche legate alle utenze di servizi come gas ed elettricità quando il nominativo del titolare non è riportato correttamente dentro i sistemi che elaborano i dati;
- ✓ ***conformità del dato:*** il dato deve essere espresso in una forma conforme alle leggi ed ai regolamenti; ad esempio, nell'ambito di alcune transazioni finanziarie la precisione dei numeri

con la virgola deve essere di almeno 6 cifre decimali.

A tali requisiti **si aggiungono due ulteriori qualità** per la salvaguardia dei dati:

– **RTO: tempo totale necessario per il ripristino della piena funzionalità di un servizio IT**, comprensivo dei dati in esso contenuti, in caso di incidente; è composto da varie fasi, dall'individuazione dell'incidente o malfunzionamento a tutto quanto serve per ripristinare la piena funzionalità del servizio che tratta i dati e quindi la piena disponibilità di ogni dato in esso memorizzato.

– **RPO: tempo nel passato cui è possibile tornare con il ripristino dei dati**, significa che in caso di incidente grave che comporta la distruzione di un archivio dati, il backup periodico deve garantire la possibilità di ritornare ad un dato momento nel passato.

Se, ad esempio, salviamo il contenuto di un disco di un PC a mezzanotte e poi un guasto cancella tutti i dati alle 10 del giorno dopo, sarà possibile

ripristinare solo i dati come erano a mezzanotte; esistono sistemi (costosi) in cui l'RPO è meno di un minuto, il che significa praticamente che non si possono perdere dati.

Andiamo oltre: analisi del rischio.

Le qualità definite nel paragrafo precedente sono ciò cui è necessario tendere. Questo significa che **dobbiamo da un lato definire quali valori per ciascuna delle qualità sopra definite sono necessari per ogni trattamento dei dati e dall'altro valutare il rischio di uscire da valori**, a causa di eventi accidentali come, ad esempio, i guasti software e hardware o di eventi deliberati come i virus o gli attacchi informatici.

Questo si può attuare con **un processo standardizzato chiamato gestione del rischio (Risk Management)**, definito nello standard ISO 31000. Possiamo definire in breve l'analisi, gestione e prevenzione/riduzione del rischio (Risk Assessment, Management e Treatment) con un proverbio: "Prevedere il peggio per gioire del meglio".

Infatti la gestione del rischio prevede di:

- ***individuare**, basandosi su esperienza, buone pratiche e altre metodologie codificate, **tutti i rischi**, ossia gli eventi (casuali e non) che possono alterare il risultato atteso;*
- ***quantificare l'impatto**, ossia l'effetto dannoso di tali eventi sulle qualità del servizio sopra descritte;*
- ***quantificare la probabilità del verificarsi di tali eventi**;*
- ***attribuire un peso al rischio** combinando insieme probabilità ed impatto (esistono varie formule standard per questo);*
- ***individuare i rischi con peso più alt**o, definendo quindi quali sono i rischi "importanti" che richiedono contromisure e quali invece i rischi "accettabili";*
- ***stabilire quali azioni possono ridurre la probabilità** o l'impatto o entrambi per questi rischi, ed il loro costo;*
- ***applicare queste contromisure** e stabilire il nuovo peso del rischio.*

Il GDPR prevede che queste analisi del rischio debbano essere fatte prima di ogni progetto di nuovo trattamento. In realtà poi l'analisi del rischio viene ripetuta periodicamente, all'interno di un processo di miglioramento continuo.

Applichiamo ora il GDPR.

Tutti i requisiti di sicurezza del dato, seguendo il GDPR, vanno affrontati in modo completo e organico fin dall'inizio.

Vediamo ora insieme ***una possibile sequenza di passaggi con un esempio legato all'azione di un ufficio clienti*** presso un'azienda che si rivolge a clienti finali e che vende ad essi.

Supponiamo dunque che il trattamento da progettare ex novo sia l'archivio clienti di un particolare prodotto con una garanzia di assistenza gratuita di 24 mesi dopo l'acquisto, e focalizziamo l'attenzione sui requisiti richiesti dal GDPR, in particolare per security e privacy:

- **Anzitutto circoscriviamo il perimetro, partendo dallo scopo del trattamento** che è legato ad un particolare contratto ("liceità") e che prevede che i dati saranno conservati per 12 mesi dopo la cessazione del rapporto commerciale. I dati sono personali (relativi a persone fisiche), quindi soggetti a tutte le regole del GDPR.
- **I dati devono essere raccolti all'atto della stipula del contratto**, corredato del consenso informato con tutte le specificazioni richieste dal GDPR. La firma del contratto è completata con la firma specifica del consenso informato. La copia di contratto e consenso informato firmata dal cliente è raccolta, scansionata e poi depositata in archivio cartaceo a parte, mantenuto sotto chiave.

- **Le copie dei contratti raccolti devono essere tenute in contenitori chiusi durante il trasporto verso i sistemi dove avviene la scansione**, onde evitare che persone non autorizzate vedano i dati personali in essi scritti.
- **I dati vengono inseriti da persone autorizzate** che ricevono la trasmissione della scansione. La copia della scansione ricevuta dagli addetti, ultimata l'operazione di inserimento, viene cancellata.
- A questo punto occorre applicare tutti i principi ai dati: l'archivio dei dati, costruito ad hoc, deve applicare i principi di pseudonimizzazione e minimizzazione dei dati stessi. **Il servizio IT e le sue componenti devono essere protetti da guasti accidentali e da attacchi informatici.**
- **Occorre ora un'analisi del rischio**, tesa a stabilire le conseguenze rispetto ai principi del GDPR di eventi infausti:
  - ✓ ***una eventuale corruzione o perdita dei dati impedirebbe la godibilità della***

garanzia *e quindi la violazione degli accordi contrattuali, violando anche il GDPR,*

- ✓ ***un eventuale trafugamento di dati violerebbe la privacy dei clienti*** *e costringerebbe l'azienda alla comunicazione esplicita a tutti i propri clienti ed al garante di quanto avvenuto, con la conseguente perdita di reputazione.*

❖ Con i risultati del punto precedente **diventa necessario inserire tra i vari requisiti tutti quelli funzionali, non funzionali e di qualità tesi ad applicare una sicurezza** adeguata. Potremo quindi prevedere:

- ✓ ***Firewall a protezione dei sistemi*** *che contengono i dati.*
- ✓ ***Crittografia applicata sulle connessioni*** *di accesso ai sistemi.*
- ✓ ***Eventuale crittografia applicata entro il database*** *per evitare che accessi non autorizzati ad esso possano portare a trafugamento o modifiche di dati.*
- ✓ ***Regole di accesso ferree per l'applicativo:*** *gli addetti al trattamento dati*

possono vedere solo i dati specifici necessari per svolgere la loro funzione aziendale.

- ✓ ***Controlli di qualità sul sistema con vulnerability assessment*** *da realizzare periodicamente e processi di aggiornamento e gestione delle non conformità riscontrate.*
- ✓ ***Politiche di backup e ripristino opportune****, tese a minimizzare la probabilità di perdita di dati e, allo stesso tempo, a migliorare i valori di RPO e RTO.*
- ✓ ***Politiche opportune di scelta e gestione delle password****.*

❖ Infine, **i ruoli di accesso dovranno essere distribuiti opportunamente** rispetto alla privacy.

Per concludere:

L'esempio pratico appena esposto rende manifesto come – introducendo le buone pratiche di analisi del rischio, rispetto dei requisiti di sicurezza e privacy fin dall'inizio del progetto, ed applicandovi opportunamente le regole metodologiche e tecniche – s**i è in regola anche rispetto al GDPR, oltre a costruire servizi IT**

di trattamento dati di qualità e funzionamento migliore.

Tutto questo – concludiamo – ha un costo superiore rispetto alla disattesa di tali prassi? Sicuramente sì, ma è necessario considerare il rapporto costi/benefici non soltanto all'inizio, ma durante tutto il ciclo di vita del servizio IT.

NB: nel prossimo articolo tratteremo le conseguenze del GDPR sull'IT Service Management ossia sulla gestione dell'esercizio dei servizi IT.

08. GDPR IT Service Management: la progettazione dei nuovi Servizi IT nel rispetto della normativa.

Il quadro della situazione.

Nei precedenti articoli, **dopo una visione delle problematiche di sicurezza, diretta ed indiretta**, legate agli strumenti IT, **abbiamo focalizzato l'attenzione sul Regolamento Europeo GDPR** (General Data Protection Regulation), soprannominato anche "Gran Decreto Privacy", e **sulle sue conseguenze rispetto alla progettazione di nuovi servizi IT** per il trattamento dati.

In questo articolo **concentriamo l'attenzione su alcune delle richieste che il GDPR pone per i trattamenti dei dati in essere**, specialmente per le persone che li svolgono usando gli appositi servizi IT:

- ✓ ***la sicurezza dei dati;***

- ✓ ***il principio di responsabilità (accountability).***

Sicurezza che non **vale** solo per i trattamenti nuovi, progettati dopo il maggio 2018, ma **per tutti i trattamenti di dati personali in essere** presso un'azienda od organizzazione.

L'obbligo della sicurezza.

In particolare partiamo dall'articolo 32 del GDPR, il cui paragrafo 1 afferma: ***"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento****, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche,* ***il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza*** *adeguato al rischio…"*

Cosa significa in pratica questo? Che:

1. **Occorre una adeguata analisi del rischio**, che presuppone la conoscenza
   - *dei trattamenti in essere,*
   - *delle loro finalità,*
   - *di chi li svolge (e con quale ruolo),*
   - *di quali strumenti e servizi IT sono usati per tali trattamenti.*
2. **L'analisi del rischio deve portare a determinare probabilità e impatto dei rischi che incombono** rispetto ai diritti e le libertà delle persone.
3. **Devono essere predisposte le adeguate contromisure e quindi**, per ogni singolo trattamento, sempre dall'articolo 32:
   - ✓ *"la capacità di **assicurare** su base permanente **la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi** e dei servizi di trattamento";*
   - ✓ *"la capacità di **ripristinare** tempestivamente **la disponibilità e l'accesso dei dati** personali in caso di incidente fisico o tecnico";*

- ✓ ***"una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche*** *e organizzative al fine di garantire la sicurezza del trattamento".*

Inoltre, **per le aziende con più di 250 dipendenti o in cui i trattamenti sono a rischio per i diritti degli interessati**, come ad esempio commercialisti, studi di medicina del lavoro, assicurazioni e altri, **vale anche l'obbligo di realizzare un registro dei trattamenti contenente informazioni** come:

- ✓ "***il nome e i dati di contatto del titolare del trattamento*** *e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati";*
- ✓ "***le finalità del trattamento****";*
- ✓ "***una descrizione delle categorie di interessati e delle categorie di dati personali****".*

Una serie di informazioni, dunque, che completano quanto visto prima. L'articolo 30 del

GDPR, che definisce tale registro, prosegue elencando altre informazioni, tra cui:

- ✓ "*ove possibile,* ***i termini ultimi previsti per la cancellazione delle diverse categorie di dati****";*
- ✓ "*ove possibile,* ***una descrizione generale delle misure di sicurezza tecniche e organizzative*** *di cui all'articolo 32, paragrafo 1" riallacciandosi, quindi, a quanto abbiamo visto sopra.*

Le conseguenze.

Un'azienda deve:

- ❖ **Conoscere obbligatoriamente i trattamenti dei dati** al proprio interno.
- ❖ **Poter fare un'analisi del rischio** (descritta nell'articolo precedente) per ciascun trattamento e prendere le eventuali contromisure adeguate.

Ovvero **l'azienda deve conoscere bene sè stessa ed i processi entro cui avvengono i**

trattamenti dei dati. Il lavoro per realizzare una base di conoscenza che consenta questo è ampio e non può essere visto semplicemente come un mero adempimento ad un obbligo di legge. Va visto come **un investimento per migliorare la propria efficienza e la propria robustezza.**

Infatti, combinando insieme il tutto, osserviamo che:

1. Conoscere i processi (e le attività interne ad essi) in cui avvengono i trattamenti significa **avere una mappa dei processi conforme alla ISO9001** e avere coincidenza fra quanto è scritto e quanto si fa;
2. Conoscere i trattamenti e le loro finalità di business significa **conoscere il valore che i trattamenti hanno per l'azienda**;
3. Conoscere la base giuridica significa **avere consapevolezza delle leggi e avere i documenti legali** (contratti, consensi informati) associati ai trattamenti;
4. Conoscere le categorie di dati trattati e gli interessati e definire i termini di conservazione

dei dati stessi significa **conoscere in modo preciso l'uso operativo dei dati**;

5. Conoscere i referenti interni e chi tratta i dati significa **avere stabilito una catena di responsabilità entro l'organigramma** (come previsto dagli standard sui processi come ISO15504);
6. Conoscere i referenti esterni significa a**vere un legame tra la mappa dei fornitori ed i servizi di trattamento che questi offrono** (condizione obbligatoria nelle buone pratiche di ITIL e di altri framework per la gestione dell'IT);
7. Conoscere le categorie di destinatari dei dati significa **conoscere i flussi di dati che partono dall'azienda**, sia interni, sia oltre i confini dell'Unione Europea;
8. Conoscere le modalità di trattamento dei dati significa **conoscere gli strumenti tecnici (applicativi, servizi IT, interni ed esterni all'azienda) che vengono utilizzati per trattare i dati stessi**; in questo caso avviene quindi una integrazione con il catalogo dei servizi previsto dagli standard come ITIL;

9. Conoscere le misure di sicurezza significa **avere sotto controllo la sicurezza dell'azienda** e poter dimostrare di avere preso le misure idonee a ridurre al minimo i rischi.

Appare evidente da tutto questo come **il GDPR è conforme** (o, per meglio dire, ispirato) **alle buone pratiche di framework internazionali** come ITIL, COBIT e PMBoK e agli standard di sicurezza (ISO27001), di gestione del rischio (ISO 31000) e della privacy (ISO 29000).

Un esperto di normative ha definito il GDPR come "una normativa ISO imposta per legge e che trasuda ISO da tutte le parti".

Un esempio operativo.

Con riferimento all'esempio dello scorso articolo sull'archivio clienti, supponiamo che tale archivio esista già. C**ome possiamo applicare i punti sopra descritti?**

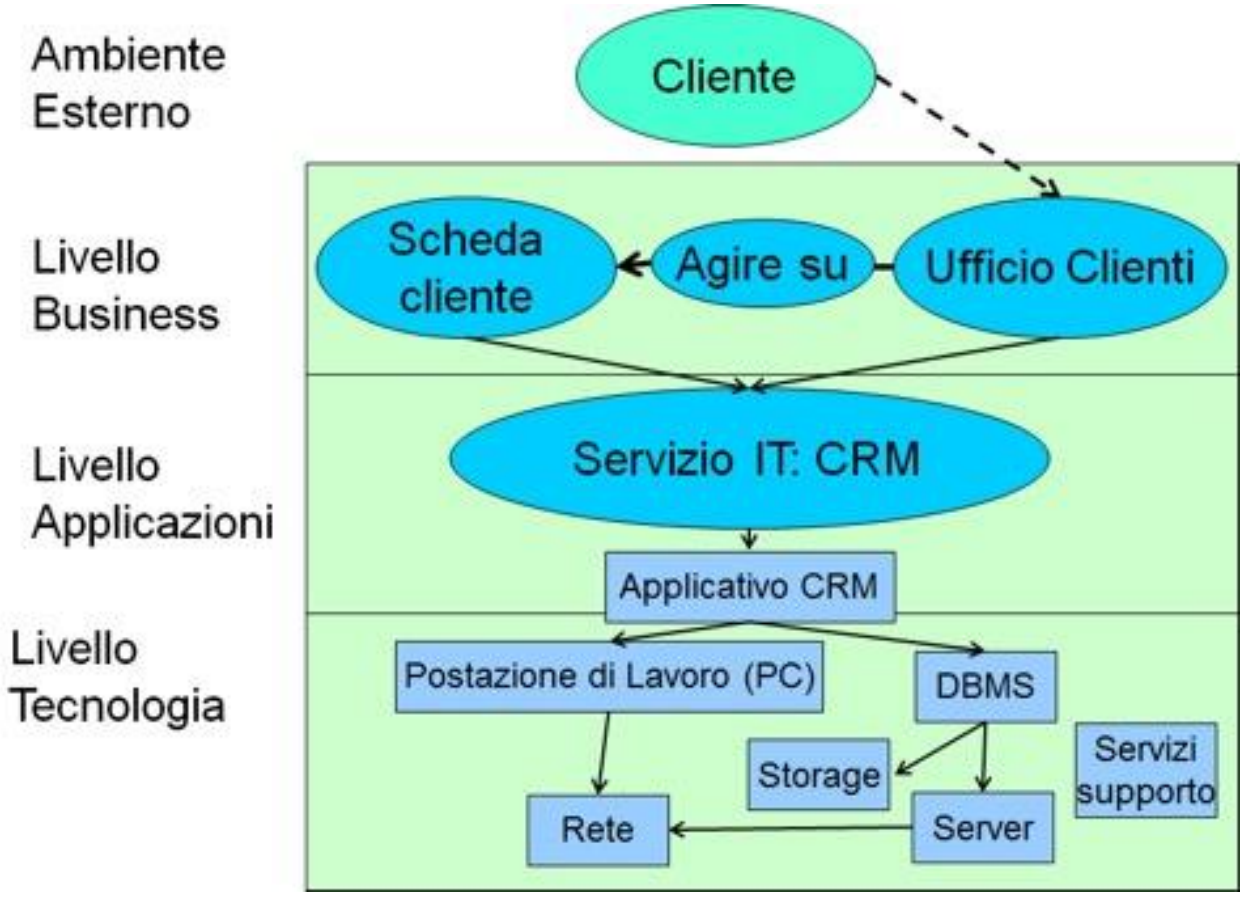
Nella figura è descritto in modo molto semplificato l'uso del catalogo dei servizi ITIL,

con una mappa ispirata alla architettura enterprise di TOGAF, applicato all'esempio corrente.

1. **Il cliente ha bisogno di un servizio di assistenza** ed interpella l'ufficio clienti attraverso una mail, una telefonata o l'apertura di una richiesta (ticket) su un portale Web di assistenza.
2. **L'ufficio clienti a sua volta ha bisogno**, per poter esaudire la richiesta del cliente, **di agire sulla scheda cliente** (insieme di dati personali ed altro), contenuta nel servizio IT CRM.
3. **Il Servizio CRM** è composto dall'applicazione software (applicativo) CRM che, **per funzionare, necessita della postazione di lavoro (tipicamente il PC)** che l'impiegato dell'ufficio clienti usa e, a livello più tecnico, del database, ossia lo strumento IT che contiene i dati;
4. **Il database opera entro un server ed utilizza un sistema di storage**, ossia

memorizzazione permanente; senza tali componenti non potrebbe operare ed i dati non sarebbero disponibili (violazione dell'articolo 32 e dei diritti del cliente);

5. **Sia la postazione di lavoro, sia il server hanno bisogno della rete per comunicare fra loro**; quindi entrambi dipendono dalla rete, come indicato dalle frecce;
6. **Il buon funzionamento di tutte le componenti è garantito dai servizi di assistenza e supporto**.



Seguendo lo schema **possiamo farci alcune domande relative alla sicurezza**:

- **L'impiegato è adeguatamente addestrato per compiere tutte le operazioni** che il ruolo di assistenza cliente richiede?
- Come l'impiegato accede al servizio IT CRM? Che tipo di credenziali sono utilizzate? Sono mantenute al sicuro? Quanto frequentemente sono cambiate?
- **Qualora l'impiegato sia in ferie o in malattia il sostituto può svolgere il suo compito senza conoscere le sue credenziali**, ma con altre credenziali che lo identifichino univocamente?
- Qualora l'impiegato stampi una scheda cliente contenente dei dati personali, **esiste una procedura per minimizzare il rischio di accesso non autorizzato a questa stampa?** Ad esempio, viene tenuta sotto chiave o in bella vista sulla scrivania?
- **L'impiegato può accedere solo ai dati che gli servono per il suo ruolo o anche ad altri?** Riallacciandoci al principio della

minimizzazione e rovesciando la questione: nel sistema sono presenti più dati personali di quelli che effettivamente servono?

- **Che misure vengono prese per garantire il buon funzionamento dei componenti tecnici come il database o il server?** In caso di guasto, in quanto tempo il servizio può essere ripristinato (RPO e RTO, si veda l'articolo precedente)?
- **Che misure di protezione vengono prese rispetto ad attacchi deliberati ai sistemi e/o ai dati?** Ad esempio, che antivirus sono in dotazione?
- Che contratto esiste con i servizi di supporto? I suoi termini sono conformi al GDPR? Che livelli di servizio sono garantiti? E che tipo di accesso ai dati del database possono avere i servizi di supporto?
- **Tutti questi aspetti sono verificati periodicamente**?

Queste sono solo alcuni **esempi di domande che è necessario porsi come base per un'analisi del rischio**, primo passo verso

l'adozione di opportune misure di sicurezza, se necessarie, o verso la convalida di una situazione esistente, se "adeguatamente" sicura.

Passare al GDPR.

Non dobbiamo mai dimenticare che il GDPR chiede ai titolari ed ai responsabili del trattamento di essere in grado di dimostrare di avere messo in atto ***"misure tecniche ed organizzative adeguate"*** e **non minime!**

Quindi, sicuramente, per giungere alla conformità prevista dal GDPR il primo passo è conoscere sé stessi, ovvero conoscere la propria azienda e

sapere come funziona. Ed **ecco perché il passaggio al GDPR comprende aspetti legali, organizzativi, tecnici e formativi delle risorse umane. L'approccio non può che essere multidisciplinare** e i responsabili delle funzioni operative aziendali, che conoscono il funzionamento quotidiano dei processi, devono essere coinvolti nel processo di adeguamento. **Ed è necessaria una "cabina di regia", in grandi organizzazioni, guidata dall'ufficio qualità o compliance.**

Presto saranno trattati aspetti legali per il GDPR mentre nel prossimo articolo tratteremo il concetto di servizio, dentro e fuori l'azienda, e il passaggio del mercato verso una logica "universale" del servizio.

Conclusioni

Il settore dell'Information Technology (It) guida la trasformazione digitale del paese. Come leggiamo a questo link: *"Gli investimenti in progetti di digital transformation, a livello mondiale, raggiungeranno i 2.200 miliardi di dollari nel 2019, [...]. Già in un'anteprima di un paio di giorni fa, era emerso il dato relativo all'Italia, dove il mercato dell'Information technology (IT) per quest'anno dovrebbe registrare un +3,1%, per un valore complessivo di 22,7 miliardi."*

Uscito dalla crisi 2008 -2014 grazie a un processo di trasformazione evolutiva che ha generato potenzialità innovative ed elevate competenze, cruciali per sostenere la digitalizzazione del Paese, il settore ICT è tornato ad assumere un ruolo strategico nel sostenere la digitalizzazione del paese, contribuendo in modo rilevante al suo Pil.

La ripresa rischia purtroppo una brusca frenata. In vista dell'appuntamento elettorale del 2018 i piani di investimento per il nuovo anno da parte delle aziende

del settore sono all’insegna della prudenza, con riduzione del budget.

La mancata trasformazione digitale della PA resta la principale criticità nonché la questione delle competenze.

E l'adeguamento, più che mai attuale, del GDPR? L’attenzione è alta, e lo dimostra la serie di wokshop e seminari dedicati all’argomento. Ma a che punto siamo arrivati in Italia? Il nostro Paese **avanza con lentezza e in modo scoordinato nell’armonizzazione della disciplina nazionale con il GDPR. Le carenze si riscontrano in quanto:**

- **c'è poca chiarezza sul Responsabile del trattamento** (quasi sempre indicato con l’acronimo dalla versione inglese **DPO**) e,
- **sono troppo generiche le norme sul riutilizzo dei dati sanitari, in forma anonima, per scopi statistici e di ricerca.**

Tutelare l'importanza dei dati di produzione e non, è divenuta misura cautelativa sempre più cruciale per ogni azienda e, **proprio in vista dell'applicazione del regolamento GDPR, notevole diffusione sta avendo la tecnica del data masking**.

Il data masking è una tecnica che consiste **nel nascondere i dati sensibili originali con dati fittizi**. Può prevedere la sostituzione dei dati con dati simili, la sostituzione dei dati con dati casuali o il rimescolamento dei dati fra loro allo scopo di rendere i dati non correlabili a un'identità originaria, pur mantenendo la validità delle informazioni.

I dati devono infatti essere sempre fruibili e significativi, rispettando il contesto e gli obiettivi di utilizzo.

Novità e impegno non mancano, dunque, ma: *"Oggi l'instabilità politica pesa molto di più in termini di punti di Pil, di credibilità e quindi di investimenti. E nella maratona digitale l'Italia non può permettersi di farsi superare più di quanto non abbia già fatto."*

Sitografia

Per le normative e i decreti legge fare clic sul nome per connettersi al documento che riporta il testo.

- www.wikipedia.org
- Giulio Destri, "Sistemi Informativi. Il pilastro digitale di servizi ed organizzazioni", Ed. FrancoAngeli, 2013
- www.certificazioneprofessioni.org
- Testo del GDPR in Italiano
- Portale EUROPRIVACY
- Portale del Garante Italiano della Privacy
- Lo standard ISO31000 del Risk Management

About

GIULIO DESTRI

Giulio Destri è ingegnere elettronico e Ph.D. in ingegneria informatica.

Opera come Business Advisor nel settore ICT e dei sistemi informativi e tecnologici interni ad aziende e pubbliche amministrazioni.

Dal 2003 è professore a contratto di Sistemi Informativi presso l'Università di Parma, per la quale ha scritto anche il libro di testo 'Sistemi informativi. Il pilastro digitale di servizi e organizzazioni'.

Dal 2008 ha iniziato a svolgere attività di mentoring e business coaching.

È certificato Oracle, ITIL, COBIT, SCRUM Master, NLP Coach con specializzazione in Business e Team Coaching, ed esaminatore UNI11506-UNI11621.

Appassionato di arti marziali e trekking, scrive articoli, racconti e poesie e gli piace fare fotografie di viaggi e paesaggi.

MAPS GROUP

Dai *Big Data* ai *Relevant Data*, il gruppo sviluppa sistemi *software* che creano conoscenza a supporto dei processi decisionali. I prodotti Maps Group strutturano il patrimonio di informazioni di aziende private e Pubbliche Amministrazioni in *Data Warehouse*, gestionali ed analitici, che si pongono come strumenti di *governance* e di *business.*

6MEMES

Quando si parla di Dati, l’attenzione si sposta su questioni numeriche o, al limite statistiche, ma sotto a quest’algida apparenza la realtà è un’altra.

Il blog 6Memes, dedicato all’opera Six Memos for the Next Millennium di Italo Calvino, vuole mettere a nudo le potenzialità dei Dati, traducendoli nei linguaggi dell’Uomo: Cultura, Natura, Economia, Arte e, perché no, Ironia.

memes

MAPS GROUP

www.mapsgroup.it