

STRATEGIA GLOBALE E LA CRESCITA DIGITALE

Il progetto nazionale dell'agenda digitale è entrato a far parte dei grandi progetti per crescita

dell'occupazione, della qualità della vita, di una presa di coscienza generazionale e democratica. Se poniamo al centro del progetto cittadini, imprese e il concetto di una vera innovazione tecnologica possiamo ritenere la strada del digitale un investimento pubblico

che coincide immediatamente con una riforma strutturale del Paese. A partire da questo numero e per prossimi necessari voglio focalizzare lo stato generale della digitalizzazione nella pubblica amministrazione e nei settori privati.

- Le azioni per una crescita digitale
- *Sistema Pubblico*
- *Sicurezza*
- *Consolidamento data center e cloud computing*
- *Servizio Pubblico d'Identità Digitale (SPID)*
- *Anagrafe*
- *Pagamenti elettronici*
- *Fatturazione elettronica PA*
- *Fatturazione B2B*
- *Open Data*
- *Sanità digitale*
- *Scuola Digitale*
- *Giustizia Digitale*
- *La casa del cittadino*
- *Le competenze digitali*
- *Smart City*

In questa parte affronteremo con Voi i seguenti argomenti:

- Le azioni per una crescita digitale
- *Sistema Pubblico*
- *Sicurezza*
- *Consolidamento data center e cloud computing*

Nel settore privato è necessaria una strategia territoriale sulla ricerca, l'innovazione e la competitività del sistema produttivo. In quest'ottica, deve realizzarsi una piena sinergia con le strategie pubbliche in essere, sia di pertinenza del governo nazionale sia di competenza regionale, che delle amministrazioni locali. Una massima attenzione alle esigenze di modernizzazione e sviluppo digitale di cittadini e imprese italiane, utilizzando il settore pubblico come elemento catalizzatore.

Una buona soluzione potrebbe essere quella di dare più potere all'agID(Agenzia per l'Italia digitale) e utilizzarla per il coordinamento di tutti gli interventi di trasformazione digitale e l'avvio di un percorso di centralizzazione della programmazione della digitalizzazione del Sistema. Diventa di vitale importanza la diffusione di cultura digitale e lo sviluppo di competenze digitali in imprese e cittadini, la modernizzazione della pubblica amministrazione partendo dai processi, superando la logica delle regole tecniche e delle linee guida e puntando alla centralità dell'esperienza e bisogno dell'utenza. E' importante un sistema dinamico che abbia la capacità di adattarsi agli scenari sia nazionali che europei.

E' una questione di PIL !!!

Il mercato del digitale viene indicato come una delle più accreditate ricette anticrisi sia in Italia che in Europa, parliamo addirittura di un valore pari al 3% del Pil/anno, perciò le risorse pubbliche devono servire per promuovere la trasformazione digitale delle imprese italiane e sviluppare le competenze dei cittadini, infatti tutti gli addetti ai lavori sia privati che istituzionali parlano di "crescita digitale" che potrà essere concretizzata da una veloce logica di switch-off del tradizionale. In particolare la pubblica amministrazione dovrà puntare sui seguenti elementi.

- Determinando il progressivo switch off dell'opzione analogica per la

fruizione dei servizi pubblici

- Progettando la digitalizzazione della pubblica amministrazione in un'ottica centrata sull'utente
- Coordinando e mettendo a sistema le diverse azioni avviate da tutte amministrazioni pubbliche
- Garantendo crescita economica e sociale, attraverso lo sviluppo di competenze nelle imprese e di diffusione di cultura digitale fra i cittadini
- Creando nuova domanda capace di generare offerta innovativa e qualificata
- Coordinando in materia unitaria la programmazione e gli investimenti in innovazione digitale e ICT

Un altro elemento importante la diffusione è l'utilizzo dei servizi in rete . In Italia la fascia media degli utilizzatori comprende una età dai 16 ai 24 anni che per la verità si differenzia di circa 10 punti rispetto alla media europea.

Le recenti statistiche, sempre col beneficio degli ultimi aggiornamenti, dal 2011 l'utilizzo di Internet per la ricerca di informazioni sanitarie è cresciuto dal 45% al 60%, così come l'utilizzo del web per leggere informazioni, giornali e riviste è passato dal 50% al 60% nell'ultimo periodo del 2015. Allo stesso tempo, sono cresciuti sensibilmente i servizi finanziari, assicurativi e gli acquisti di beni e servizi. Le relazioni online con la Pubblica Amministrazione, sono il pagamento delle tasse (30%), l'iscrizione a scuole superiori o all'università (25%).

Qual è il grado di soddisfazione dei servizi on-line?

82% di utenti molto o abbastanza soddisfatti

73% rispetto alle pratiche sanitarie a quelle anagrafiche

I servizi più diffusi tramite internet sono:

- la gestione dei certificati medici
- dai servizi per il lavoro
- posta elettronica certificata
- gare d'appalto al 18%
- fatturazione elettronica

Un altro elemento che caratterizza il processo di digitalizzazione è la

razionalizzazione

del patrimonio ICT, consolidamento data center e cloud computing, questo perché il processo di digitalizzazione deve essere sempre accompagnato da una razionalizzazione del suo patrimonio ICT attraverso standardizzazione ed ottimizzazione delle applicazioni, partendo da un'analisi dell'esistente. La straordinaria portata innovativa del cloud computing ha completamente scardinato le modalità di approccio alle architetture IT, rendendo ineludibile, anche per le PA, un percorso conseguente per la trasformazione delle proprie infrastrutture.

Parlare di internet e della diffusione dei servizi ad esso collegato non possiamo prescindere dalla sicurezza dei dati pubblici e personali anche perché i veri rischi di interconnessioni dove le nuove esigenze e le innovazioni tecnologiche sfuggono sempre di più alla regolamentazione sulla privacy e alla sicurezza delle informazioni e cresce, infatti, sempre di più l'appetito dei criminali informatici. Proviamo a considerare le città dei prossimi 20 anni dove i cittadini useranno internet come strumento comune da cui reperire le informazioni dalle più semplici alle più complesse che il più delle volte invadono anche la sfera privata. Quale sarà il grado di sicurezza su cui ognuno potrà contare nello svolgimento delle attività quotidiane come ad esempio gli acquisti on-line, l'uso dei social, il dialogo con la Pubblica Amministrazione. I futuri cittadini saranno sempre più informatizzati, automatizzati e sempre più connessi e passeggiando per le strade cittadine e quindi in luoghi comuni, comunicheranno con la propria banca, assicuratore, ospedale, attiverà e controllerà a distanza l'allarme della propria abitazione, tutte leccornie per ladri di identità, furti telematici, ladri di abitazioni private. Tutto ciò significa che decine di miliardi di informazioni viaggeranno nella rete in micro secondi e quindi i custodi dei cosiddetti big data dovranno sempre di più sviluppare controlli e tecnologie per la protezione dagli attacchi informatici sviluppando in termini di efficacia e rilevamenti di controllo. Abbiamo parlato di tecnologie e sicurezza e un riferimento privilegiato va agli Open data grazie ai quali che per una volontà generalizzata stanno diventando sempre più trasparenti nell'intercomunicazione con i cittadini e non di meno verso la Pubblica Amministrazione per interconnettere verso i servizi. Con questi scenari bisogna riconoscere che sempre di più dovremo affrontare difficoltà molto complesse anche perché, in primo luogo, mancano ancora criteri condivisi di standardazione nella gestione delle informazioni e in tale senso è auspicabile o

meglio necessario un confronto sia all'interno delle organizzazioni pubbliche senza trascurare il confronto tra queste e le aziende. Pertanto a conclusione di questa prima analisi possiamo considerare la tematica smart cities e Big data il vero obiettivo tanto per il settore pubblico che per le aziende che sviluppano servizi sia per il pubblico che per il privato accomunati nel compito di individuare e realizzare tecnologie a sostegno del miglioramento della qualità della vita dei cittadini vista come bene assoluto di una società libera e democratica.

La società digitale è un processo irreversibile e quali rischi personali?

Innanzitutto bisogna riflettere sugli ultimi sondaggi sui livelli di consapevolezza sulla sicurezza maturata da parte delle persone e delle aziende. Per quanto riguarda le persone basti pensare all'elevato numero di denunce per truffe telematiche che dagli ultimi dati si posiziona su un incremento dell'8% anno. Volendo, invece, fare un focus sulle aziende, dagli ultimi dati di ricerca è evidente una minore sensibilità nei confronti della sicurezza informatica da parte dell'Italia rispetto a molti paesi europei, per non parlare poi del divario che è stato riscontrato tra le aziende europee rispetto a quelle di oltre oceano. A seguito è riportato un estratto della ricerca riguardante i livelli di consapevolezza in generale e del controllo dei rischi informatici e il relativo confronto con l'Europa anche per quanto riguarda le minacce informatiche.

I numerosi sondaggi e attente analisi non risolvono i problemi ma sicuramente sono serviti ad accendere importanti riflettori sugli obiettivi presenti e futuri. Abbiamo capito, per esempio, che si sta affermando sempre di più un nuovo mestiere in tutto il mondo: l'hacker. Tutto ciò, sommato ad una sempre più auspicabile consapevolezza dei livelli di pericoli, richiederà alle persone di ripensare il proprio modello di vita e principalmente alle aziende di riformulare le proprie strategie organizzative e di business.

Quali sono i focus su cui indirizzare i livelli di consapevolezza di sicurezza informatica?

Al di là delle componenti strutturali in cima alla classifica ci sono i trend tecnologici come i tablet e smartphone che stanno costituendo i fondamentali della rivoluzione digitale con cui le persone interagiscono. Un'altra rivoluzione tecnologica è la tecnologia Cloud che in termini quantitativi possiamo affermare che c'è stata una esplosione negli ultimi tre anni e inoltre sta determinando una

profonda trasformazione nel modello economico di buona percentuale di imprese, pertanto l'evoluzione verso le infrastrutture porterà crescita e guadagni a chi saprà utilizzare al meglio le informazioni in termini di sicurezza e contenimento dei costi. Un settore che è fortemente legato ai livelli di sicurezza è l'e-commerce, è sempre più in crescita l'integrazione tra il consumatore digitale interattivo e le aziende che effettuano la vendita virtuale multicanale. L'insieme di tutti questi processi sta sviluppando ambiti verticali che sempre di più si integrano tra loro all'interno di strutture come la Smart City per costituire ,poi, scelte fondamentali per la digitalizzazione dell'Italia e Europa.

Parliamo ancora di competenza e formazione

Un mondo digitale chiede sempre più spesso riferimenti sicuri, consulenza sulle scelte tecnologiche e una formazione che ci faccia stare a passo con l'evoluzione. A questo proposito le aziende sono sempre più chiamate a dare una consulenza qualificata, offrire qualcosa che vada oltre la semplice vendita di servizi tecnologici e quindi una competenza su nozioni di economia, finanza, analisi aziendali ecc..... I manager più attenti sanno che in un mercato in continua trasformazione cambia il modo di approccio con i propri interlocutori e che non basta più vendere tecnologia ma è necessario fornire un servizio a 360°. Inoltre questa rapida evoluzione del cambiamento tecnologico unita al processo di globalizzazione hanno comportato una profonda trasformazione nella raccolta, nell'utilizzo e nel trasferimento dei dati personali. Il sistema sempre più universale dei flussi dei dati, delle modalità di raccolta, del trasferimento e dello scambio delle informazioni personali , le grandi quantità di dati trasferiti a livello globale in un solo secondo nonché lo sviluppo dei servizi multimediali, richiede anche una importante revisione e condivisione delle regole che risultano desuete e non adatte alle nuove forme di comunicazione. In particolare, i servizi che consentono agli utenti l'accesso alle risorse informatiche di terzi senza l'archiviazione presso il sito locale, pongono nuove sfide per le autorità preposte alla tutela dei dati, in considerazione dei flussi informativi in tempo reale da una zona territoriale di competenza all'altra, anche al di fuori dell'Ue. Le regole per la tutela dei dati dovranno essere aggiornate per progressi tecnologici sconfinati e a volte incontrollabili.

Che significa parlare di sicurezza

Una classificazione della sicurezza informatica è possibile nella misura in cui vengono stabiliti gli indicatori fondamentali **del livello di sicurezza** che vengono attribuiti dalle normative in ambito nazionale, europee e internazionali, classificando le informazioni e i documenti che siano analogici o digitali a secondo della importanza dell'informazione stessa. La classificazione della sicurezza informatica e delle informazioni in generale seguono il criterio della gravità del danno che la rivelazione non autorizzata della stessa causerebbe alla sicurezza personale inteso come persona fisica e aziendale inteso come attacco alle informazioni primarie per il proprio core business.

Quali sono le azioni principali per definire dei buoni livelli di sicurezza

- **profilare l'accesso** a una determinata informazione per i soli soggetti che abbiano necessità di conoscerla nell'esercizio delle proprie funzioni
- **predisporre un sistema di controllo** che assicuri la limitazione dell'accesso. Il sistema di controllo dovrà essere proporzionato alla rilevanza dell'interesse tutelato, e quindi tanto più incisive quanto più si sale di livello da **riservato** a **segretissimo**
- **qualificare le informazioni** indicando l'identità certa di chi ha prodotto l'informazione o il documento e la rispettiva appartenenza

Attacchi Informatici: Cosa aspettarsi , Cosa temere, Possiamo difenderci?

Attacchi alla sicurezza informatica più diffusi: Codici maligni 48% -Furti di informazioni da cellulari 45% -Phishing 36% -Hard ware 30% -Software 24% - Reti 24% -Accessi per aggiornamenti non autorizzati 18%

Il ruolo della sicurezza nell'era di Internet

Le autostrade di internet sono affollatissime e ricche di insidie ma anche fonti di servizi, pensiamo agli acquisti e ai pagamenti online. La fiducia verso i servizi Internet è in continuo crescente questo anche all' introduzione della Identità Digitale Sicura e grazie a sempre più sofisticate tecnologie che aumentano il livello di sicurezza, sempre di più vengono utilizzati i servizi online offerti dalla Pubblica Amministrazione, dai privati , dallo sviluppo sempre più crescente dell' e-commerce. L'uso del sistema sicuro di Identità Digitale consente e consentirà di contrastare in maniera molto efficace i fenomeni criminali e in particolare il Furto d'Identità quindi assisteremo sempre di più alla richiesta di tutela della privacy e ad una riduzione di archivi che contengono dati personali, una

standardizzazione e una definizione di un insieme di attributi relativi ad una entità sicura e protetta con l'uso di credenziali che vengono utilizzati per poter accedere in modo sicuro ai servizi (One Time Password, Smart Card, App di sicurezza, sistemi biometrici. Quanto detto dimostra che la situazione è abbastanza preoccupante e che quindi la conoscenza dei tipi di attacco alla sicurezza dei dati personali e la violazione della Identità Digitale sono argomenti su cui riflettere e far riflettere.

Cosa stanno facendo gli altri paesi?

L'orientamento tecnologico ed i regolamenti stessi prediligono soluzioni semplici e dirette, senza entrare nei dettagli tecnici sofisticati ma definendo schemi di processi che possano creare una sorta di ecosistema per le autostrade che percorrono quel globo chiamato Internet che mette al centro l'utente e quindi i cittadini fornendogli una sorta di "passaporto sicuro" per comunicare in modalità multimediale. Quanto fin qui detto merita una riflessione sulla anagrafe digitale, sulla verifica della Identità Digitale, Tessera sanitaria e quindi sui gestori di servizi che sono sia pubblici che privati sia nazionali che internazionali e quindi si ritorna ancora alla conclusione di sempre, di scelte sempre più condivise e sempre più globali. E' logico che quando si vogliono adottare scelte condivise è importante adottare schemi di processi con un grande livello di flessibilità e standardizzazione di sistemi di autenticazione che evolveranno anche sulla base di nuove tecnologie sempre più sofisticate offerte dal mercato.

In Italia cosa succede?

E' stato avviato un progetto Pilota aperto a tutte quelle società che vi vorranno partecipare sia in qualità di Gestori di Identità, sia di Gestori di Servizi.

Tutti i siti della Pubblica Amministrazione dovranno adeguarsi ai sistemi di Identificazione Elettronica previsti dall'art. 64 del Codice dell'Amministrazione Digitale.

Logiche politiche e di mercato

Con la promessa di dedicare un prossimo articolo che vada oltre questa sintesi, possiamo affermare, senza timore di smentita, che parlare di sicurezza significa

anche una politica comunitaria più consapevole per confrontarsi con un business nascente che riguarda il furto di identità. E in atto una crescente vendita al mercato nero di dati degli utenti, fornendo al migliore offerente informazioni “sensibili” e personali con la compravendita su Internet dei dati rubati, nomi, indirizzi, email. Rubare un’identità è un business internazionale che interessa pirati informatici in ogni parte del mondo, francamente confesso un brivido di paura.



Strategia per la crescita digitale 2014-2020

IL DIGITALE potrà contribuire ad una Italia migliore

Carissimi lettori,

benvenuti a questo primo numero della rubrica dig@ITALIA, l'Italia Digitale, che affronterà in ottica giuridica, dottrinale e tecnica il mondo complesso della digitalizzazione e degli obiettivi che con essa si intendono raggiungere.

Questa rubrica si pone anche un obiettivo interattivo col lettore affrontando anche argomenti suggeriti da Voi che arriveranno alla nostra redazione.

Il mondo sta cambiando con una velocità "digitale" tutti ostentiamo scenari diversi, si affacciano nuove professionalità e alcune delle quali potranno essere l'arma vincente per affrontare le complessità che si insinuano nel mondo digitale.

Perché nasce questa rubrica.

Perché la digitalizzazione del documento e tutti i processi connessi richiedono conoscenza e professionalità e un confronto costante col mercato e le istituzioni.

Spero, anche col Vostro aiuto, di poter contribuire ad una maggiore conoscenza di questo nuovo mondo e ottenere la convinzione che il digitale non è un mostro da combattere ma una ottima opportunità per migliorare la comunicazione tra Pubblica amministrazione e cittadini, tra fornitori di servizi e utenti, tra una Europa sempre più unita.

Dialogare in questo ampio raggio presuppone anche una conoscenza dei rischi relativi alla protezione dei nostri dati personali e quelli che costituiscono "il bene aziendale".

Un messaggio forte in tal senso arriva anche dall'Unione europea ,grazie alla riforma della protezione dei dati, nel quale viene sancito il diritto fondamentale circa la protezione dei dati. Intanto gli accadimenti recenti sulla violazione dei dati ha diffuso qualche sconcerto ed ha aumentato la sensibilità circa la questione della sicurezza e privacy anche per il fatto che la dematerializzazione dei dati e la conseguente digitalizzazione si sta sempre più diffondendo.

La diffusione dei servizi in outsourcing obbliga le imprese ad alzare il livello di sicurezza per garantire ai propri utenti una risposta adeguata ai loro timori e nell'immediato futuro la sicurezza delle informazioni creerà competizione tra le aziende e la sicurezza delle informazioni sarà sempre di più un argomento che farà la differenza nell'ambito del business.

La normativa in materia di sicurezza e privacy dei dati oggi è sempre più uno strumento prezioso per consentirci di muoverci nell'era digitale.

La richiesta di servizi digitali in outsourcing obbligano le aziende a rendere sempre più accessibile alle applicazioni interne ai clienti o utilizzatori esterni su soluzioni web.

E' sempre più in crescita la digitalizzazione delle informazioni ed a esternalizzare servizi che esulano dal core business aziendale, con la conseguente scelta da parte delle aziende che erogano servizi di investire in sicurezza e mentre da una parte assistiamo ad un incremento di Data Center dedicati dall'altro si tende a prediligere sistemi con tecnologia modulare e virtuale.

Internet ormai costituisce uno strumento friendly a livello mondiale che consente l'accesso a tutti ed è per questo motivo che la trasmissione dei dati è rischiosa soprattutto quando sono particolarmente sensibili.

Nonostante le misure di sicurezza siano elevate, sussiste sempre la possibilità che i dati vadano persi o vengano intercettati, manipolati da persone non autorizzate o addirittura da delinquenti che si appropriano della nostra identità o delle informazioni di natura personale.

Le problematiche da affrontare sono tante e questo sarà l'obiettivo dei prossimi articoli.

