GDPR, Misure Minime di Sicurezza ICT, Piano Triennale…. Opportunità o sfida impossibile?

29 maggio 2018

Fabrizio Pedranzini – GdL ICT CODAU

Premesse/1

Trend di contesto in atto:

- Incremento esponenziale:
  - della quantità di dati raccolti e trattati da applicazioni e servizi ICT
  - delle possibilità di correlazione diretta o indiretta dei dati, non solo per effetto dell'integrazione tra i servizi
- Crescente delocalizzazione dei dati e dei servizi
- Abbassamento delle barriere di carattere tecnologico ed economico alla creazione ed erogazione dei servizi

Premesse/2

Rischio di trattamenti:

- non leciti nel merito delle informazioni raccolte
- non leciti per le operazioni svolte
- effettuati in condizioni non sicure (es. su sistemi non presidiati in termini di policy di aggiornamento o obsoleti)
- effettuati in modo non trasparente o inconsapevole
- potenzialmente appetibili per usi impropri

Difficoltà rilevate

- Difficoltà nel coinvolgere e sensibilizzare gli attori coinvolti
  - Chi definisce i processi ed i trattamenti => revisione dei processi, censimento dei trattamenti e definizione delle informative
  - Chi li implementa => attenzione a tutti i layer coinvolti/attraversati
  - Chi attribuisce i diritti di accesso ai dati => ACL e policy di provisioning/deprovisioning
  - Chi effettua i trattamenti => azioni di formazione/sensibilizzazione

  sia con riferimento alle attività di carattere amministrativo che legate alle didattica ed alla ricerca
- Difficoltà nel far emergere e se necessario rivedere trattamenti non noti (non censiti) ed effettuati in condizioni “migliorabili”
- Difficoltà di coordinamento e controllo, di integrazione dei servizi e di visione d’insieme

Quadro normativo

Questa situazione si inserisce nel quadro di un contesto normativo, nazionale e comunitario, in rapida evoluzione e di grande complessità, che subisce continui adeguamenti anche per «inseguire» un contesto tecnologico di servizi in costante cambiamento:

a. GDPR
b. Misure Minime di Sicurezza ICT
c. Piano triennale per l'informatica nella PA:
    - Censimento delle risorse ICT (e dei servizi critici)
    - Piattaforme abilitanti: SPID, pagoPA, fatturazione elettronica, …
    - Ecosistemi
d. Responsabile per la transizione digitale RTD

Si tratta di un "combinato disposto" di formidabile complessità e portata per gli interventi richiesti (tipicamente da realizzarsi a risorse costanti).

Effetti

- Queste norme forniscono ai RTD gli strumenti per intervenire ed incidere sulla realtà
- E' aumentata la sensibilità su questi temi, anche da parte di componenti tradizionalmente refrattarie. Magari la percezione è che si tratti di adempimenti burocratici e ci si preoccupa di essi solo a ridosso della scadenza, ma c'è la consapevolezza che alcuni interventi siano ineludibili => sta agli RTD far sì che siano sostanza e non solo forma…
- Sicuramente è emersa la necessità di "fare sistema", si pensi al GdL ICT CODAU:
  - Gruppo tematico e Linee Guida sul GDPR
  - Note sulle MMS
  - Note sulla compilazione del censimento
- Sta emergendo un interessamento a questi temi anche da parte della CRUI (es. recenti webinar su GDPR e Censimento del patrimonio ICT), il cui contributo è determinante per un'azione più incisiva.

Criticità/1

Le disposizioni definiscono interventi che, in generale, trascurano le peculiarità del sistema universitario:

- Necessità di avere flessibilità e possibilità di sperimentazione, tipiche del mondo della ricerca
- Presenza di competenze avanzate e di infrastrutture di qualità con SLA elevati
- Presenza di soluzioni applicative e servizi sviluppati con approccio condiviso da tutto il comparto
- Erogazione di servizi in ottica federata
- Presenza di provider di servizi infrastrutturali ed applicativi

Ciò può essere comprensibile considerando il fatto che di tratta di normative di carattere generale, tuttavia andrebbe prevista la possibilità di tener conto di finalità e caratteristiche specifiche del comparto.

Criticità/2

Peraltro il sistema universitario, grazie alle sue specificità, potrebbe essere preso come esempio virtuoso.

Va segnalato che, rapportandosi come comparto con gli interlocutori istituzionali, qualche risultato si è ottenuto, ma si è solo all'inizio:

- Garante: incontri, parere sulle Linee Guida,
- AgiD:
  - incontri di approfondimento con i referenti delle differenti tematiche (SPID, pagoPA, MMS, Piano Triennale)
  - circolare con precisazione sulla possibilità di investimenti in risorse dedicate alla ricerca

Per il censimento del patrimonio ICT però, ben poco si può fare a fronte di un questionario di rilevazione rigidamente incapace di rappresentare significative varianti rispetto alla realtà prefigurata e schematizzata.

Conclusioni

Il processo di adeguamento è necessario, ma per avere qualche speranza di sostenibilità e successo:

- E' necessario fare sistema a tutti i livelli:
  - All'interno degli Atenei
  - Nel comparto lavorando in modo sinergico con CODAU, CRUI, GARR e CINECA. Ovviamente sarebbe ottimale ed auspicabile un coordinamento con MIUR
  - Con AgID e gli altri interlocutori istituzionali per dare un contributo concreto all'evoluzione dei servizi ed ottenere al contempo un livello di attenzione adeguato.
- E' necessario aumentare la consapevolezza ed il coinvolgimento dei nostri interlocutori istituzionali, Rettori e Direttori Generali.

Scelte locali e non coordinate non giovano al benessere complessivo.

Grazie per l'attenzione!

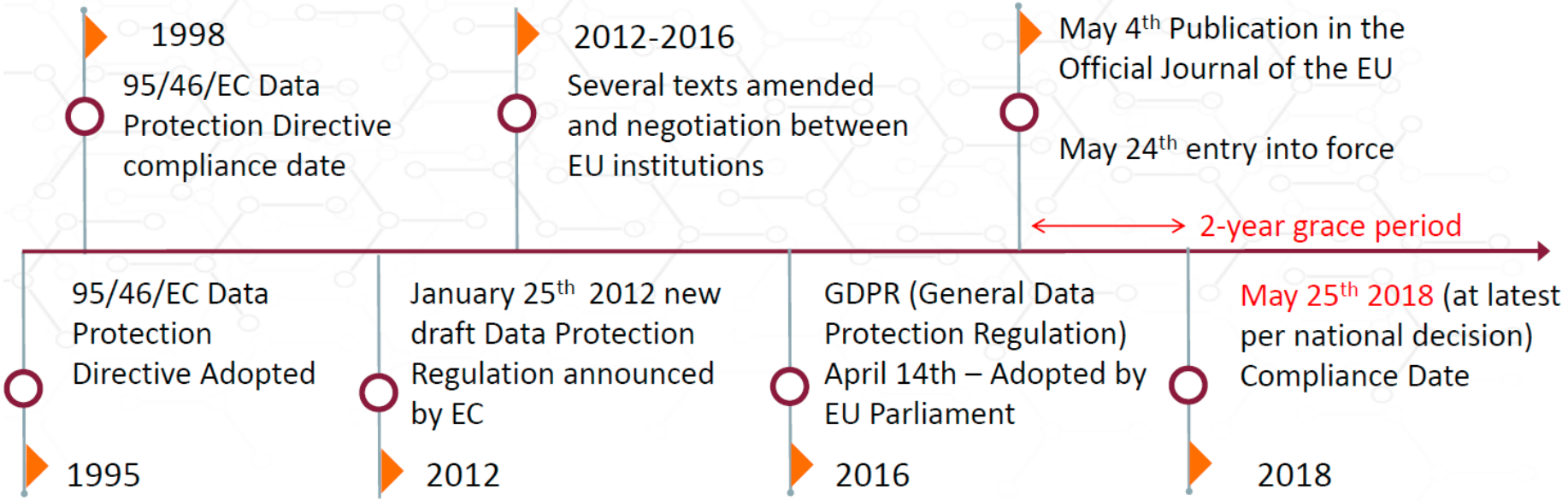
fabrizio.pedranzini@polimi.it

02 2399 2377

335 7866796

General Data Protection Regulation (GDPR) /1

http://www.garanteprivacy.it/regolamentoue



Articolo 5

Principi applicabili al trattamento di dati personali /1

1. I dati personali sono: (C39)

   a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**«liceità, correttezza e trasparenza»**);

   b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati per- sonali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (**«limitazione della finalità»**);

   c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**«minimizzazione dei dati»**);

   d. 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 (**«esattezza»**);

Articolo 5

Principi applicabili al trattamento di dati personali /2

e. 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attua- zione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (**«limitazione della conservazione»**);

f. 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»**).

Articolo 5

Principi applicabili al trattamento di dati personali /3

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (**«responsabilizzazione»**). (C74)

Considerando 74

È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.

In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure.

Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78) /1

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78) /2

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento.

   Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Articolo 32 – Sicurezza del trattamento (C83) /1

1. 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, che comprendono, tra le altre, se del caso:
   a. la pseudonimizzazione e la cifratura dei dati personali;
   b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Articolo 32 – Sicurezza del trattamento (C83) /2

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Misure minime di sicurezza ICT /1

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT

PER LE PUBBLICHE AMMINISTRAZIONI

(*Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015*)

CIRCOLARI

AGENZIA PER L'ITALIA DIGITALE

CIRCOLARE 18 aprile 2017, n. **2/2017**.

Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

Premessa.

L'art. 14-*bis* del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera *a)*, tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica.

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

La presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella *Gazzetta Ufficiale* n. 79 del 4 aprile 2017).

Misure minime di sicurezza ICT /2

1- INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

2 - INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

3 - PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

4 - VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

Misure minime di sicurezza ICT /3

5 - USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

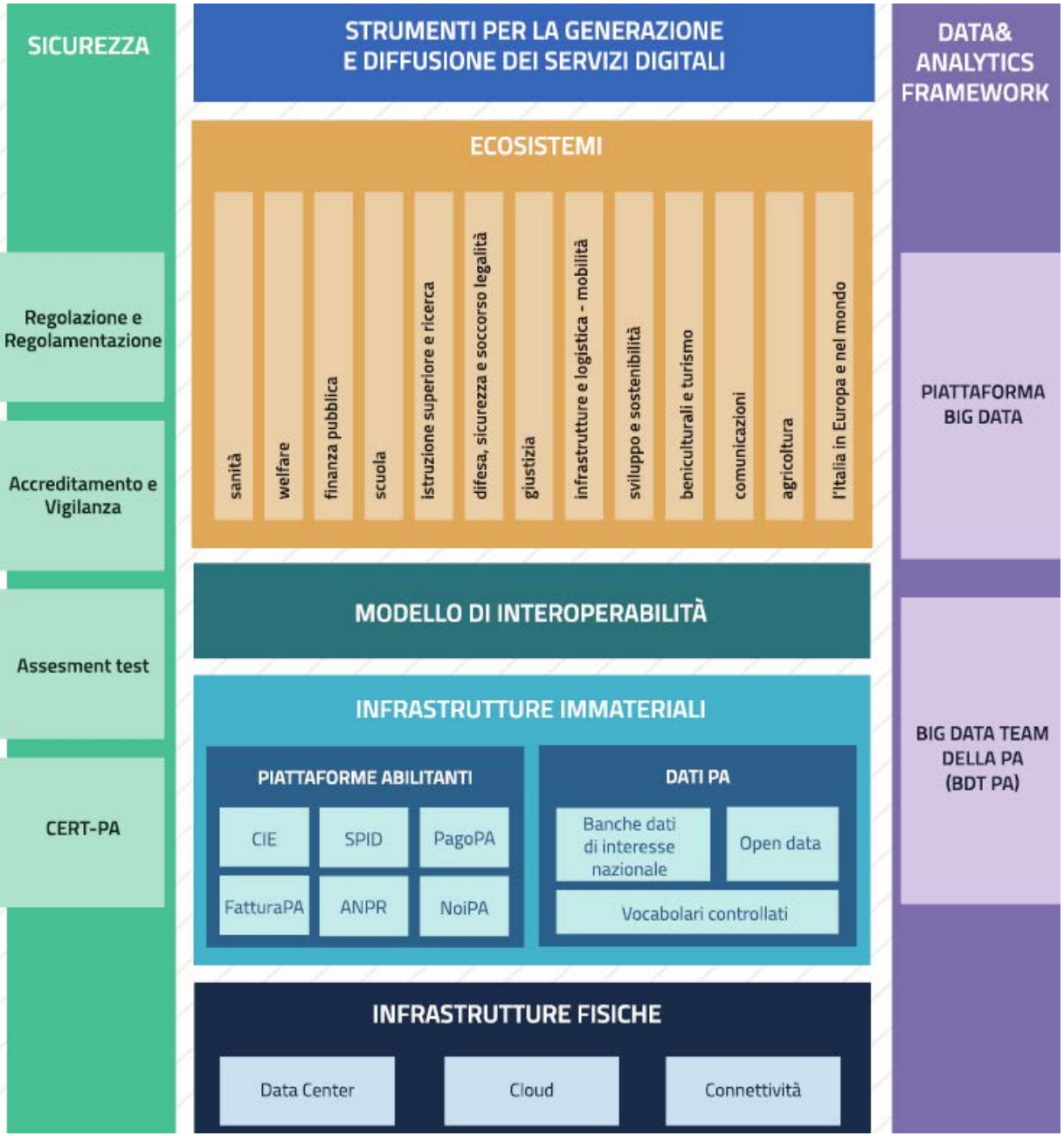
8 - DIFESE CONTRO I MALWARE
Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

10 - COPIE DI SICUREZZA
Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

13 - PROTEZIONE DEI DATI
Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

Piano Triennale per l'informatica nella PA /1

Modello strategico AgID



Piano triennale ICT PA - Infrastrutture fisiche /1

3 Infrastrutture fisiche

Le Infrastrutture fisiche nazionali sono, principalmente, gli *asset* hardware necessari per la realizzazione del Piano: le reti di comunicazione, i *data center*, il *cloud* della PA, i sistemi di *disaster recovery* e di *business continuity*, gli apparati per il monitoraggio e la sicurezza. Il Piano si svilupperà lungo tre principali direttrici:

- la riorganizzazione del parco dei data center della Pubblica amministrazione attraverso un'opera di razionalizzazione utile, sia a ridurre i costi di gestione, sia a uniformare e aumentare la qualità dei servizi offerti alle Pubbliche amministrazioni, anche in termini di business continuity, *disaster recovery* ed efficienza energetica;
- la realizzazione del *cloud* della PA, grazie al quale sarà possibile virtualizzare il parco macchine di tutte le Pubbliche amministrazioni, con importanti benefici in termini di costi e di gestione della manutenzione. I servizi *cloud* saranno offerti in modalità *IaaS* (*Infrastructure as a Service*), *PaaS* (*Platform as a Service*) e *SaaS* (*Software as a Service*);
- la razionalizzazione delle spese per la connettività delle Pubbliche amministrazioni e l'aumento della diffusione della connettività nei luoghi pubblici a beneficio dei cittadini.

Piano triennale ICT PA - Infrastrutture fisiche /2

I Poli strategici nazionali potranno anche svolgere funzioni di conservazione dei documenti secondo quanto previsto dal CAD, ferma restando la possibilità di creare ulteriori poli (pubblici o privati) specializzati nella conservazione.

Le Pubbliche amministrazioni, come riportato anche nella Circolare Agid 24 Giugno 2016, n. 2[16], non possono sostenere spese relative alla costituzione di nuovi *data center o all'evoluzione di data center esistenti non eletti a Poli strategici nazionali.*

Le Pubbliche amministrazioni potranno procedere - previa approvazione di AgID[17] - agli adeguamenti dei propri data center esclusivamente al fine di:

- evitare problemi di interruzione di pubblico servizio;
- anticipare processi di dismissione dei propri data center per migrare al *cloud* della PA;
- consolidare i propri servizi su data center di altre PA al fine di ottenere economie di spesa.

Inoltre, a supporto del raggiungimento degli obiettivi indicati nelle diverse fasi, AgID fornirà linee guida utili alla realizzazione del sistema, allo sviluppo di applicazioni *cloud* native e per la migrazione in *cloud* dei sistemi legacy.

Piano triennale ICT PA – Circolare 5 del 30/11/17

Una volta completato il Censimento del Patrimonio ICT, si procederà alla valutazione delle necessità IT infrastrutturali nell'ambito del Piano Triennale e, in funzione del processo di razionalizzazione, verranno proposti i PSN da qualificare. Non è previsto un numero minimo di PSN da eleggere, ovvero, in assenza dei requisiti richiesti, sarà possibile anche non eleggere alcun PSN.

Si specifica altresì che, ai sensi della Circolare AgID 24 giugno 2016, n. 2, come richiamata dal Piano Triennale (cfr. Paragrafo 3.1.3. Linee di azione- azione 1), in materia di spesa le PA non possono effettuare spese o investimenti in materia di Data center, ma – previa approvazione di AgID – possono procedere agli adeguamenti dei propri Data center esclusivamente al fine di:

- evitare problemi di interruzione di pubblico servizio (inclusi gli interventi necessari a garantire la sicurezza dei dati e dei sistemi, in applicazione delle regole AgID Basic Security Controls);
- anticipare processi di dismissione dei propri Data center per migrare al Cloud della PA;
- consolidare i propri servizi sui Data center di altre PA per ottenere economie di spesa.

Attraverso una *procedura informatica* dedicata, pubblicata sul sito istituzionale dell'Agenzia, sarà possibile sottoporre la richiesta d'approvazione

Sono esclusi dalla richiesta di approvazione gli adeguamenti che prevedono acquisti nei seguenti ambiti:

- progetti di ricerca a titolarità di istituzioni universitarie e/o enti di ricerca;
- sistemi a supporto della diagnostica clinica.

Piano triennale ICT PA – Circolari SaaS e CSP 11/04/18 /1

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

AgID | Agenda Digitale | Documenti

Home › Notizie › **Piano Triennale: le circolari "Software as a Service per Cloud" e "Cloud service provider" PA**

Piano Triennale: le circolari "Software as a Service per Cloud" e "Cloud service provider" PA

Mercoledì, 11 Aprile, 2018

Dopo un percorso di consultazione, pubblicate le due circolari relative ai criteri per la qualificazione dei Cloud Service Provider per la PA e per la qualificazione di servizi SaaS per il Cloud della PA.

Sono online le circolari sui criteri per la qualificazione dei Cloud Service Provider (CSP) per la PA e per la qualificazione di servizi Software as a Service (SaaS) per il Cloud della PA.

Piano triennale ICT PA – Piattaforme abilitanti «future» /1

- **ComproPA**: sistema nazionale di *e-procurement* che interconnette, in modalità interoperabile, tutti gli attori del processo di *e-procurement* garantendo la gestione, la digitalizzazione e il governo dell'intero ciclo di vita degli appalti pubblici nel rispetto delle disposizioni del Codice degli appalti e delle direttive europee;
- **Sistema di avvisi e notifiche di cortesia**: un sistema, in conformità con quanto previsto anche dalla normativa eIDAS[60], per consentire al cittadino di ricevere e inviare avvisi e notifiche di cortesia, anche con valore legale, in formato digitale, da e verso tutta la PA, assicurando la tracciabilità, l'integrità, la confidenzialità e il non ripudio;
- **SIOPE+:** evoluzione del sistema SIOPE (utile alla gestione dei flussi di cassa) finalizzato a garantire l'analisi e la valutazione della spesa, il monitoraggio e il controllo dei conti pubblici e a favorire l'attuazione del federalismo fiscale, attraverso attività di armonizzazione e standardizzazione di schemi e flussi dati;

Piano triennale ICT PA – Piattaforme abilitanti «future» /2

- **NoiPA:** evoluzione dell'attuale sistema di gestione del personale che eroga servizi stipendiali alle PA, a cui saranno aggiunte funzionalità per la gestione delle componenti non economiche del personale, anche a supporto della recente riforma della PA (Legge 124/2015 recante "Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche");
- **Sistema di gestione dei procedimenti amministrativi nazionali**: garantisce la comunicazione digitale tra cittadini e PA attraverso lo strumento del domicilio digitale. Permette la dematerializzazione dei procedimenti amministrativi, così da contribuire alla realizzazione di un sistema cooperativo tra amministrazioni che renda interoperabili i flussi documentali tra di esse, riconducendo a unitarietà la gestione dei dati, degli eventi e dei documenti informatici non strutturati;
- **Poli di conservazione:** sistema realizzato delle PA per l'erogazione di servizi di conservazione documentale, con il coinvolgimento dell'Archivio centrale dello Stato che permette la conservazione perenne degli archivi digitali della PA.

Piano triennale ICT PA – Ecosistemi /1

Ciascun ecosistema individua un settore tematico con caratteristiche di omogeneità. Comprende enti e organismi pubblici e può anche includere soggetti privati, quali ad esempio le associazioni che, a vario titolo, svolgono funzioni importanti all'interno dell'ecosistema. Ad esempio, l'ecosistema "Finanza pubblica" comprende sia soggetti pubblici, come Ministero dell'Economia e delle Finanze, il Ministero dell'Interno, l'Agenzia delle Entrate, le Regioni, la Guardia di Finanza, ma anche soggetti privati come commercialisti, CAF, avvocati fiscalisti.

Al fine di facilitare il coordinamento tra gli attori coinvolti, ogni ecosistema:

- definisce le basi di dati di riferimento, le regole di alimentazione delle stesse e implementa i meccanismi di comunicazione con il *Data & Analytics Framework*;
- contribuisce alla definizione delle linee guida specifiche per l'ecosistema stesso;
- definisce le regole condivise e trasparenti per il proprio funzionamento;
- utilizza le piattaforme abilitanti;
- espone i propri servizi attraverso API.

L'applicazione delle regole definite nel Modello di interoperabilità all'interno di ciascun ecosistema rappresenta il linguaggio comune che abilita la comunicazione tra gli ecosistemi.

Piano triennale ICT PA – Ecosistemi /2

- sanità
- welfare
- finanza pubblica
- scuola
- istruzione superiore e ricerca
- difesa, sicurezza e soccorso legalità
- giustizia
- infrastrutture e logistica - mobilità
- sviluppo e sostenibilità
- beni culturali e turismo
- comunicazioni
- agricoltura
- l'Italia in Europa e nel mondo

Piano triennale ICT PA – Ecosistemi /3

6.3 Linee di azione

Per ogni ecosistema AgID raccomanda, in coerenza con le priorità indicate nella Strategia per la crescita digitale 2014-2020, la costituzione di un *Gruppo di lavoro dell'ecosistema* (di seguito GdL), che si occupi della gestione e dello sviluppo tecnologico dell'ecosistema medesimo, definendo i processi operativi da digitalizzare e le esigenze tecnologiche che caratterizzano l'ecosistema stesso.

Il GdL avrà il compito di:

- definire le azioni da realizzarsi per l'implementazione dell'ecosistema e le loro priorità (roadmap), anche nel rispetto dei vincoli normativi;
- individuare e interagire, qualora necessario, con le amministrazioni che possono variare e condizionare il quadro normativo di merito dell'ecosistema;
- definire il Piano di attività attraverso l'individuazione dei progetti utili allo sviluppo dell'ecosistema;
- garantire la diffusione dei temi tecnologici che riguardano l'ecosistema attraverso il coinvolgimento di tutti i soggetti interessati;
- verificare la coerenza complessiva con il Piano triennale e in particolare con i principi di interoperabilità, API, sicurezza, utilizzo delle piattaforme abilitanti, linee di design e sviluppo software, come illustrato nel capitolo 2 "Modello strategico di evoluzione del sistema informativo della Pubblica amministrazione";

CAD - Art. 17. Responsabile per la transizione digitale/1

1. Le pubbliche amministrazioni garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le regole tecniche di cui all'articolo 71.

   A tal fine, ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

2. Il responsabile dell'ufficio di cui al comma 1 è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione, alla modalità digitale direttamente all'organo di vertice politico.

CAD - Art. 17. Responsabile per la transizione digitale/2

Al suddetto ufficio sono inoltre attribuiti i compiti relativi a:

a. coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

b. indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

c. indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;

d. accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

CAD - Art. 17. Responsabile per la transizione digitale/3

e. analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f. cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

g. indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;

h. progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni

CAD - Art. 17. Responsabile per la transizione digitale/4

i. promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j. pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis.

j-bis pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).