smau
BOLOGNA 7-8 GIUGNO 2018

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

GDPR e sicurezza digitale: cosa è veramente necessario e prioritario?

Marco R. A. Bozzetti m.bozzetti@aipsi.org

Presidente AIPSI, Capitolo Italiano ISSA www.aipsi.org
Ideatore e realizzatore OAD www.oadweb.it
CEO Malabo Srl www.malaboadvisoring.it

aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA
ISSA Information System Security Association
OAD Osservatorio Attacchi Digitali in Italia
malabo ICT Advisory

Marco R. A. Bozzetti e Malabo Srl

- Ingegnere elettronico al Politecnico di Milano, è Presidente AIPSI e CEO di Malabo Srl
- Ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e Gea/Gealab, oltre ad essere stato il primo responsabile dei sistemi informativi (CIO) dell'intero Gruppo ENI (1995-2000).
- Nella seconda metà degli anni 70 è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, partecipando alla standardizzazione dei protocolli del modello OSI dell'ISO
- È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser"
- Commissario d'Esame per le certificazioni eCF (EN 16234 - UNI 11506).
- Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT.

- Malabo Srl è stata creata da M. Bozzetti nel 2001
- una società di consulenza direzionale per l'ICT, che opera per Clienti lato domanda e lato offerta basandosi su una consolidata rete di esperti e di società ultra specializzate
- Obiettivo primario degli interventi di Malabo è di creare valore misurabile per il Cliente, bilanciando adeguatamente gli aspetti tecnici con quelli organizzativi nello specifico contesto del Cliente
- Dispone di un proprio laboratorio ICT con server e storage duali, virtualizzati, , collegati con switch a 10 G e connessi ad internet con fibra ottica a 100 Mbps, oltre ad uno spazio in cloud (IaaS)
- Per garantire un effettivo trasferimento di know-how, fornisce come servizio ai Clienti le proprie metodologie e gli strumenti informatici usati nell'intervento consulenziale


STARTUP SAFARI
INNOVAZIONE ACADEMY
OPEN INNOVATION
FORMAZIONE ICT

AIPSI e OAD

AIPSI, Associazione Italiana Professionisti Sicurezza Digitale

- **AIPSI, capitolo Italiano** di **ISSA, Information Systems Security Association**, (**www.issa.org**) **che conta** >>10.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo

- **AIPSI è il punto di aggregazione sul territorio e di trasferimento di know-how per i professionisti della sicurezza digitale, sia dipendenti sia liberi professionisti ed imprenditori del settore**

- **Sede Centrale:** Milano
- **Sedi territoriali**: Ancona-Macerata, Lecce, Torino, Verona-Venezia
- **Contatti**: aipsi@aipsi.org, segreteria@aipsi.org

Primari obiettivi AIPSI

- Aiutare i propri Soci nella <u>crescita professionale</u> e quindi nella crescita del loro business
  - offrire ai propri Soci servizi qualificati per tale crescita, che includono
  - Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA
  - Rapporti annuali e specifici OAD, Osservatorio attacchi Digitali in Italia
  - Supporto nell'intero ciclo di vita professionale
  - Formazione specializzata e supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016, in Italia UNI 11506)

- Rapporti con altri soci a livello nazionale (AIPSI) ed internazionali (ISSA)

- Contribuire alla diffusione della cultura e la sensibilizzazione per la sicurezza informatica agli utenti digitali

- Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte: AICA, Assintel, Assolombarda, Anorc, CSA Italy, FidaInform, FTI, Inforav, Polizia Postale, Smau, i vari ClubTI sul territorio, ecc.

Le principali novità di AIPSI 2018

- → Nuovo sito web dell' Associazione
- → Nuovo sito web per OAD
- → Sedi territoriali
- → Accordo con AICA per promuove le certificazioni eCF sulle competenze della sicurezza digitale
- → Webinar
- → Nuovo Media Partner: Reportec

Milano, sabato 30/6/2018 – ore 10-13 Convegno AIPSI

Quale sicurezza digitale per il GDPR e come evitare le truffe dei millantatori

OAD, Osservatorio Attacchi Digitali in Italia (ex OAI)

- ***Che cosa è***
  - **Indagine via web sugli attacchi digitali intenzionali ai sistemi informatici in Italia**
- ***Obiettivi iniziativa***
  - **Fornire informazioni sulla reale situazione degli attacchi digitali in Italia**
  - **Contribuire alla creazione di una cultura della sicurezza informatica in Italia, sensibilizzando in particolare i vertici delle aziende/enti ed i decisori sulla sicurezza informatica**
- ***Che cosa fa***
  - **Indagine generale annuale e specifiche su argomenti caldi, condotte attraverso un questionario on-line indirizzato a CIO, CISO, CSO, ai proprietari/CEO per le piccole aziende**
- ***Come***
  - **Rigore, trasparenza, correttezza, assoluta indipendenza (anche dagli Sponsor)**
  - **Rigoroso anonimato per i rispondenti ai questionari**
  - **Collaborazione con numerose Associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori**

OAD-OAI 2008 - 2018 : 10 anni di indagini via web

Questionario OAD 2018 on line ancora per pochi giorni: da compilare e far compilare subito!

https://www.oadweb.it/limesurvey/index.php/661199

Assolutamente anonimo, risposte predefinite tra cui scegliere, rapido da compilare con il salto automatico di domande non pertinenti, include domande su attacchi a *sistemi di automazione industriale, IoT, blockchain*

Come ringraziamento a chi completa il Questionario la possibilità di scaricare gratuitamente:

- **ISSA Journal di Gennaio 2018 con i migliori articoli del 2017**
- **Il volume (in pdf) di Reportec " ICT Security e Data Protection 2018"**


STARTUP SAFARI
INNOVAZIONE ACADEMY
OPEN INNOVATION
FORMAZIONE ICT

GDPR

GDPR: che cosa è

- GDPR è il **nuovo regolamento europeo sulla privacy**, e sostituisce la precedente norma europea sulla privacy, la Direttiva 95/46/EC
- **GDPR, General Data Protection Regulation**: EU Regulation 2016/679 → 119 pagine A4
  - http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679
- GDPR avrebbe dovuto essere applicato ed essere operativo in ogni azienda/ente UE dal **25 maggio 2018**

GDPR si applica ai dati personali dei cittadini europei anche se questi sono trattati fuori della UE. La definizione di "dato personale" è estesa a tutti i dati che consentono, direttamente o indirettamente, di identificare una persona fisica.

«Il dato personale siamo noi» (Garante Soro)

GDPR: obiettivi

- Il GDPR intende **rafforzare** e rendere **più omogenea la prote** **ali** all'interno dei confini dell' UE
  - dato l'ampio uso mondiale di servizi digit
  - data la forte crescita del mercato (v ilati, il più delle volte illegale e all'insa
  - date le diverse interpr ie con le precedenti normative
- Il GDPR affronta **one di dati personali al di fuori dell'UE** e obbliga to dei dati, anche con sede legale fuori dall' o dati di residenti nell'UE ad osservare ed previsti.

L'interessato, di cui si trattano i dati personali, è al centro del GDPR che ne definisce, aumentandoli, i diritti che devono essere garantiti , per non incorrere in severe sanzioni

re la privacy all'evoluzione tecnologica, all'ampio uso ed aumento con nternet dei flussi transfrontalieri dei dati , all'aumento dei dati scambiati tra attori pubblici e privati,

- **consentire** da un lato una più libera circolazione di dati all'interno dell'UE ma, dall'altro, un più elevato livello di protezione.

GDPR: le conseguenze

- **GDPR sostituisce ed abroga per l'Italia il Codice Unico sulla privacy, il D.Lgs. 196/2003 precedentemente in vigore.**
- Il GDPR in linea di massima **non differisce molto, a livello operativo**, dal precedente Codice Unico , ma in taluni casi meglio specifica alcuni concetti ed in altri richiede specifiche misure (nel seguito approfondite).

L'elemento di maggior impatto è dato dalle **nuove pesanti sanzioni economiche**:

a) una multa fino a **10 milioni di euro**, o fino **al 2% del volume d'affari globale** registrato nell'anno precedente nei casi previsti dall'Articolo 83, Paragrafo 4 del GDPR (violazione obblighi dei titolari e dei responsabili)

b) una multa fino a **20 milioni di euro** o fino **al 4% del volume d'affari** nei casi previsti dai Paragrafi 5 e 6 dello stesso articolo del GDPR (violazione principi base, diritti interessati, trasferimenti, ordini del Garante)

Ma alla data lo **schema di Decreto Legislativo** per **adeguare il quadro normativo nazionale alle disposizioni del Regolamento UE 2016/679** è stato inviato al Parlamento il 10/5/2018, con il consenso del Garante sui suoi contenuti (in pratica correzione del 196/2003 in ottica GDPR), **ma non è stato**

La grande vera differenza rispetto a prima

- **Le elevate sanzioni economiche**
- **Dati i costi e gli impegni complessivi non trascurabili per una effettiva compliance, in precedenza si poteva valutare più conveniente non fare nulla, o quasi, e rischiare la piccola sanzione: ma ora?**

- **Il decreto legislativo di adeguamento al 25/5/2018 non è ancora stato approvato dal Parlamento**
- **Al momento non si sa come vorrà e/o potrà procedere il Garante, ma da una recente indagine Reuters emerge come la maggior parte delle Autorità garanti dei paesi dell'UE non siano affatto adeguati per il GDPR**

Le principali novità del GDPR

- Non sono **più specificate le misure tecniche minime** (All. B Codice Unico) : responsabilità del titolare stabilirle e metterle in esercizio a fronte dell'analisi dei rischi e degli impatti
- Fondamenti di liceità del trattamento
- Approccio basato sul rischio del trattamento e **misure di accountability di titolari e responsabili**
- Informativa e **diritti degli interessati** più ampi e molto dettagliati
- Trasferimenti internazionali di dati (GDPR molto orientato alle grandi aziende multinazionali soprattutto dei servizi ICT)
- **Obbligo di denuncia di un data breach** (violazione dati personali)
- **Meglio definiti ruoli e responsabilità di titolare (ben più forti di prima)**, **responsabile**, **autorizzato** al trattamento (chiamato «incaricato» nel Codice Unico) ed introduzione **n**uova figura del **DPO** (Data Protection Officer), obbligatoria solo in alcuni casi
- **Sanzioni economiche molto forti**

Obbligo di notifica di una violazione dei dati personali (data breach) all'autorità di controllo (art. 33) e di informare gli interessati (art. 34)

- **Importante novità rispetto al Codice Unico**
- In caso di violazione dei dati personali, **il titolare deve notificare la violazione all'autorità di controllo competente** (Autorità Garante, si veda art. 55) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche

- Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento **comunica la violazione all'interessato** senza ingiustificato ritardo.
- Non è richiesta la comunicazione all'interessato se erano state messe in atto, per i dati violati, le misure tecniche e organizzative adeguate, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali **la cifratura**
- **E' quindi opportuno cifrare i dati personali, soprattutto quelli più critici (ex sensibili)**

GDPR
Le principali misure richieste

Le principali misure richieste

- Misure di tipo organizzativo
  - sia verso l'interno
  - sia verso le Terze Parti coinvolte

Nel seguito focalizzazione sulle misure di sicurezza digitale, che sono sia tecniche sia organizzative

- Le principali misure richieste di tipo tecnico
  - Architetture, tecniche e strumenti di sicurezza digitale
  - Misure di sicurezza fisica per gli archivi cartacei

- Misure di «governance», con monitoraggio e controllo delle misure in atto
  - Vale sempre il principio di accountability e di inversione dell'onere della prova
  - Documentare sempre tutto per l'inversione dell'onere della prova

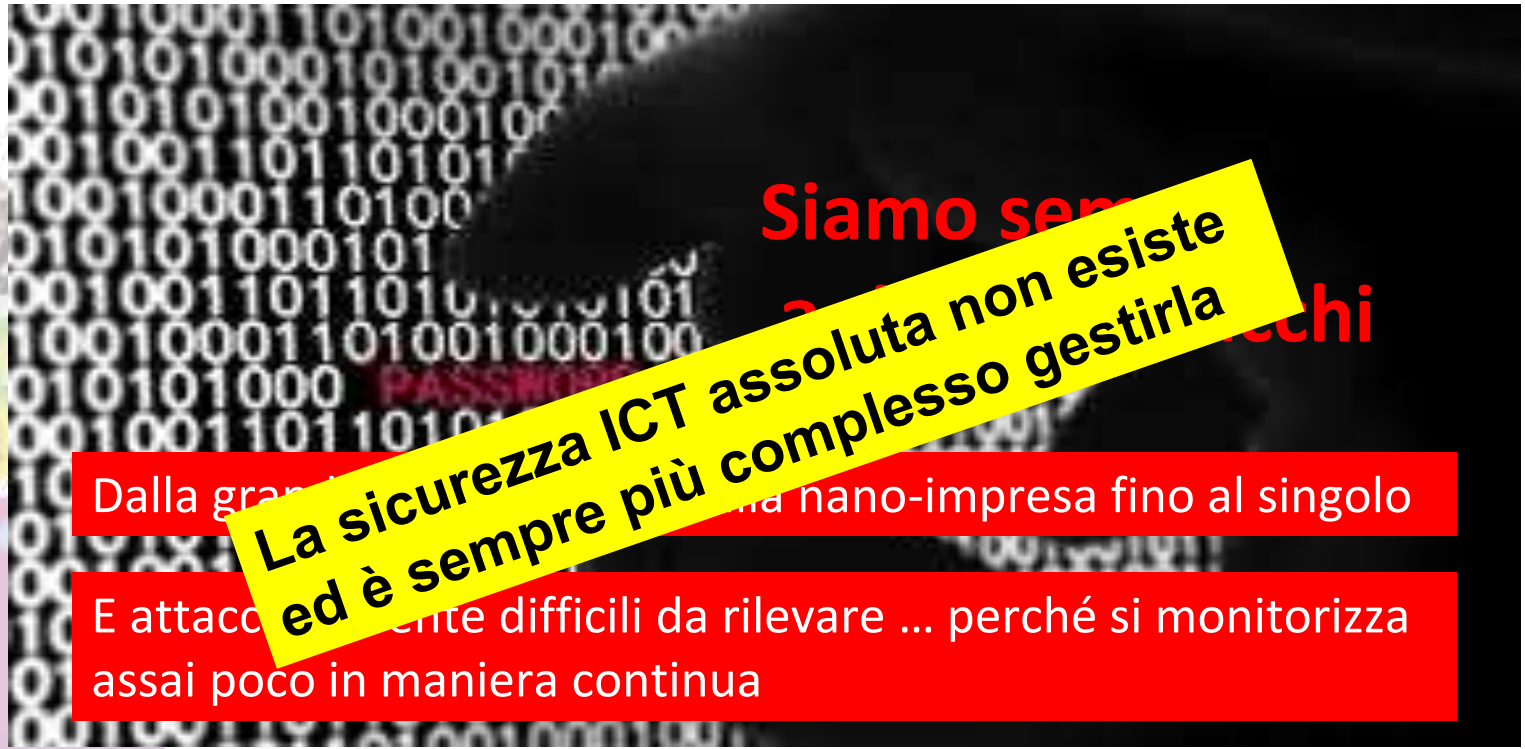
Sicurezza del trattamento (da Art. 32)

- Non sono specificate misure minime come quelle dell'Allegato B del Codice Unico, ma indicate più ampie misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono:
  - la **pseudonimizzazione** e la **cifratura dei dati personali**;
  - 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.

- In più:
  - Si deve registrare (e possibilmente gestire) i log almeno degli Amministratori di Sistema per almeno 6 mesi (Raccomandazione Garante del 2008 che rimane valida)
  - si dovrebbe essere in grado di rilevare violazioni dei dati, in partica degli attacchi

Quali attacchi e quali difese digitali?

Gli attacchi digitali: sempre di più e sempre più critici



Vulnerabilità causa delle minacc

Tutte si basano sulle **vulnerabilità tecniche e/o umane-organizzative**

- ***Vulnerabilità tecniche*** (software di base e applicativo, architetture e configurazioni)
  - siti web e piattaforme collaborative
  - Smartphone e tablette → mobilità → **>>14.000 malware**
  - Posta elettronica → spamming e phishing
  - Piattaforme e sistemi virtualizzati
  - Terziarizzazione e Cloud (XaaS)
  - Circa il 40% e più delle vulnerabilità non ha patch di correzione
- ***Vulnerabilità delle persone***
  - Social Engineering e phishing
  - Utilizzo dei **social network,** anche a livello aziendale
- ***Vulnerabilità organizzative***
  - Mancanza o non utilizzo procedure organizzative
  - Insufficiente o non utilizzo degli standard e delle best practic
  - Mancanza di formazione e sensibilizzazione
  - Mancanza di controlli e monitoraggi sistematici
  - Analisi dei rischi mancante o difettosa
  - Non efficace controllo dei fornitori
  - Limitata o mancante SoD, Separation of Duties

La vulnerabilità più grave e diffusa è quella del comportamento umano (utenti ed amministratori di sistemi):

- **Inconsapevolezza**
- **Imperizia**
- **Ignoranza**
- **Imprudenza**
- **Dolo**

Aggravata dalla non o inefficace organizzazione

Mancanza di formazione e addestramento

Le misure di sicurezza digitale per il GDPR

- Le misure richieste di sicurezza digitale riguardano:
  - Le misure generali atte a garantire riservatezza, disponibilità, integrità, resilienza
  - Misure specifiche sui dati personali per
    - Pseudonimizzazione e Cifratura
    - L'individuazione di data b
    - La gestione degli [illegible] possibilmente nominativi) e dei log
  - Misure di [illegible] monitoraggio delle misure stesse per il controllo e la [illegible] efficacia misure sicurezza
- [illegible] opportune misure di sicurezza debbono essere individuate ed attuate dal titolare contestualizzate sulla realtà delle sue attività, dei suoi sistemi informatici e dei suoi rischi

Sono necessarie e vitali per la continuità operativa aziendale

- **da approccio reattivo a proattivo**
- **contestualizzare misure tecniche ed organizzative alla propria realtà**
- **Analisi dei rischi e degli impatti**
- **approccio architetturale ben bilanciato**
- **riferimento ai principali standard e alle best practices ben consolidate: OSA, ITIL v3, Cobit, ISO 27000, NIST SP, …**

→

→

…)

…gestione delle patch e delle release del software (→ licenze)
…ttiva: formazione e addestramento, operation (ITIL v3), help-desk/contact center, ERT, ..

Pseudonimizzazione e anonimizzazione

- Definizione di **pseudonimizzazione** da art. 4 GDPR : *il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*
- La differenza con **anonimizzazione è che la pseudo consente di ritornare ai dati** originali, l'anonimizzazione no.
- Sono tecniche ben note soprattutto negli ambiti di sviluppo e di test con banche dati reali, e vengono chiamate genericamente **data masking**
- Varie soluzioni anche open source sul mercato
- Necessarie ad esempio per:
  - Effettuare analisi statistiche
  - Effettuare test e collaudi con le banche dati che verranno usate

Esempio di mascheramento di dati

Dati di produzione			Dati "Mascherati"		
Nome	Cognome	e-mail	Nome	Cognome	e-mail
Gabriele	Faggioli	gf@p4i.it	Marco	Rossi	rm@rf.it
Alessio	Pennasilico	ap@p4i.it	Giovanni	Verdi	gio@van.ni
Luca	Bechelli	lb@p4i.it	Linus	Bianchi	ver@nel.spp
Claudio	Telmon	ct@p4i.it	Bill	Fumagalli	bfi@1999.af

Fonte: ZeroUno

Crittografia

- **Simmetrica**: un'unica chiave per criptare/decriptare, che deve essere nota ad entrambi gli interlocutori. Un algoritmo di crittografia simmetrica consente di crittografare in modo efficiente grandi quantità di dati
- **Asimmetrica**: ogni interlocutore ha due chiavi, una pubblica ed una segreta., non correlate tra loro. L'informazione può essere criptata con una chiave e decriptata con l'altra. Si evita in questo modo il problema di scambiare la chiave tra i due interlocutori. Si realizzano canali sicuri tra due attori, risolvendo anche il problema della condivisione della chiave simmetrica che cripta il canale.

- Algoritmi troppo semplici di crittografia e/o una sua cattiva gestione possono rendere
- Fare riferimento agli algoritmi standard ed usare chiavi di opportuna lunghezza

Il problema delle effettive competenze sulla sicurezza digitale

Condizione necessaria, ma non sempre sufficiente, è fare riferimento a:

- professionisti **certificati**
- **Iscritti** ad **Associazioni** professionali **qualificate**

- La sicurezza digitale è **multi-disciplinare** e richiede una vasta gamma di competenze e di esperienza sul campo
- Difficilmente un'Azienda/Ente può avere al proprio interno specifiche e aggiornate competenze di sicurezza digitale
- Deve pertanto terziarizzare gran parte (o la totalità) delle decisioni e dell'operatività, e l'unico criterio di scelta è spesso il passa parola ed il costo
- Ma di chi si può fidare? Come può garantirsi sulle reali competenze dei Fornitori e dei Consulenti?

Le certificazioni eCF (EN 16234 1:2016)

- **Sono le uniche ad avere valore giuridico** in Italia e
  da un Ente accreditato Accredia)
  - AIPSI collabora con AICA, Ente C
- possono valorizzare alcune a
- si basano sulla **prova**
- qualificano il **p**
  profes

Milano, sabato 30/6/2018 – ore 10-13 Convegno AIPSI

Quale sicurezza digitale per il GDPR e come evitare le truffe dei millantatori

mpo dal professionista
ntera sua biografia
sperienze maturate nella sua vita
aver seguito un corso e superato un esame)
le eCF prevede due profili:
pecialist
curity Manager

Per concludere

Prime conclusioni ….

- Il GDPR forse (??) non sarà una bomba atomica, ma <u>richiede un impegno serio e continuo</u>, e quindi dei costi diretti ed indiretti *DIFFIDARE DA CHI PROMETTE DI RISOLVERE TUTTO A POCO PREZZO*
- La sicurezza digitale è ormai un MUST per qualsiasi attività e business, dato che è determinante per la continuità operativa dell'Azienda/Ente. E' indipendente dalla privacy, ma ne è un elemento fondamentale
- GDPR e sicurezza digitale hanno dei costi non trascurabili, ma quali sono i costi della «non privacy» e della «non sicurezza digitale»?
- Di questi tempi tutti si vendono come esperti di privacy e di sicurezza digitale .. Ma come si fa discernere tra i millantatori ed i professionisti seri, soprattutto per decisori non esperti dei temi? Un suggerimento (condizione necessaria ma non sufficiente) è verificare per la persona e/o azienda:
  - Una o più certificazioni sulla privacy e sulla sicurezza digitale , in particolare a livello personale quelle con valore legale europeo: eCF - EN 16234 1:2016
  - l'appartenenza ad una o più associazioni professionali esistenti in Italia per la privacy e la sicurezza digitale

In ritardo ? NO PANIC …. PRIORITA' A BREVE

→ In ritardo rispetto alla scadenza del 25/5/2018?

→ NESSUN PANICO: stendere un Piano di Lavoro con ragionevoli scadenze per interventi da effettuare anche dopo tale data.

→ Per gli interventi a breve, meglio se entro maggio-giugno 2018 e tutti da documentare (inversione dell'onere della prova!):

- ***A livello organizzativo:***
  - Registro dei Trattamenti
  - Nomina dei Responsabili e degli autorizzati
  - Analisi rischi ed impatti
  - Informativa interessati e loro consenso esplicito
- ***A livello tecnico***
  - attivazione e/o miglioramento misure di base per la sicurezza digitale: controllo accessi, back-up e ripristino, anti malware, log di sistema e degli Amministratori
  - Misure fisiche di sicurezza per gli archivi cartacei

Grazie per l'attenzione e ..

- Visitate il sito AIPSI e OAD, e seguite i nostri eventi
- Iscrivetevi ad AIPSI-ISSA
- *Compilate e fa[illegible]ilare il Questionario OAD 2018*

SUBITO !!!