L’approccio della PA alla sicurezza tra GDPR e Circolare AGID

Alghero, 23 giugno 2017

EUROPRIVACY.INFO
@EUROPRIVACY

Sergio Fumagalli, Clusit, Europrivacy, P4I

GDPR e sicurezza

Sicurezza

Art. 6, comma 1, lettera f

La sicurezza è uno dei principi applicabili al trattamento dei dati personali nella logica della accountability

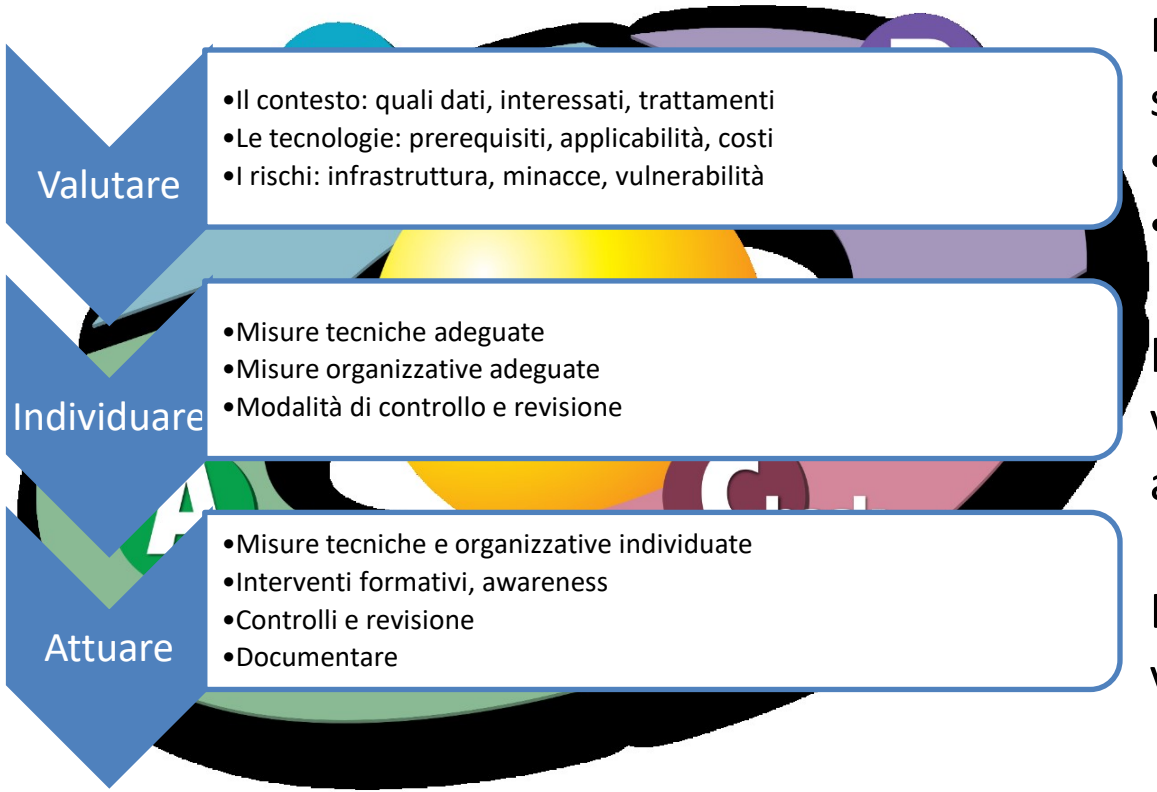
Art. 32

La sicurezza basata sulla valutazione dei rischi e sulla consapevolezza degli addetti.
L'adesione a Codici di Condotta o la certificazione risolvono l'accountability.

Artt. 33, 34

Il Data Breach è un evento di cui bisogna prevedere l'accadimento: gestire l'incident response

GDPR e sicurezza



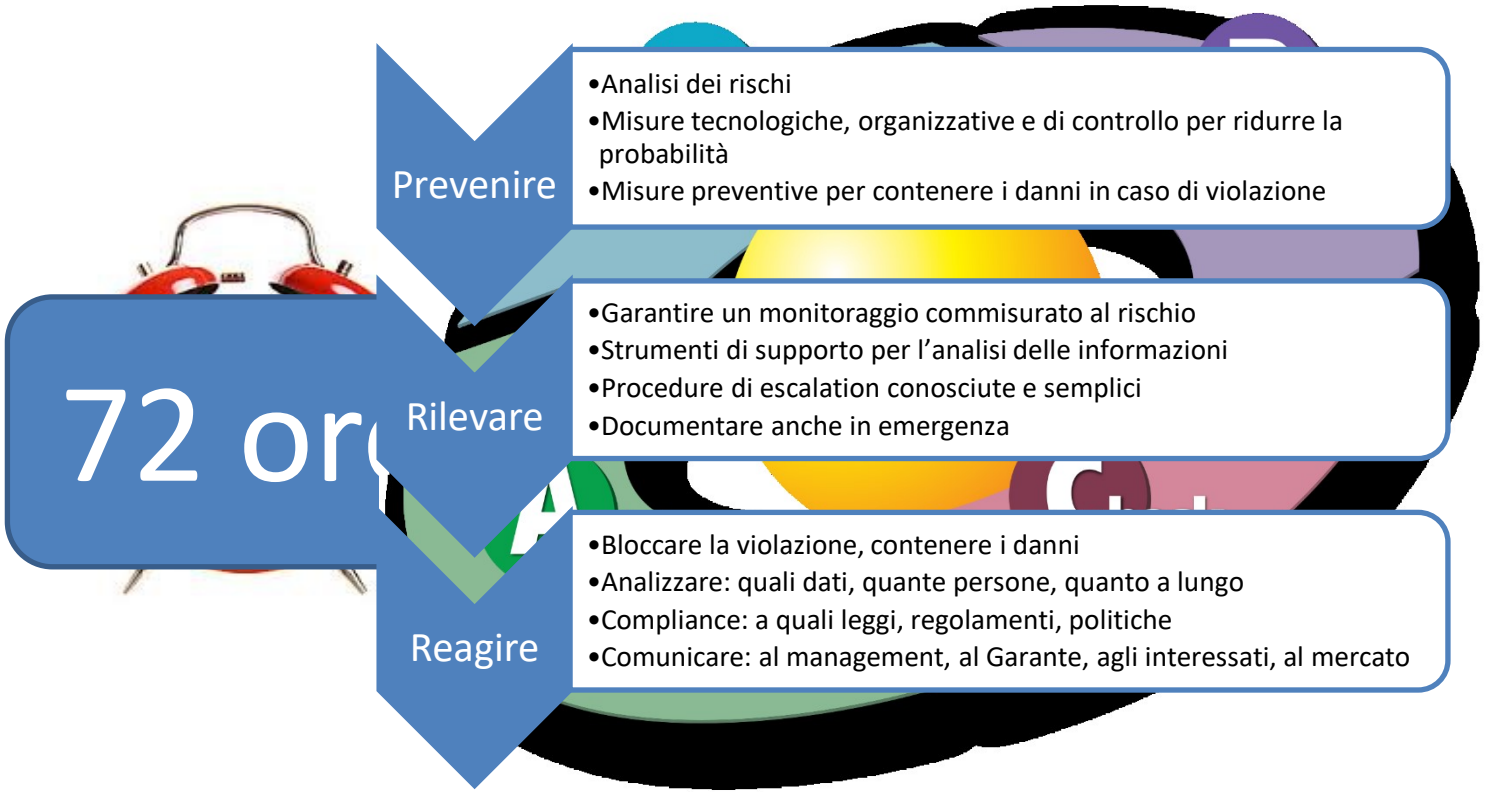
Risk based security, non ci sono misure minime

- Probabilità ➡ IT
- Danno ➡ Business

I costi sono un elemento da valutare, insieme a altri aspetti

Le valutazioni e le scelte vanno documentate ex-ante

Gestire i data breach



Sicurezza e realtà

Il 99%
Degli 8000 Comuni italiani
Dei 4.3M di imprese
NON è in grado di gestire da solo questo requisito.

Codici di condotta
Servizi condivisi
Contratti negoziati
Coordinamento

CHI
SE NE
OCCUPA
?

AGID e sicurezza per la PA

AGENZIA PER L'ITALIA DIGITALE - CIRCOLARE 17 marzo 2017 , n. 1/2017

Misure minime di sicurezza ICT per le pubbliche amministrazioni.

Art. 1. Scopo . Obiettivo della presente circolare è indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottare al fi ne di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi. **Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.**

Art. 2. Amministrazioni destinatarie. Destinatarie della presente circolare sono le pubbliche amministrazioni di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165.

Art. 3. Attuazione delle misure minime. **Il responsabile dei sistemi informativi** di cui all'art. 10 del decreto legislativo 12 febbraio 1993, n. 39, ovvero, in sua assenza, il dirigente allo scopo designato, **ha la responsabilità della attuazione** delle misure minime di cui all'art. 1.

Art. 4. Modulo di implementazione delle MMS-PA. Le modalità con cui ciascuna misura è implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2, anch'esso parte integrante della presente circolare. Il modulo di implementazione deve essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Art. 5. Tempi di attuazione. **Entro il 31 dicembre 2017** le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti.

AGID: misure minime

ABSC 1 (CSC 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

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
		1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
			Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato.				

SANS 20 v. 6
Adattato al contesto italiano
Con riferimento al Framework Nazionale di Sicurezza Cibernetica
Individuando tre livelli di protezione

AGID: misure minime

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

	MISURE MINIMEDI SICUREZZA ICTPER LE PUBBLICHE AMMINISTRAZIONI (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015) Livello di sicurezza minimo
1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.
2	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.
3	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di si-stema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.
4	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autoriz-zato.
5	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
6	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di si-stemi usati dall'organizzazione.
7	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzan-do la configurazione standard.
8	Le immagini d'installazione devono essere memorizzate offline
9	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).
10	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di si-stema report con indicazioni delle vulnerabilità più critiche.
11	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente ag-giornati con tutte le più rilevanti vulnerabilità di sicurezza.
12	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema opera-tivo sia per le applicazioni.
13	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
14	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ra-gionevole rischio.
15	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabi-lità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
16	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al ri-schio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche
17	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
18	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso
19	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
20	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
21	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri)
22	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
23	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
24	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministra-tori, alle quali debbono corrispondere credenziali diverse.
25	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconduci-bili ad una sola persona.
26	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
27	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
28	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.
29	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloc-care l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.rilevare la presenza e bloc-care l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
30	Installare su tutti i dispositivi firewall ed IPS personali.
31	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
32	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
33	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
34	Disattivare l'apertura automatica dei messaggi di posta elettronica.
35	Disattivare l'anteprima automatica dei contenuti dei file.
36	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
37	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destina-tario, prevedendo anche l'impiego di strumenti antispam.
38	Filtrare il contenuto del traffico web.
39	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente ne-cessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab)
40	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni stretta-mente necessarie per il completo ripristino del sistema.
41	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante ade-guata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
42	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente ac-cessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.
43	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
44	Bloccare il traffico da e verso url presenti in una blacklist

AGID: misure minime e analisi dei rischi

ABSC_ID #			Descrizione	Min.	Std.	Alto
4	8	1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	X	X	X

AGID e data breach

3 LA MINACCIA CIBERNETICA PER LA PA

…

Nei fatti le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte. Oltre tutto una lunga latenza della compromissione rende estremamente complessa, … l'individuazione dell'attacco primario, impedendo l'attivazione di strumenti efficaci di prevenzione che possano sicuramente impedire il ripetersi degli eventi.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure, nonché la protezione della configurazione, che è quella immediatamente successiva.

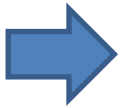
…

ART. 5

… Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

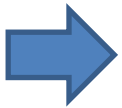
Analisi dei rischi o misure minime?

Per tutte le Amministrazioni che non sono in grado di sviluppare una adeguata analisi dei rischi (il 99% delle PA)



Le misure minime AGID possono essere la risposta per soddisfare l'art. 32 Contribuire agli artt. 33 e 34 (non soddisfarli)

Per le Amministrazioni grandi e strutturate



Le misure minime AGID sono un riferimento che consente una standardizzazione

Grazie per l’attenzione

Sergio.Fumagalli@p4i.it