Convegno Annuale AISIS

Privacy e Sicurezza
A supporto dell'innovazione digitale in Sanità

Adempimenti al GDPR, l'offerta Health Security

Andrea Ferrazzi – Security Executive Maticmind

Torino, 12 e 13 ottobre 2017
Hotel NH Torino Centro

Principali rischi alimentati dalla sottovalutazione delle minacce con riferimento ai dati personali sanitari:

- Trattamenti non autorizzati delle informazioni personali, per scopi illeciti o comunque non pertinenti alle finalità dei servizi erogati;
- Diffusione di informazioni sanitarie personali in grado di arrecare danno agli interessati;
- Frodi operate ai danni della Struttura Sanitaria attraverso un utilizzo improprio dei sistemi informatici e dei processi automatizzati;
- Perdita di disponibilità e/o di integrità delle informazioni sanitarie, attraverso modifica o cancellazione non autorizzata dei dati;
- Perdita di efficienza o interruzione di servizi critici erogati attraverso l'ausilio di servizi ICT.

Normative specifiche di settore

- DPCM 8 agosto 2013; "Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento online delle prestazioni erogate…";
- DPCM 29 settembre 2015 n. 179: "Regolamento in materia di Fascicolo Sanitario Elettronico" e allegato "Disciplinare Tecnico";
- Circolare Agid n. 1/2017, contenente le misure minime di sicurezza ICT per le PP.AA.

Norme vigenti per la tutela dei dati personali, e precisamente:

- D.Lgs 30 giugno 2003, n. 196: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- Pronunciamenti e Provvedimenti del Garante Privacy specifici per il SSN;
- Regolamento (UE) 679/2016 "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

Elementi sensibili del GDPR

- Il legislatore indica di adottare un modello di tipo risk based, ma non indica le contromisure come succedeva con l'allegato B della 196 e pronunciamenti garante.
- Affida al titolare del trattamento dei dati personali anche la responsabilità di definire i criteri di trattamento del rischio.

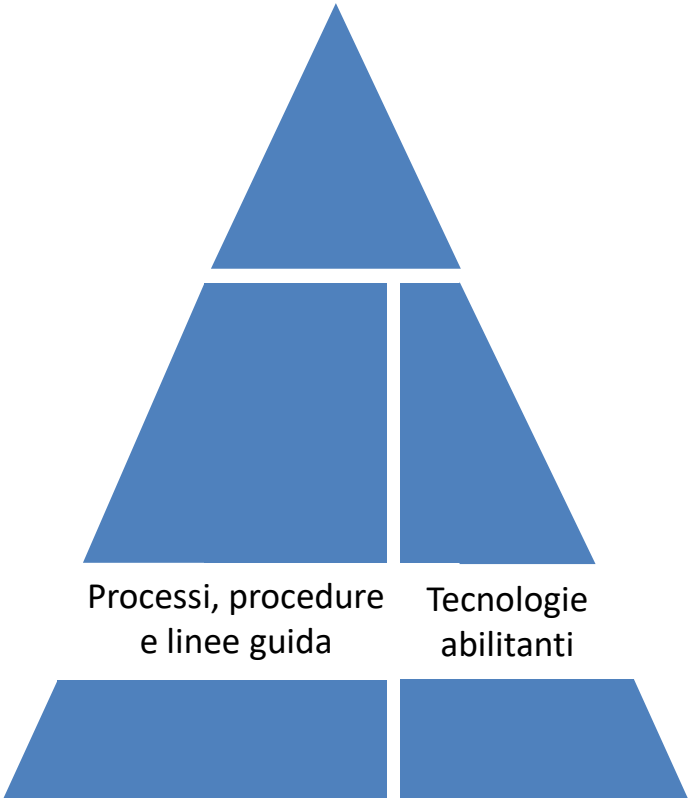
Elementi sensibili dei requisiti minimi AGiD

- Identificazione delle misure tecnologiche funzionali alla compliance GDPR
- Complessità dell'adozione delle misure tecnologiche identificate

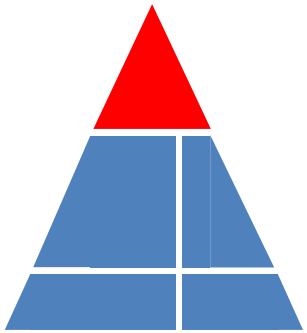
Supporto pianificazione e progettazione

Attuazione degli adempimenti

Manutenzione



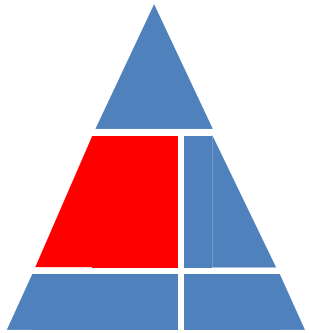
Supporto pianificazione e progettazione



- Elemento cardine è il concetto di risk assessment da dichiarare e di cui deve essere data evidenza con produzione documentale
- Parole chiave - Data Protection Impact Analysis o Privacy Impact Analysis
- Elementi di offerta: metodologia proprietaria per il PIA a norma ISO 29134 comprensiva di una libreria di contromisure che va a coprire riservatezza, disponibilità ed integrità con un focus specifico per gli impatti privacy, in conformità con requisiti minimi AGiD (strutture sanitarie pubbliche) e GDPR.

Attuazione degli adempimenti

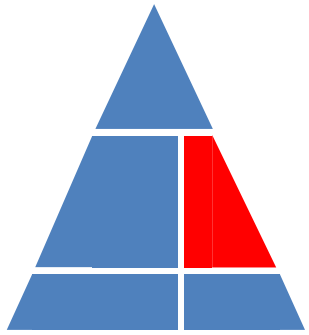
Processi procedure e linee guida



- Contempla procedure e linee guida che documentano i processi che sottendono l'implementazione di un sistema di gestione della sicurezza continuativo
- Parole chiave – Security by design
- Elementi di offerta: Adempimenti formali; Politica generale per la sicurezza; Politica di sicurezza per il trattamento dei dati sanitari; Linee guida per la classificazione dei dati sanitari; Linee guida per la conduzione delle attività di audit di sicurezza delle informazioni; Regole per l'utilizzo delle postazioni di lavoro; Procedura operativa per la gestione delle utenze interne; Procedura operativa per la comunicazione degli incidenti di sicurezza informatica….

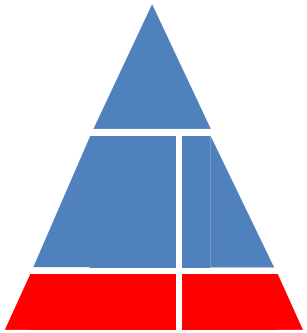
Attuazione degli adempimenti

Tecnologie abilitanti



- Contempla tutta la parte di attuazione mediante misure tecnologiche
- Parole chiave – Identity protection, Data Breach Prevention
- Elementi di offerta a supporto della tutela della riservatezza:
  - Logiche e progetti I&AM, strong authentication, crittografia dei media
- Elementi di offerta a contenimento e governo del data breach:
  - Logiche e progetti di Log Management & Correlation
  - Servizi di breach monitoring e supporto operativo alla gestione in quanto implica necessariamente l'adozione di un processo standard per il rilevamento ed il contenimento (incident handling)

Manutenzione evolutiva



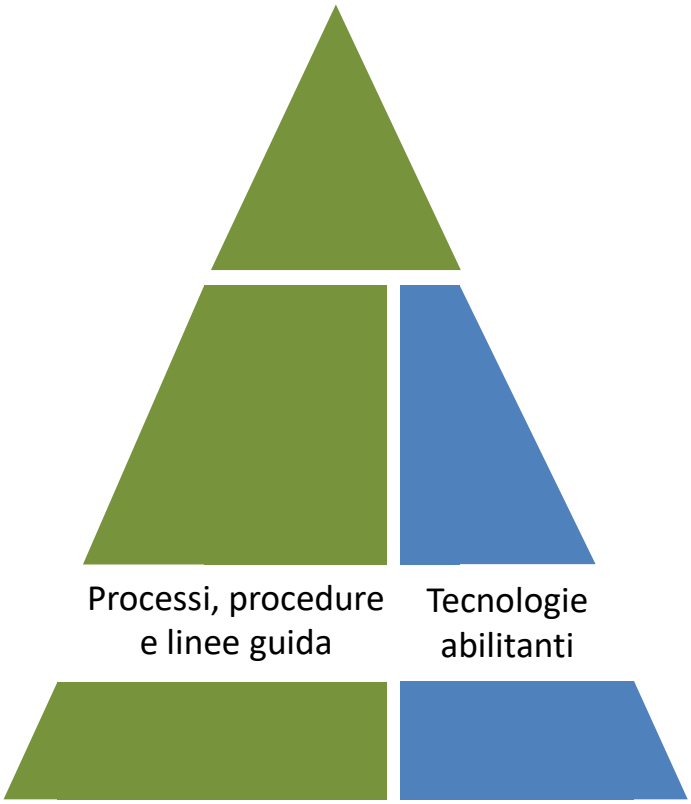
- Rappresenta un requisito implicito nel concetto di gestione continuativa del rischio
- Parole chiave – Security by design in ottica ciclo di vita dei servizi
- Elementi di offerta a supporto:
  - Revisione delle policy
  - Reiterazione del risk assessment
  - Recepimento indirizzamenti cogenti successivi

OFFERTA HEALTH SECURITY
ACCORDO QUADRO SPC2 CLOUD E SICUREZZA IN PARTNERSHIP CON LEONARDO

Supporto pianificazione e progettazione

Attuazione degli adempimenti

Manutenzione



Grazie dell'attenzione e buon lavoro