DATA BREACH SUBÍTO DALL'ASL CN1
DATA BREACH SOTTO PROCEDURA.

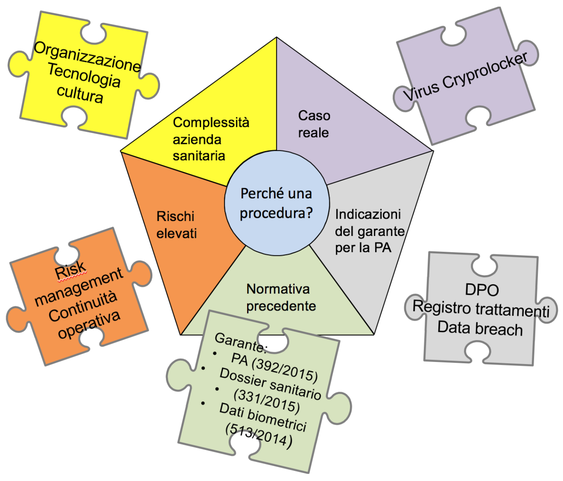
A. Amidei[1], P. Carena[2], G. Guerra[3], N. Rosati[1], S. Salvemini[1], M. Grillo[4].

[1]Direzione Sanitaria Savigliano, [2]DPO interaziendale ASL CN1, CN2 ASO S. Croce Carle,
[3]Direttore Sanitario PP.OO. Savigliano, [4]Coordinatore Presidi Ospedalieri ASL CN1.

Parole chiave

Data Breach, Notifica, Violazione Dati Personali.

Introduzione



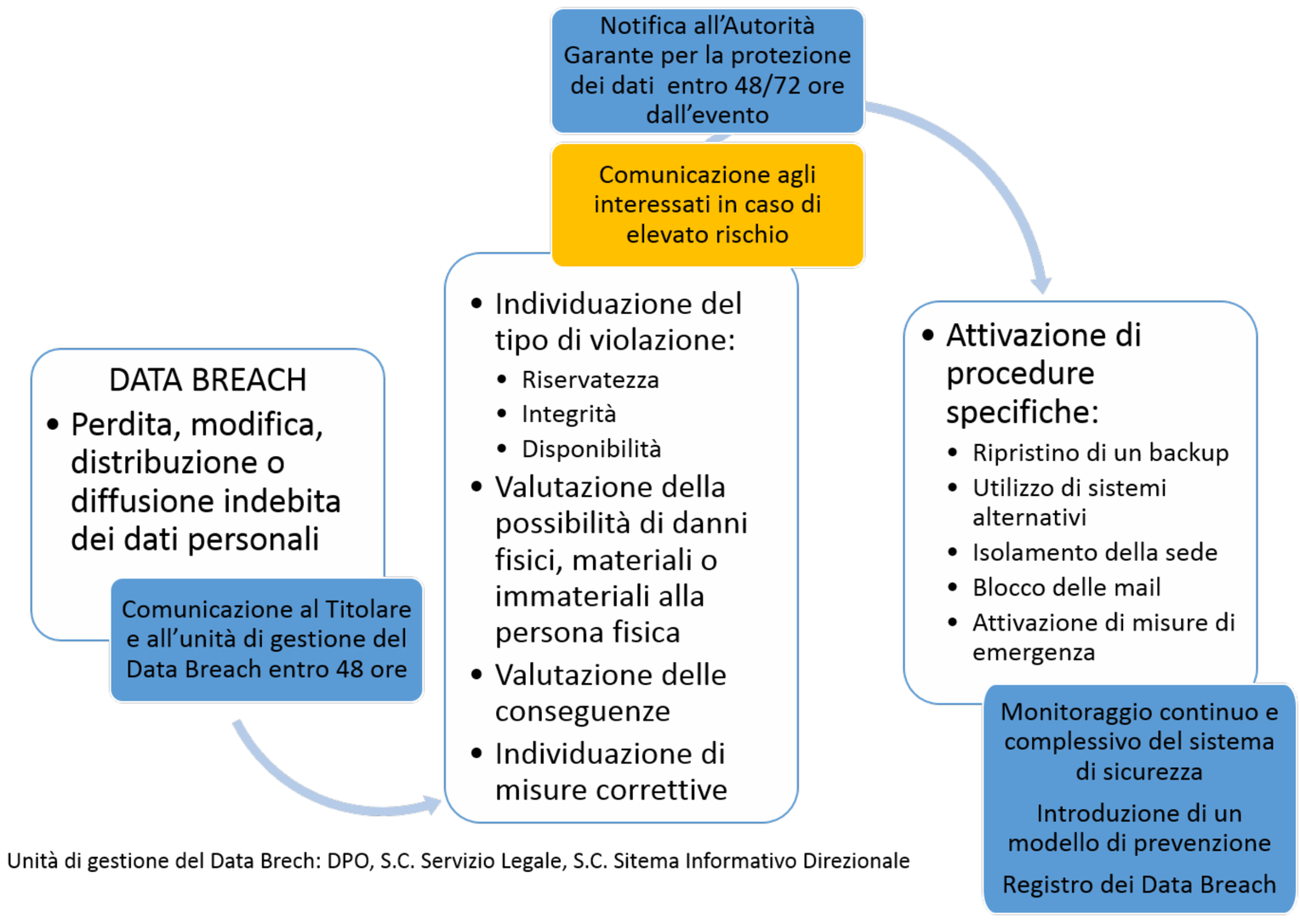
L'applicazione del Regolamento Europeo 2016/679 "Regolamento Generale sulla Protezione dei dati" del 17 aprile 2016 in Sanitá richiede complessitá di interventi sia dal punto di vista organizzativo sia da quello tecnologico sia da quello culturale.

L'ASL CN1 ha subito un attacco hacker in data 16/02/2018 per il quale si é trovata ad isolare la rete informatica su 2 dei 5 ospedali presenti. L'attacco é stato gestito su piú fronti; informatico (isolamento server punto di accesso) organizzativo (ritorno al sistema cartaceo e intensificazione del personale del comparto)

Contenuti

La procedura é stata costruita seguendo le indicazioni sia del Reg. UE 2016/679 sia delle linee guida del WP29 "Guidelines on Personal data breach notification under Regulation 2016/679", adottate il 03/10/2017. Si é inoltre utilizzata la documentazione predisposta dal Garante per la protezione dei dati personali, il Provvedimento n. 392 del 2 luglio 2015, sia per gli aspetti normativi, sia per quelli organizzativi, sia per la documentazione da predisporre.

Il documento della procedura é stato definito dal Data Protection Officer Interaziendale, che si é confrontato per gli aspetti giuridici con il Servizio Legale e per gli aspetti tecnologici con i Servizi Informatici; é stato inoltre importante collaborare per l'intero processo come Direzione Sanitaria per gli aspetti organizzativi contribuendo alla comprensione dei livelli di gravitá degli impatti.



Conclusioni

Aver realizzato la procedura per la gestione del data breach ci ha permesso di:

- aumentare la sensibilitá sul tema in tutto il personale dipendente
- avere uno strumento univoco per la sua gestione contraddistinto dalle seguenti fasi:
  - accertamento della violazione
  - individuazione del tipo di violazione
  - notifica
  - comunicazione
  - registrazione

Bibliografia

[1] Regolamento generale sulla Protezione dei Dati Regolamento Europeo 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("GDPR").

[2] Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali

[3] Provvedimento dell'Autoritá Garante per la Protezione dei Dati Personali n. 392 del 02/07/2015 (per i dati biometrici si fa riferimento al Provvedimento del Garante n. 513 del 12/11/2014 e per il dossier sanitario elettronico al Provvedimento del Garante n. 331 del 04/06/2015)

[4] Prescrizioni del WP29 Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 03/10/2017 (ultima revisione 06/02/2018)

[5] Direttiva (UE) 2016/1148 (Direttiva NIS) del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

[6] Decreto Legislativo 18 maggio 2018, n.65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

[7] Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)", pubblicata in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017)