Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – NOVEMBRE 2017
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque.

E' disponibile il blog http://blog.cesaregallotti.it.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy:
http://www.cesaregallotti.it/Newsletter.html.

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Stato delle norme ISO/IEC 270xx - Novembre 2017

Dal 30 ottobre al 3 novembre 2017 si è tenuto a Berlino il 56mo meeting del ISO/IEC JTC 1 SC 27, ossia del gruppo che si occupa delle norme internazionali della serie ISO/IEC 270xx, dei Common criteria e della privacy.

Questa volta ho partecipato molto poco ai lavori (la delegazione italiana era composta da 4 persone: me, Fabio Guasconi, Stefano Ramacciotti e una rappresentante del Garante privacy). Ciò non ostante, segnalo le cose a mio avviso più interessanti (ringrazio gli altri 3 delegati per aver verificato l'assenza di errori da questo mio resoconto, e per aver fornito alcuni contributi; le opinioni espresse sono unicamente mie).

ISO/IEC 27005 (information security risk management): di questa norma verrà pubblicato a breve un aggiornamento; si tratta in realtà di correzioni necessarie per l'allineamento ad altre norme. Nella sostanza non cambierà nulla. Le discussioni per una nuova versione della norma, con contenuti aggiornati allo stato dell'arte, stanno comunque proseguendo.

ISO/IEC 27006 (requisiti per gli organismi di certificazione): sono stati rilevati possibili errori nella norma e sono pertanto in fase di studio.

ISO/IEC 27552 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management – Requirements and guidelines). A mio parere si tratta di uno schema troppo oneroso, visto che richiede, come prerequisito, la certificazione ISO/IEC 27001. Penso che anche altri stiano maturando lo stesso sospetto, ma questo non è emerso compiutamente durante il meeting (confesso che io stesso sono indeciso perché vedo sì uno standard poco invitante, ma forse uno standard più "leggero" sarebbe da evitare in quanto potrebbe avere conseguenze negative). Vedremo come evolveranno le cose: lo standard è ancora in stato di CD e si prevede la pubblicazione a novembre 2019.

Tra l'altro, mi hanno spiegato che forse la ISO/IEC 27552 non sarebbe lo schema di certificazione privacy previsto dal GDPR: essa è infatti uno standard per sistemi di gestione, mentre il GDPR richiede che gli organismi di certificazione lavorino in conformità alla ISO/IEC 17065, norma relativa alla certificazione di prodotti, processi e servizi e non ai sistemi di gestione. Sono in corso riflessioni in merito, dimostrando così che la faccenda non è banale.

Stanno proseguendo i lavori per altre norme, in particolare:
- ISO/IEC 27102 (Guidelines for cyber insurance);
- ISO/IEC 27002, per una nuova impostazione dei controlli, auspicabilmente più snella (da pubblicare tra qualche anno);
- ISO/IEC 27008 (Guidelines for the assessment of information security controls).

Il gruppo che si sta occupando di Common Criteria (ISO/IEC 15408), ha avviato la revisione delle norme (quindi le nuove versioni saranno pubblicate tra qualche anno). L'obiettivo è quello di pubblicare la versione 4 dei CC nel 2020. Lo standard sarà articolato su un maggior numero di volumi dell'attuale e si preannunciano importanti novità che tengono conto della notevole evoluzione che c'è stata in questi anni.

Sarà a breve pubblicata la ISO/IEC TR 27103, dal titolo "Cybersecurity and ISO and IEC Standards" (si tratta di uno studio che, in parole povere, ricorda che la cybersecurity, così come intesa dal CSF del NIST, è già inclusa nelle ISO/IEC 27001 e ISO/IEC 27002).

Sono stati aperti ulteriori studi in merito alla possibilità di pubblicare ulteriori standard sulla cybersecurity, posto che la prima necessità è quella di concordare in cosa si distingue dalla "sicurezza delle informazioni".

Ulteriore elemento di interesse è l'avvio di uno Study period per discutere dell'utilità (o meno) dello Statement of applicability (o Dichiarazione di applicabilità). Di questo si era

discusso molto durante la redazione della ISO/IEC 27001:2013, ma senza, in realtà, che i sostenitori delle diverse posizioni si ascoltassero veramente. Personalmente non sono convinto né della sua utilità né della sua inutilità, ma spero che questo Study period sia l'occasione per capire meglio tutte le posizioni e arrivare più sereni alla redazione della prossima versione della ISO/IEC 27001 (tra qualche anno).

Il prossimo meeting si terrà a Wuhan, in Cina, a metà aprile 2018.

****

02- Delega al Governo per modificare il Dlgs 196 del 2003

Legge di delegazione europea 2016-2017. L'articolo 13 tratta proprio del D. Lgs. 196 del 2003 (Codice privacy):
- http://www.altalex.com/documents/news/2017/11/07/legge-di-delegazione-europea-2016.

In poche parole: il D. Lgs. 196 sarà modificato per abrogare quanto in contrasto con il GDPR e allineare tutto ciò che c'è da allineare. Non darò notizie sulle varie bozze del D. Lgs. 196 modificato perché non credo sia utile agitarsi per delle bozze.

Ringrazio Pietro degli Idraulici della privacy (e Monica Perego per averli creati).

****

03- VERA 4.4

Ho pubblicato le nuove versioni (in inglese e italiano) di VERA, il mio foglio di calcolo per la valutazione del rischio relativo alla sicurezza delle informazioni. Siamo alla 4.4.

Non grandi cambiamenti, tranne l'aggiunta di una minaccia ("perdita di fornitori").

Ho poi corretto alcuni (troppi!) errori di battitura, sia in italiano sia in inglese. Nessuno me li aveva mai segnalati. Forse nessuno li aveva mai notati?

Per questa versione ringrazio Ivana Catic, Andrea Colato, Vito Losacco, Luciano Quartarone e Giovanni Sadun. Non ho usato tutti i loro suggerimenti, ma sono stati utili e interessanti.

Trovate il file qui:
http://www.cesaregallotti.it/Pubblicazioni.html.

Per i miei lettori volonterosi (e che sono riusciti a leggere fin qui): ho abbozzato un VERA-27001+privacy; se qualcuno a voglia di guardarlo, forse provare a usarlo e commentarlo entro il 10 dicembre (così lo pubblico con la newsletter di dicembre e poi comincio a lavorare ad un VERA-solo-privacy da pubblicare a gennaio), me lo faccia sapere. Da notare che, al momento, vorrei fare 3 VERA: uno solo 27001 (quello che è già pubblicato), quello 27001+privacy (quindi più complesso del VERA-27001) e quello solo-privacy (che credo potrà essere più semplice degli altri due).

****

04- Mio intervento il 30 novembre alla Statale di Milano (e iscrizioni Corso di Perfezionamento)

Segnalo questo evento in cui interverrò:
- https://www.linkedin.com/feed/update/urn:li:activity:6336633715602653184.

30 novembre 2017 ore 15-19 Statale di Milano.
"Dalla data protection alla data governance: il GDPR". Previsto intervento prof. Francesco Pizzetti.

Un sacco di gente interessante (chissà io che ci faccio).

Questo evento è collegato al Corso di perfezionamento "Data Protection e Data Governance" promosso dalla Statale di Milano. E' possibile presentare la richiesta di ammissione entro il 12 dicembre:
- http://www.unimi.it/studenti/corsiperf/112084.htm.

****

05- Mio intervento l'11 dicembre a Napoli

Lunedì 11 dicembre terrò un intervento per l'evento "Sicurezza delle informazioni" organizzato da ITAdvice a Napoli, presso il Grand Hotel Parker's.

L'evento sarà la mattina e, oltre al mio, ci saranno interventi di Massimiliano Musto, Silvio Tortora Maione, Biagio Lammoglia, Emanuela Franco.

Su LinkedIn e Twitter posterò, quando sarà disponibile, il link ufficiale all'evento.

Personalmente sono molto contento di partecipare perché avrò l'opportunità di confrontarmi con Biagio su come mettere insieme in modo furbo la 27001 e il GDPR (da notare che un modo non furbo sapremmo anche trovarlo da soli!).

****

06- Rischi delle tecnologie sanitarie

Marco Fabbrini, che ringrazio, mi segnala il report "Top 10 Health Technology Hazards for 2018" dell'ECRI Institute:
- https://www.ecri.org/Pages/2018-Hazards.aspx.

Ecco cosa mi scrive Marco: "Alla fine i rischi sulla sicurezza IT sono arrivati in cima alla classifica. In particolare da notare il primo della classifica (Ransomware and Other Cybersecurity Threats), ma anche il nono (Flaws in Medical Device Networking Can Lead to Delayed or Inappropriate Care).

Il nuovo regolamento MED, per fortuna, prende in considerazione in maniera forte gli aspetti legati al software ad alla parte IT, punto molto debole fino ad oggi nella gestione dei dispositivi e sistemi medicali".