Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – OTTOBRE 2018
****

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

****
00- Nota

Succede: un mese (settembre 2018) con 24 articoli e quello successivo con 4 articoli, peraltro tutti miei.

****
01- Stato delle norme ISO/IEC 270xx - Ottobre 2018

La prima settimana di ottobre a Gjøvik (Norvegia) si è concluso l'incontro semestrale del ISO/IEC JTC 1 SC 27, ossia del comitato che si occupa della redazione delle norme della serie ISO/IEC 27000.

Non ho partecipato direttamente e quindi fornisco indicazioni tratte dai resoconti finali.

Per quanto riguarda i lavori sulle norme della privacy:
- la ISO/IEC 27552 (ossia lo standard che potrebbe essere quello su cui sarà basata la "certificazione GDPR") dovrebbe passare allo stato di DIS e quindi essere pubblicata a fine 2019;
- la ISO/IEC 27018 (Code of practice for PII protection in public clouds acting as PII processors) è stata aggiornata per allinearla alle altre norme uscite in questi anni e la pubblicazione della nuova versione è prevista per fine anno;
- per la l'ISO/IEC 29101 (Privacy Architecture Framework), la situazione è la medesima della ISO/IEC 27018;
- per la ISO/IEC 27550 (Privacy engineering for system life cycle processes) sono proseguiti i lavori.

Per quanto riguarda le attività del WG 1, ossia quelle più strettamente collegate alla ISO/IEC 27001, segnalo le cose per me più interessanti:
- avvio formale, con la prima bozza, dei lavori per la prossima versione della ISO/IEC 27002 sui controlli di sicurezza (a questo punto prevista non prima del 2021);
- ulteriore proseguimento dei lavori per la futura ISO/IEC 27005 sulla valutazione del rischio (i lavori sono ripartiti dalle discussioni preliminari);
- continuazione dei lavori per apportare correzioni alla ISO/IEC 27006, la norma per gli organismi che certificano

ISO/IEC 27001;
- continuazione dei lavori per aggiornare la ISO/IEC 27013, ossia la norma che tratta delle relazioni tra ISO/IEC 27001 e 20000-1, visto il recente aggiornamento di quest'ultima;
- avvio dei lavori per un aggiornamento minore della ISO/IEC 27007, linea guida per la conduzione degli audit sulla ISO/IEC 27001, per allineamento alla ISO 19011:2018; pertanto partirà dallo stato di DIS per essere pubblicata ad autunno 2019 (ricordo che la ISO/IEC 27007 è stata aggiornata nel 2017 e tutte queste rilavorazioni di norme mi lasciano perplesso);
- passaggio a DIS (con possibile pubblicazione ad autunno 2019) della ISO/IEC 27102 sulle cyber-assicurazioni;
- sono proseguite le discussioni sull'utilità del SOA; dal rapporto dell'incontro capisco che il 75% dei partecipanti vuole mantenere nella ISO/IEC 27001 l'Annex A e il requisito sul SOA.

Il WG 4, dedicato ad aspetti più tecnici della sicurezza, ha lavorato alla seconda bozza di lavoro della norma ISO/IEC 27030 dal titolo "Guidelines for security and privacy in Internet of Things (IoT)". La prima bozza era un documento sostanzialmente vuoto.

Altri documenti su cui ha lavorato il WG 4, che io ritengo interessanti, ma ancora in fase di bozza, sono:
- aggiornamento della ISO/IEC 27031 sulla continuità operativa;
- aggiornamento della ISO/IEC 27032 sulla sicurezza Internet (era un documento dedicato alla Cybersecurity, tema ora demandato alle norme della serie 271xx);
- ISO/IEC 27045 sui big data.

Per quanto riguarda i partecipanti, so solo che al WG 1 (i gruppi sono 5 e il WG 1 è il più numeroso) hanno partecipato esperti e delegati da 29 Paesi. La delegazione italiana (per i soli WG 1 e WG 5) era composta da ben (!) tre persone.

Prossimo meeting: aprile 2019.

****

02- Mio articolo sulla nuova ISO/IEC 29100 "Privacy framework"

Avevo già scritto che è stato recentemente pubblicato un aggiornamento della ISO/IEC 29100 dal titolo "Privacy framework". Ho approfondito un po' la questione in questo articolo:
- https://www.ictsecuritymagazine.com/notizie/aggiornamento-della-iso-iec-29100-privacy-framework/.

****

03- Mio articolo sulla nuova versione della ISO 19011 sugli audit

Un mio articolo dal titolo "Nuova versione della ISO 19011 sugli audit":
- https://www.ictsecuritymagazine.com/articoli/nuova-versione-della-iso-19011-sugli-audit/.

****

04- Mio articolo "Nuova versione della ISO/IEC 20000-1"

Un mio articolo su ICT Security Magazine sulle novità della ISO/IEC 20000-1:2018, che sostituisce la ISO/IEC 20000-1:2011:
- https://www.ictsecuritymagazine.com/notizie/nuova-versione-della-iso-iec-20000-1/.

****