Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – NOVEMBRE 2019
****

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- Standard: Nuova versione della ISO 22301 sulla continuità operativa

E' uscita la nuova versione della ISO 22301, lo standard con i requisiti per (e per certificare) un sistema di gestione per la continuità operativa. Il titolo corretto è: "ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements":
- https://www.iso.org/standard/75106.html.

Ringrazio Claudio Sartor che mi ha segnalato questo articolo dal titolo "Come cambia lo standard internazionale di business continuity (ISO 22301)":
- https://www.ictsecuritymagazine.com/articoli/come-cambia-lo-standard-internazionale-di-business-continuity-iso-22301/.

****

02- TISAX - Infosec per automotive

TISAX è uno schema per i sistemi di gestione per la sicurezza delle informazioni per il settore automotive.

Lo schema riprende quanto già previsto dalla ISO/IEC 27001. Però è interessante leggere l'Excel di autovalutazione, visto che approfondisce alcuni temi:
- https://www.vda.de/en/services/Publications/information-security-assessment.html.

****
03- Minacce e attacchi: Rapporto MELANI 2019/01

Melani è la "Centrale d'annuncio e d'analisi per la sicurezza dell'informazione" della Confederazione Svizzera. Forse sbaglio, ma dovrebbe essere il CERT nazionale o un suo equivalente. Ogni 6 mesi pubblica un rapporto sullo stato della sicurezza. L'ultimo è quello relativo al primo semestre 2019: https://www.melani.admin.ch/melani/it/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-1.html.

Io penso che sia il rapporto meglio scritto e meglio organizzato di tutti quelli che ho visto. Conosco pochissimi equivalenti e li ritengo meno interessanti (e mi dispiace che non ci siano più emulatori; il nostro www.certnazionale.it è inguardabile, da questo punto di vista).

MELANI ha anche creato liste di controllo per attacchi DDOS, sistemi industriali, CMS e siti web (oltre ad altri documenti):
- https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide.html.

****
04- Privacy: una riflessione sulle certificazioni ISO/IEC 27701

Pierfrancesco Maistrello mi ha scritto una riflessione interessante sulle certificazioni privacy, la ISO/IEC 27701 e la necessità o meno di avere certificazioni con accreditamento ISO/IEC 17021 o 17065 (ricordo che il GDPR richiede il secondo).

<<
Non credo che le organizzazioni siano pronte a certificarsi GDPR art.42-43: è un passo troppo lungo e complesso per molti. Senza contare che il vantaggio di queste certificazioni è tutto da dimostrare. Ricordo sempre il ragionamento di Bolognini, che diceva che una certificazione ex art.42 non pienamente gestita o "bucata" potrebbe trasformarsi in un aggravio delle inadempienze del titolare, in caso di valutazione della sanzione amministrativa.

Ma certo molta gente ha bisogno di indicazioni per strutturare il sistema di gestione delle proprie misure e quindi una norma autorevole, anche se non coerente a GDPR art. 42-43, è utile.

Ulteriore riflessione. Guardando il recente sweep del garante fatto con Netcomm, si vede che hanno chiesto ad aziende che hanno attività e-commerce se le loro data breach policies contengono specifiche indicazioni sulla gestione delle eventuali azioni correttive. Io trovo questa attitudine al miglioramento delle misure di sicurezza la principale lacuna dei clienti con cui lavoro in questi mesi. Questo mi riporta a pensare che una norma come la ISO/IEC 27701, anche se non GDPR art. 42-43, sarà utile in questo senso.
>>

****

05- Privacy: Il DPO deve essere un legale (ma forse anche no)

Ricordo che a settembre avevo citato una sentenza del TAR del Friuli Venezia Giulia per cui il DPO deve essere un legale:
- blog.cesaregallotti.it/2018/09/il-dpo-deve-essere-un-legale-cosi-dice.html.

Pierfrancesco Maistrello mi ha segnalato un commento dalla newsletter di IAPP. Non credo che il contenuto sia liberamente distribuibile, perciò traduco molto liberamente come segue.

"Non c'è niente di male nell'usare un legale come DPO, ma si rischia di pagare tanto per persone (gli avvocati) che, per attitudini, sono estremamente avversi ad ogni rischio. Ma l'applicazione di normative come il GDPR si basa su un approccio "basato sul rischio" e questo può essere garantito anche, e forse meglio, da persone non legali, ma con approccio pragmatico. I legali possono essere utilissimi per interpretazioni e chiarimenti".

****

06- Privacy: Telecamere sul posto di lavoro e nel processo penale

Sull'uso delle telecamere, recentemente sono arrivate due notizie.

La prima la fornisco in modo molto sintetico perché non ho molto di più. Però dal titolo si capisce molto: "La violazione della disciplina privacy non è motivo di inutilizzabilità delle videoriprese nel processo penale".
- https://www.forensicsgroup.eu/2019/10/la-violazione-della-disciplina-a-tutela-della-privacy-non-puo-costituire-uno-sbarramento-rispetto-alle-preminenti-esigenze-del-processo-penale/.

La seconda è invece un intervento del nostro Garante su una sentenza della Corte di Strasburgo. Il comunicato "Telecamere sul luogo di lavoro: dichiarazione di Antonello Soro, Presidente del Garante per la privacy, su sentenza Corte di Strasburgo":
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9164334.

Mi pare che si possa sempre ritrovare il rispetto del principio di proporzionalità (ossia installazione sulla base di sospetti circostanziati, tempo e area limitati, mancanza di alternative per dimostrare l'evento). Copio e incollo: La videosorveglianza occulta è, dunque, ammessa solo in quanto extrema ratio, a fronte di "gravi illeciti" e con modalità spazio-temporali tali da limitare al massimo l'incidenza del controllo sul lavoratore. Non può dunque diventare una prassi ordinaria.

****

07- Privacy: Stato delle assicurazioni GDPR in Europa

Pierfrancesco Maistrello mi ha segnalato questo schema che indica la possibilità di assicurarsi rispetto alle multe del GDPR:
- https://www.dlapiper.com/de/austria/insights/publications/2019/07/updated-guide-on-the-insurability-of-gdpr-fines-across-europe/.

Lo studio completo è disponibile dietro registrazione e mi sembra curioso, visto che si parla di privacy. Comunque ho deciso di non registrarmi e quindi di non leggere il rapporto completo. Infatti l'Italia appare come Paese in cui non sono disponibili assicurazioni per multe da GDPR, ma mi sembra che qualche cosa sia invece stato sviluppato. Forse il rapporto completo riporta qualche indicazione in più.
****