Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – DICEMBRE 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

****
00- Editoriale

Come ogni anno, a dicembre faccio gli auguri ai miei lettori.

Il 2019 ha portato molte novità e secondo me anche il 2020 ne porterà. Dovremo stare attenti.

Sono molto contento che finalmente la sicurezza sia diventata un tema significativo. Questo ha ampliato molto il numero di sedicenti esperti e anche il numero di articoli, pareri, post, convegni e interventi vari. Alcuni sono validi, moltissimi sono evidentemente improvvisati. E non perdono neanche tanto l'inesperienza: prima di scrivere o parlare in pubblico bisognerebbe avere studiato un po' di più.

Quindi dobbiamo stare attenti a distinguire gli interventi validi, in modo da valorizzarli e ricordarsi positivamente gli autori, da quelli improvvisati, imprecisi o frutto di stanche ripetizioni di concetti scorretti o superati, in modo da ricordarsi di stare alla larga da questi autori. Non è facile. Errori, poi, ne fanno tutti (c'è una lista bella lunga con i miei), ma dobbiamo ricordarci di quelli che li fanno per superficialità o disinteresse verso la qualità dell'intervento (mentre l'interesse economico è invece sempre presente) e di quelli che magari non hanno accesso a tutte le informazioni o eccedono in entusiasmo.

Non è facile, ma questo, a mio parere, sarà il nostro compito nel 2020 (oltre a seguire la certificazione del cybersecurity act, quella ISO/IEC 27701, le prossime pubblicazioni ENISA e chissà cos'altro). Confesso che non mi interessa chi sarà il prossimo Garante per la privacy.

Quindi, dopo questo concione: Buone feste a tutti. In particolare, Buon Natale e Buon anno.

****

01- Privacy: Partito l'accreditamento per la ISO/IEC 27701 (certificazione privacy)

Accredia ha pubblicato la "Circolare tecnica DC N° 10/2019 – Disposizioni in merito all'accreditamento norma ISO/IEC 27701":
- https://www.accredia.it/documento/circolare-tecnica-dc-n-10-2019-disposizioni-in-merito-allaccreditamento-norma-iso-iec-27701/.

In essa sono fornite le regole che devono seguire gli organismi di certificazione per accreditarsi e quindi fornire servizi di certificazione per la ISO/IEC 27701.

Ricordo che la ISO/IEC 27701 è la norma per certificare il sistema di gestione per la protezione dei dati personali (personal information management system), di cui già parlai in precedenza:
- http://blog.cesaregallotti.it/2019/10/stato-delle-norme-isoiec-270xx-aggiunta.html.

Questa mossa sta facendo muovere un po' di cose. Purtroppo ho letto, anche su testate prestigiose, elucubrazioni in merito alla possibilità di usare questa norma per la "certificazione in base all'articolo 42 del GDPR" (errori in cui io stesso incappai, per la verità) e retroscena mai visti. Ribadisco: la ISO/IEC 27701 non può essere usata per la "certificazione in base all'articolo 42 del GDPR" e al momento non sono disponibili standard di organismi di normazione riconosciuti che vanno in questo senso. L'unico retroscena è che il gruppo editoriale non aveva pienamente riflettuto sul fatto che uno standard costruito sulla base della ISO/IEC 27001 (come la ISO/IEC 27701) non avrebbe potuto riportare requisiti per la certificazione di un processo (ossia sulla base della ISO/IEC 17065, come richiesto dal GDPR), ma solo per la certificazione di un sistema di gestione (ossia sulla base della ISO/IEC 17021).

Purtroppo poi alcuni nomi, anche significativi, confondono le acque, fornendo indicazioni e critiche non completamente corrette, per promuovere altri schemi (che però hanno più problemi di quelli denigrati):
- https://dptel.imperialida.com/2019/12/prassi-di-riferimento-e-simili-come-meccanismi-di-certificazione-della-protezione-dei-dati/.

Per questo, raccomando di leggere la risposta di Fabio Guasconi su LinkedIn:
- https://www.linkedin.com/posts/rosarioimperiali_prassi-di-riferimento-e-simili-come-meccanismi-activity-6611178784567762944-xdP-/.

Tornando alla circolare Accredia, apprezzo il fatto che alcune richieste sono poste in modo meno prescrittivo, mentre per altri schemi erano poste in modo molto più preciso. Mi riferisco ad alcune richieste che io ritengo fuori luogo, come la visita presso tutti i data centre o la necessità, per gli auditor, di avere competenze sulla ISO/IEC 20000 o altri standard non pertinenti.

****

02- Privacy: ISDP 10003:2018 di Inveo disponibile gratuitamente

Inveo ha reso disponibile gratuitamente la ISDP 10003:2018, ossia il documento con i requisiti per ottenere una certificazione privacy e con accreditamento ISO/IEC 17065 (ossia come richiesto dal GDPR):
- https://www.in-veo.com/it/newsletter-privacy-tools.

Io ebbi l'opportunità di leggere le bozze (questa non la scarico perché richiede la registrazione), ma avevo sollevato delle obiezioni. Non ricordo bene quali, per la verità. In generale, però, non ho colto finezze particolari per la certificazione di processo anziché di sistema di gestione.

L'obiettivo è evidentemente quello di promuovere e diffondere ulteriormente lo schema e si aggiunge ad altre iniziative di Inveo in questo senso (la pubblicità, la partecipazione a studi, la richiesta, purtroppo accolta, ad Accredia di promuovere i corsi su questa norma).

Io continuo a pensare che queste certificazioni dovrebbero basarsi su norme discusse e pubblicate da enti di normazione riconosciuti, non da singoli enti (per quanto meritori possano essere).

Ringrazio Andrea Caccia per la segnalazione (e anche per il supporto).

****

03- Privacy: Multa del CNIL per chiamate di marketing indesiderate (e uso del campo note)

Pierfrancesco Maistrello mi ha segnalato la multa di 500mila Euro fatta dal CNIL alla società Futura Internationale per violazione del GDPR:
- https://www.cnil.fr/fr/futura-internationale-sanction-de-500-000-euros-pour-demarchage-telephonique-illegal.

In sostanza, questa società ha chiesto a diversi contact centre esteri di fare chiamate di marketing ai potenziali clienti, senza però attivare processi per l'esercizio del diritto di opposizione. Trovo bello poi che il CNIL abbia multato anche la carenza di informazioni fornite al personale interno. Altri due punti sono: mancata collaborazione con l'autorità e carenza di garanzie nel trasferimento dei dati.

Ultimo punto significativo del provvedimento è l'uso scorretto dei campi note nei software usati per tracciare le chiamate e le relazioni con i clienti e potenziali clienti. Su questo argomento non avevo mai riflettuto. Invece il CNIL ha scritto una nota:
- https://www.cnil.fr/fr/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper.

Ecco i consigli:
- informare gli interessati della raccolta delle note;
- pensare che gli interessati potrebbero esercitare il diritto di accesso;
- scrivere note oggettive, mai eccessive o insultanti (su questo vanno formati gli operatori);
- attenzione ai dati personali appartenenti a categorie particolari;
- usare strumenti tecnologicamente appropriati (p.e. evitare i campi note in favore di menu a tendina, avere funzionalità per verificare periodicamente come sono usati i campi note).

****

04- Controlli sui lavoratori e certificati penali (sentenze cassazione)

Luca De Grazia mi ha segnalato un articolo di Donato Apollonio su Pluris (a cui non ho accesso).

Sui precedenti penali, mi sono segnato quanto segue.

La sentenza Cass. Sez. Lav. 17 luglio 2018, n. 19012 dice: la richiesta del certificato penale integra un limite rispetto alla previsione di cui all'articolo 8 dello Statuto dei Lavoratori ("è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi (...) su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore") che si giustifica con la rilevanza ai fini della valutazione dell'attitudine professionale del lavoratore della conoscenza di date informazioni relative all'esistenza di condanne penali passate in giudicato".

Quindi sembra che sia legittimo richiedere il certificato penale in molti casi.

Più curiosa è la questione relativa all'aspirante lavoratore che si è impegnato a produrre il certificato dei carichi pendenti mediante la sottoscrizione di un format di dichiarazione individuale. In questo caso, risultano irrilevanti le lamentate violazioni di legge in ordine all'art. 8 dello Statuto dei lavoratori e all'art. 27 della Costituzione ed è legittimo il rifiuto del datore di procedere all'assunzione per carenza dei requisiti previsti (Cass. Sez. Lav. 12 settembre 2018, n. 22173; in senso conforme è anche Cass. Sez. Lav. 16 maggio 2017, n. 12086).

Io sono sempre dell'idea che sia scorretto valutare la professionalità di una persona in base ai suoi precedenti (sia perché il debito nei confronti della società dovrebbe essere estinto, sia perché l'impossibilità di lavorare potrebbe riportare la persona a delinquere), però mi pare giusto segnalare questi orientamenti.

Aggiungo però (anche perché ripreso da Pierfrancesco Maistrello!) che non mi pare che queste sentenze citino il GDPR. E infatti il GDPR prevede che i dati giudiziari possano essere trattati solo se questo è autorizzato da una norma di legge e non mi pare che la normativa citata dalle sentenze autorizzi esplicitamente al trattamento dei dati giudiziari nell'ambito lavorativo in questione.

****

05- Conversione del DL Perimetro sicurezza nazionale cibernetica

Fabrizio Monteleone di DNV GL mi ha segnalato la conversione del DL 105 del 2019 "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica ((e di disciplina dei poteri speciali nei settori di rilevanza strategica))". La conversione è avvenuta con la Legge 133 del 2019. Su Normattiva si consulta il DL 105 modificato:
- https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-09-21;105!vig=.

Alcuni spunti sulle novità sono in questo articolo su Agenda Digitale:
- https://www.agendadigitale.eu/sicurezza/sicurezza-cibernetica-italiana-cosi-le-misure-si-rafforzano-in-parlamento/.

****

06- Statistiche sui dipendenti pubblici

Riporto un tweet di Paride Leporace, da un tweet di Ernesto Belisario: "L'Italia è un paese di impiegati di mezza età : Dipendenti pubblici sotto i trent'anni d'età: 2,9% . Età media del dipendente pubblico ministeriale: 54,9 anni".

Ho ritrovato questi dati (ricercando qualche fonte) in questo articolo del Corriere della Sera:
- https://www.corriere.it/economia/finanza/19_ottobre_22/porte-aperte-statali-ma-chi-sceglie-giovani-df58d144-f4b3-11e9-bd4f-0986d8452d56.shtml.

Il commento di Ernesto Belisario: "L'età media dei dipendenti pubblici è un fattore che deve essere tenuto in considerazione in tutte le iniziative di trasformazione digitale. Ma - a mio avviso - non rappresenta, in assoluto, un ostacolo all'innovazione del settore pubblico".

Direi che ce n'è abbastanza per ragionare.

Però aggiungerei anche altri dati. Il primo è che il 73% degli italiani usa Internet (uno su quattro NON lo usa!). Il secondo è che solo una parte di questi italiani usa i social network:
- https://wearesocial.com/it/blog/2018/01/global-digital-report-2018.

Io quindi emenderei così il commento: la capacità (e l'età) del personale di un'organizzazione e dei cittadini di usare Internet e gli strumenti informatici, oltre alle esigenze di sicurezza informatica, deve essere tenuta in considerazione quando si avviano iniziative di trasformazione digitale.

****

07- ISO/IEC 330xx - Process assessment (e ISO/IEC 15504 - SPICE)

Sono noti alcuni schemi di valutazione della maturità (o della capacità) dei processi. A me non convincono perché troppo basati sulla quantità di documenti e di registrazioni e perché sono convinto che la realtà non sia facilmente modellabile e l'illusione di farlo, oltre che costare tanto, è pericolosa. Però è bene conoscere questi standard.

Lo schema dell'ISO/IEC era noto come ISO/IEC 15504 e con il nome, piuttosto divertente, di SPICE (Software process improvement and capability determination), dal nome del progetto da cui è partito lo sviluppo dello standard.

Per motivi a me ignoti, la serie ISO/IEC 15504 è in fase di sostituzione da parte degli standard della serie ISO/IEC 330xx.

Ecco quindi lo stato attuale degli standard:
- ISO/IEC 33001: 2015 (concetti e terminologia), che sostituisce la parte 1 della ISO/IEC 15504;
- ISO/IEC 33002:2015 (requisiti per valutare i processi), ISO/IEC 33003:2015 (requisiti per misurare i processi) e ISO/IEC 33004:2015 (requisiti per i modelli di processo) che sostituiscono le parti 2 e 7 della ISO/IEC 15504;
- ISO/IEC 33015:2019 (determinazione dei rischi di processo) al posto delle ISO/IEC 15504-4 e ISO/IEC 15504-9;
- ISO/IEC 33020: 2015 (misurazioni per la valutazione della capacità) che sostituisce parte della 15504-2;
- ISO/IEC 33030:2017 (esempio di valutazione) che sostituisce parte della 15504-3;
- ISO/IEC 33053:2019 (Process Reference Model (PRM) for quality management).

Rimangono ancora "vive" le seguenti:
- ISO/IEC 15504-5 (An exemplar software life cycle process assessment model);
- ISO/IEC 15504-6 (An exemplar system life cycle process assessment model);
- ISO/IEC 15504-8 (An exemplar process assessment model for IT service management);
- ISO/IEC 15504-10 (Safety extension).

Ulteriori documenti sono in fase di lavorazione nella serie ISO/IEC 330xx.

****

08- ENISA good practices for security of IoT

Alessandro Cosenza di BTicino mi ha segnalato che ENISA ha recentemente pubblicato (19 novembre 2019) di "Good practices for security of IoT: Secure Software Development Lifecycle":
- https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1.

Mi sembra molto completo. Tratta di governo, processi, gestione del personale e soluzioni tecnologiche. Mentre i primi punti sono "i soliti", più originali sono le soluzioni tecnologiche. Per chi volesse approfondire, poi, sono segnalati diversi riferimenti (anche se molti riferimenti "tecnici" sono in realtà generici).

****

09- Red and blue team

Vito Losacco mi ha segnalato questo articolo dal titolo "Cybersecurity Red Team Versus Blue Team — Main Differences Explained":
- https://securitytrails.com/blog/cybersecurity-red-blue-team.

Mi pare dia nomi nuovi a gente che prima chiamavamo "Ethical hacker" e "SOC". Però è sempre bene conoscerli.

Trovo interessante la lista delle cose che deve fare la squadra blu (blue team, aka SOC):
- Security audits, such as a DNS audit;
- Log and memory analysis;
- pcap;
- Risk intelligence data analysis;
- Digital footprint analysis;
- Reverse engineering;
- DDoS testing;
- Developing risk scenarios.

****

10- Fine supporto Windows 7

Sta finendo il supporto a Windows 7. Questo articolo di Agenda Digitale indica alcune possibili soluzioni (oltre ad aggiornare i sistemi):
- https://www.agendadigitale.eu/sicurezza/fine-aggiornamenti-windows-7-e-2008-a-rischio-i-pc-della-pa-ecco-i-consigli.

Prego osservare come, in alcuni ambiti, l'esperienza acquisita con la fine del supporto di Windows XP NON sia servita e alcuni si trovano in difficoltà anche in questo caso.

Attenzione: non voglio dire che sia facile dismettere un sistema operativo da un'organizzazione, solo che, in alcuni ambiti, non si è riusciti ad evitare il ripresentarsi

dei problemi poco tempo prima della scadenza.

****

11- Ricerca DNV GL su Privacy & Information Security

DNV GL Business Assurance ha pubblicato la sua ricerca su privacy e sicurezza:
- https://www.dnvgl.com/assurance/viewpoint/viewpoint-surveys/2019Q4/highlights.html.

La segnalo anche perché ho partecipato alla sua progettazione e ho collaborato per alcune sue parti.

Non mi piacciono molto le ricerche, come ho già avuto modo di dire. Però segnalo alcune cose interessanti (a mio parere) emerse da questa:
- consapevolezza del fatto che le competenze sono più necessarie degli strumenti (tool); sembra banale per chi si occupa di sistemi di gestione, ma molti, in realtà, pensano siano più importanti gli strumenti;
- la maggior parte degli intervistati è incerta sugli impatti, in termini di privacy e sicurezza, positivi o negativi delle nuove tecnologie; questa risposta è in controtendenza rispetto a quello che è promosso;
- poche persone si qualificano come esperte in sicurezza e privacy; a vedere lo sbandieramento di certificati e articoli, avrei scommesso su un minor livello di umiltà.

Altre cose si possono ricavare dal rapporto; io ho indicato quelle che a me hanno colpito maggiormente.