Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – GIUGNO 2015

****

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.

E' possibile iscriversi o dis-iscriversi
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/Newsletter.html

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

****

Indice

****

01- Sono su Twitter

Sono su Twitter da metà maggio, dopo che troppe persone mi hanno segnalato quanto fosse importante.

Scriverò solo di cose professionali. In altre parole, non fornirò contenuti diversi da quelli già presenti su blog e newsletter. Solo saranno dei riassunti di 140 caratteri.

Per festeggiarmi, ecco quindi un articolo di Bancaforte su Twitter e su quelli che lo lasciano (o dicono di volerlo lasciare):
- http://www.bancaforte.it/articolo/quelli-che-smettono-di-cinguettare-RB70187w

****

02- Standardizzazione: ISO/IEC 33000 e ISO/IEC 15504 (SPICE)

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione di alcune norme della serie ISO/IEC 33000. Esse sostituiscono le norme della serie ISO/IEC 15504, note come SPICE e dedicate alla valutazione dei processi.

Nel dettaglio:
- la ISO/IEC 33001 (Concepts and terminology) sostituisce la ISO/IEC 15504-1;
- la ISO/IEC 33002 (Requirements for performing process assessment) sostituisce la ISO/IEC 15504-2 e la ISO/IEC 15504-7;
- la ISO/IEC 33003 (Requirements for process measurement frameworks) riprende delle parti delle ISO/IEC 15504-2 e ISO/IEC 15504-7;
- la ISO/IEC 33004 (Requirements for process reference, process assessment and maturity models) riprende delle parti delle ISO/IEC 15504-2 e ISO/IEC 15504-7;
- ISO/IEC 33014 (Guide for process improvement) riprende delle parti delle ISO/IEC 15504-4 e 7;
- ISO/IEC 33020 (Process measurement framework for assessment of process capability) riprende delle parti delle ISO/IEC 15504-2.

La ISO/IEC 33001 segnala la futura pubblicazione di molte altre norme della famiglia.

Come noto, promuovo con prudenza le misurazioni dei processi e, quindi, sono ancora meno entusiasta di quanto riguarda capacità dei processi e modelli di maturità. Però sono argomenti che è bene conoscere almeno in modo generale (segnalo, per un riassunto, il Cobit 5).

Di queste pubblicazioni ho potuto solo vedere dei pdf iper-protetti che non permettono neanche la stampa. Vedo che l'ISO sta cercando di proteggere sempre più efficacemente la sua proprietà intellettuale (per quanto riceva soldi anche dalle stesse persone che scrivono gli standard...).

****

03- Standardizzazione: ISO/IEC 2382

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione della ISO/IEC 2382 dal titolo "Information technology -- Vocabulary".

È gratuita e quindi si può scaricare direttamente da www.iso.org.

In realtà pdf consta di 4 pagine, perché il documento vero e proprio è visualizzabile direttamente dal web. Ho provato a copiare e incollare il contenuto e ho visto che occupa poco meno di mille pagine. Segnalo poi che ho avuto qualche difficoltà con alcuni browser.

Sicuramente, però, si tratta di un documento importante:
- https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en.

****

04- Standardizzazione: ISO/IEC 20000 e informatica - Altri spunti

Tony Coletta, rappresentante italiano al SC 40, è stato stimolato (come speravo) dal mio breve articolo di metà aprile:
- http://blog.cesaregallotti.it/2015/05/isoiec-20000-e-informatica.html

Quindi, da qui in poi, riporto solo e unicamente le sue parole e lo ringrazio.

La confusione è ancora grande sotto il cielo.

I britannici e comunque anche l'attuale convenor insistono che la ISO/IEC 20000 si applica anche al di fuori dell'IT ma ogni volta che tentano di ufficializzare la cosa, il tentativo viene respinto.

Il WG25 (incaricato, tra le altre cose, della redazione della ISO/IEC 20000-1) è uscito dal SC7 per andare a costituire il SC 40 insieme a quelli della Governance ma JTC1 gli ha imposto il titolo: "SC40 - IT Service Management and IT Governance".

Non possono sfuggire. Fino a quando restano in JTC1 devono rimanere nel dominio Information Technology.

Poi possiamo essere d'accordo o meno che la maggior parte dei requisiti della norma si possono applicare ai servizi in generale ma la norma è stata scritta per l'IT service management.

Nel testo della norma non si dice ogni volta IT Service Management perché "Information Technology" fa parte del titolo in prima pagina quindi è superfluo ripeterlo ogni volta.

D'altronde per essere valida per tutti i servizi, nel working group che l'ha sviluppato, avrebbero dovuto esserci i rappresentanti di tutti gli altri servizi non-IT ma questo non è vero. C'erano solo informatici.

Comunque la cosa si complica ulteriormente se cominciamo a parlare dei servizi "IT enabled", cioè servizi che di per sé non sono servizi IT ma che vengono erogati tramite tecnologie informatiche.

****

05- Standardizzazione: ISO 22313 in italiano

UNI ha pubblicato la versione italiana della ISO 22313 dal titolo "Sistemi di gestione per la continuità operativa: Linee guida".

Non si tratta della ISO 22301 con i requisiti utili anche per la certificazione, che rimane solo in inglese. Trovo bizzarro che abbiano tradotto le linee guida di accompagnamento e non la norma di requisiti, ma tant'è.

La norma, che peraltro non ho trovato illuminante, si può acquistare direttamente da UNI su store.uni.com.

Grazie a Franco Ferrari di DNV GL Business Assurance Italia per la segnalazione.

****

06- Privacy: 2 giugno e Provvedimento cookie

Il 2 giugno 2015 scade il periodo di transizione previsto dal provvedimento del Garante Privacy n. 229 del 4 maggio 2014, il cosiddetto "Provvedimento cookie" applicabile a quasi tutti i siti web.

Non mi dilungo oltre e segnalo questo articolo di Filodiritto, che mi sembra il più completo visto finora:
- http://www.filodiritto.com/articoli/2015/05/cookie-policy-si-avvicina-la-scadenza-del-2-giugno.html

Successivamente, da Twitter (@uniprivacy), ho ricevuto notizia del documento del Garante dal titolo "Chiarimenti in merito all'attuazione della normativa in materia di cookie":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4006878

Un articolo critica questo ulteriore documento (che in effetti non chiarisce tanto):
- http://www.wired.it/attualita/2015/06/05/documento-garante-privacy-chiarisce-tutti-gli-aspetti-sui-cookie

Noto una cosa: alla domanda "Uso di piattaforme che installano cookie" mi sembra manchi qualcosa. Io ho un blog gestito da Blogger (Google). Io (insieme alla mia amica Anita) non ho fatto altro che scegliere un'impostazione del blog, cambiare colori e aggiungere qualche opzione come quella per inserire il logo Creative Commons. Cosa dovrei fare? Ogni chiarimento del Garante non lo dice, anche se l'articolo di Wired fa notare che molti si sono fatti questa domanda.

Io ho deciso di non fare quasi nulla anche perché non posso fare nulla, se non scrivere poche righe in merito.

****

07- Privacy: E-mail personali e dati sanitari

Questa me l'ha segnalata Marco Fabbrini, che ringrazio:
- http://www.esanitanews.it/?p=2908.

Se ho capito bene la notizia, si tratta di una cosa buffa e bizzarra: una signora invia un messaggio promozionale a due clienti-amici chiedendo di inoltrarlo ad altri. Essendo però anche amici, aggiunge notizie personali relative alla propria salute. Gli amici, facendole un piacere, inoltrano l'e-mail ai propri contatti commerciali (ritoccando però le cifre dell'offerta), senza però cancellare le notizie personali. La signora se ne risente e fa reclamo al Garante della privacy (chiedendo tra l'altro di riinviare la comunicazione con le cifre originali).

Il provvedimento del Garante:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3966213

Mi viene da pensare che la signora abbia perso un paio di amici. Oltre a ciò, qualche lezione da imparare:
- fate attenzione alle "amiche" (o "amici"), che uniscono notizie professionali a notizie personali e poi non esitano a fare ricorso all'autorità;
- quando inoltrate i messaggi, verificate che non ci siano cose da cancellare;
- se avete dei colleghi-amici, mandate mail separate per cose personali e cose professionali.

La cosa buffa: il Garante ha dovuto richiamare i due "inoltratori selvaggi" chiedendo loro di mandare informative, di non trattare più i dati della signora e di vigilare sull'operato delle proprie persone. Ho

capito che dovrò inviare un'informativa a tutte le persone che si comportano da "amici" con me e cancellare ogni e-mail che mi mandano!

****

08- Privacy: Provvedimento biometria - Errata corrige del Garante

Mauro Bert mi ha segnalato che il Garante privacy ha corretto il "Provvedimento generale prescrittivo in tema di biometria".

L'errata corrige Rettifica alla Deliberazione n. 513 del 12 novembre 2014 recante 'Provvedimento generale prescrittivo in tema di biometria' - 15 gennaio 2015 - doc. web n. 3701432) si trova a questo link:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3701432

Il Provvedimento aggiornato si trova al precedente link:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992

Mauro (che ringrazio) riassume: "viene corretta l'errata citazione eliminando UNI e 2005, ma continuando ad ignorare l'esistenza della UNI CEI ISO/IEC 27001:2014".

****

09- Privacy: Data protection officer - Un buon articolo

Finalmente leggo un buon articolo su cosa è e cosa non è il famoso DPO e su quanto valgono le certificazioni professionali attualmente promosse da alcuni enti:
- http://www.filodiritto.com/articoli/2015/05/professioni-non-regolamentate-lo-strano-caso-del-privacy-officer.html

Breve riassunto: ritengo che queste certificazioni siano delle bufale.

Aggiornamento: in sede UNINFO sono in fase di avvio le attività per discutere di uno standard su "Figure professionali operanti nel settore ICT – Profili professionali relativi alla privacy".

****

10- Privacy level agreement

Pierfrancesco Maistrello di Vecomp mi ha segnalato questo interessante documento del Cloud security alliance (CSA) dal titolo "Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union":
-
https://downloads.cloudsecurityalliance.org/assets/research/pla/downloads/2015_05_28_PrivacyLevelAgreementV2_FINAL_JRS5.pdf

Il documento riporta le clausole contrattuali da prevedere tra cliente e fornitore cloud, che sia esso titolare autonomo (controller) o responsabile del trattamento (processor). Mi sembra completo e interessante.

Una sola critica, che è poi quella che faccio sempre: purtroppo il titolo riguarda solo i servizi cloud, quando invece mi sembra applicabile a tutti i fornitori di servizi informatici; ecco quindi che mi

preoccupa questa estrema attenzione ai fornitori di servizi cloud perché non ne vedo una simile per le altre tipologie di fornitori, in alcuni casi più numerosi e critici di quelli cloud.

****

11- BYOD e dispositivi mobili

Da Twitter, Alessandro Vallega ha inoltrato il link a questo articolo dal titolo "Safeguarding the Public Sector against the Threat of Device Loss":
- http://www.infosecurity-magazine.com/opinions/chris-mayers-chief-secarccitrix/.

In sintesi, il CESG, ossia l'autorità nazionale UK per la sicurezza informatica, ha pubblicato delle guide sul BYOD e sull'uso di dispositivi mobili (in verità le guide sono del 2014, ma all'epoca forse ci eravamo distratti):
- https://www.gov.uk/government/collections/bring-your-own-device-guidance;
- https://www.gov.uk/government/collections/end-user-devices-security-guidance.

Confesso che ho trovato la lettura più complicata di quanto mi aspettassi. Forse perché il tutto è diviso in più documenti che ho fatto fatica a collegare tra loro. Oppure perché si tratta di una "alpha release".

****

12- Medical Device Security Guidance for Developers

Dal SANS Newbites: è disponibile la pubblicazione "Building Code for Medical Device Software Security". Si può scaricare da questo breve articolo di presentazione:
- http://www.scmagazine.com/guidance-meant-to-reduce-the-risk-of-malicious-attacks-on-medical-devices/article/416163/.

Vale la pena osservare che si tratta di una sorta di "SSDLC in sintesi" e non applicabile ai soli dispositivi medici.

Leggendo questo documento si trovano un paio di interessanti link, sempre legati allo sviluppo sicuro.

Il primo è la pagina Cybersecurity di ieee che mette a disposizione alcuni articoli interessanti:
- http://cybersecurity.ieee.org/

Più interessante ancora è la pubblicazione "Avoiding the Top 10 Security Flaws":
- http://cybersecurity.ieee.org/center-for-secure-design/avoiding-the-top-10-security-flaws.html

Il secondo link che segnalo è quello di SAFECode:
- http://www.safecode.org/

Nella sezione "pubblicazioni" ci sono molte cose interessanti, tra cui "Fundamental Practices for Secure Software Development" e "Security Engineering Training".

****

13- Google Identity Platform

La Google Identity Platform sembra una bella iniziativa di Google (notizia dal Sans NewsBites): un insieme di programmi per incoraggiare gli sviluppatori a creare apps e siti web più sicuri:
- http://www.cnet.com/news/google-beefs-up-user-identity-safety-net-for-apps/

Chissà quanti ne faranno uso?

****

14- Guida NIST sui sistemi industriali

Massimo Cottafavi di SNAM mi ha segnalato la nuova edizione della Special Publication 800-82 del NIST dal titolo "Guide to Industrial Control Systems (ICS) Security". La precedente risale al 2006. Si trova a questo link:
- http://csrc.nist.gov/publications/PubsSPs.html#800-82

Non l'ho ancora letta con attenzione. Spero di trovarci considerazioni sulle caratteristiche dei sistemi industriali e non le "solite cose" facilmente mutuabili dai normali sistemi informatici (password, autorizzazioni, difesa perimetrale, eccetera).

Qualcosa l'avevo trovata nel Quaderno Clusit numero 7 dal titolo "Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, ecc.)" (si trova al link http://www.clusit.it/download/index.htm).

****

15- Analisi sugli impianti industriali insicuri

Segnalo questo articolo, con link ad un'ulteriore ricerca più approfondita, su quanto sono esposti i sistemi informatici di controllo industriale:
- https://www.linkedin.com/pulse/un-sacco-di-pallini-blu-sullitalia-impianti-esposti-su-enzo-m-tieghi

Confermo che alcune imprese stanno lavorando al miglioramento del loro livello di sicurezza. Evidentemente non abbastanza.

****

16- Intrusione nel sistema IT di un aereo

La notizia ha fatto il giro del mondo, ma io l'ho presa dal SANS NewsBites: un ricercatore, che si sta dedicando molto alla (in)sicurezza dei sistemi di volo, ha dichiarato di essere riuscito ad accedere a quelli di almeno 14 aerei su cui ha volato. Questo usando il sistema di intrattenimento presente su molti apparecchi.

Un paio di link:
- http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/
- http://arstechnica.com/security/2015/05/fbi-researcher-admitted-to-hacking-plane-in-flight-causing-it-to-climb/

Mancano dettagli per capire se si tratta di uno scherzo o di una cosa vera. Io copio, incollo e traduco un tweet, a sua volta riportato dal secondo articolo: "O ha mentito sull'intrusione negli aerei in volo o è

veramente riuscito ad accedere ai sistemi di aerei in volo. Tutte e due le opzioni sono inaccettabili da un professionista di sicurezza delle informazioni".

****

17- I bambini possono insegnarci la sicurezza delle informazioni

Interessante articolo che rigiro dalla newsletter di Anssaif:
- http://www.key4biz.it/assetprotection-sensibilizzare-i-ragazzi-alla-sicurezza-per-aiutare-anche-gli-adulti/118303/

I bambini e i ragazzini sono delle spugne e, se si spiega loro l'importanza della sicurezza su Internet, stanno attenti. I bambini, l'avrete notato, si arrabbiano quando noi adulti non seguiamo le stesse regole che abbiamo dato loro; insomma, come avere un allarme ogni volta che facciamo qualcosa di avventato su Internet!

Forse i millennials saranno più bravi dei loro predecessori che scrivono di tutto su Internet senza preoccuparsi delle conseguenze e forse più bravi degli ultra 30enni che o non usano Internet del tutto o lo fanno in modo molto insicuro.