****
IT SERVICE MANAGEMENT NEWS – MAGGIO 2011
****

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 disiscriversi
- 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- ISO/IEC 20000-1:2011 e traduzione in italiano

Tony Coletta mi annuncia: "La nuova edizione della ISO/IEC 20000-1 è stata pubblicata il 12 aprile 2011. Abbiamo pronta la traduzione fatta da un gruppo di volontari itSMF ed il sottoscritto. L'abbiamo sottoposta all'approvazione dell'UNI. Attendiamo fiduciosi"

Lo ringrazio per l'aggiornamento.

Aggiungo poi che non ci sono ancora notizie sulle certificazioni ISO/IEC 20000-1:2011 perché gli Organismi di Accreditamento non hanno pubblicato alcun regolamento in merito. Appena riceverò notizie, le pubblicherò sul blog http://blog.cesaregallotti.it/ e, come al solito, sulla newsletter mensile.

****

02- Privacy: ulteriori semplificazioni

Daniela Quetti (della DFA) segnala: la lettura del DECRETO-LEGGE 70 del 13 maggio 2011, in particolare dell'art. 6 comma 2 lettera a) che modifica il Codice Privacy (decreto legislativo 30 giugno 2003, n. 196). Il titolo dell'articolo è "Ulteriori riduzione e semplificazioni degli adempimenti burocratici"

Daniela ci ricorda che siamo ancora in fase di Decreto Legge (pertanto non ancora convertito in Legge), ma di fatto cogente.

Link al testo:

http://www.normattiva.it//dispatcher?task=attoCompleto&service=212&datagu=2011-05-13&redaz=011G0113&parControllo=si&connote=false&aggiorn=si&datavalidita=20110517#

****

03- Privacy: Pubblicazione di dati personali

Il 2 marzo, il Garante ha pubblicato le "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web".

Inizialmente ho ignorato questo Provvedimento, visto che è specifico per la Pubblica Amministrazione. Lo segnalo perché comunque molti privati pubblicano sui propri siti dati personali, atti e documenti e dovrebbero comunque prendere spunto da quanto previsto per la PA.

Il Provvedimento:
http://www.garanteprivacy.it/garante/doc.jsp?ID=1793203

****

04- Privacy: dei Titolari e dei Responsabili esterni (puntata del 18 maggio 2011)

Dopo il mio articolo del mese scorso, tre miei lettori hanno dichiarato la loro contrarietà alle mie deduzioni. Uno ha "promesso" un articolo (ma non l'ha ancora pubblicato), un altro ha "promesso" di inviarmi dei link a delle sentenze (non ancora arrivati) e l'ultimo mi ha segnalato che sono in corso di preparazione delle linee guida del Garante sul trattamento dei dati personali da parte delle banche.

Quest'ultimo caso è il più interessante: la bozza dice che un outsourcer deve essere nominato responsabile esterno quando il titolare ha potere su: (i) assumere decisioni relative alle finalità del trattamento; (ii) impartire istruzioni e direttive vincolanti; (iii) svolgere funzioni di controllo. Non dice cosa bisogna fare negli altri casi.

Avrei voluto, infine, riflettere su come sono stati scritti gli articoli del Codice Privacy italiano rispetto alla Direttiva Europea e su altre cose. Ci proverò per la prossima volta.

****

05- Abrogazione del SAS 70 e i nuovi SOC Report

Un articolo dell'ISACA Journal Volume 2 del 2011 dal titolo "Understanding the New SOC Reports" segnala l'abrogazione dei report SAS 70 in favore dei nuovi SOC reports.

Infatti, i report SAS 70 erano nati per gli audit sui sistemi contabili e recentemente erano stati utilizzati in modo improprio anche per dimostrare la sicurezza di un IT service provider su standard di controlli di sicurezza non definiti.

L'AICPA ha quindi definito 3 nuove tipologie di report:
- il SOC-1 o SSAE 16, che rimpiazza il SAS 70 propriamente detto e che riguarda i soli sistemi contabili
- il SOC-2 è un report più tecnico, dedicato a uno o più elementi (sicurezza, disponibilità, integrità, riservatezza e privacy), i cui relativi controlli sono descritti nel "Trust Services Principles and Criteria";
- il SOC-3 è una sorta di riassunto del SOC-2 destinato alla pubblicazione; è possibile paragonarlo alla certificazione ISO/IEC 27001 con tanto di marchio da pubblicare sul sito web.

I SOC possono essere di tipo 1 (meno estesi e più legati alla fase di pianificazione dei controlli) o di tipo 2 (con anche la valutazione di come i controlli operano in pratica e la descrizione dei test condotti dall'auditor)

Maggiori (e quasi sicuramente più precisi) dettagli:
-
http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TrustServices/DownloadableDocuments/10957-378%20SOC%20Whitepaper.pdf

I "Trust Services Principles and Criteria" sono disponibili su
http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TrustServices/DownloadableDocuments/FINAL_Trust_services_PC_Only_0609.pdf

****
06- Sicurezza dei dati in ambito farmaceutico

Il 22 marzo ho assistito al Workshop "Annex 11" organizzato a Milano da CTP System (www.ctpsystem.com), società specializzata in consulenza in ambito farmaceutico.

Per capire meglio di cosa si tratta, riporto il link alla presentazione:
http://www.ctpsystem.com/home/images/PDF/articoloncfmarzo2011_annex11.pdf

In poche parole, si tratta della pubblicazione della nuova versione del capitolo 4 e dell'Annex 11 delle Good Manufacturing practice (GMP), di supporto alla Direttiva 2003/94/EC, che entreranno in vigore a giugno 2011 e che costituiscono lo standard di riferimento per la sicurezza delle informazioni in ambito farmaceutico.

Le nuove normative hanno introdotto i concetti di risk assessment e risk management, di ciclo di vita dei sistemi e di sistemi di gestione. E' stato comunque fatto rilevare che le best practices di settore trattavano già ampiamente questi temi.

Argomenti, quindi, ben noti a chi segue questa newsletter. In questo caso, però, affrontati con l'ottica delle aziende di produzione e non di servizi. Quindi, un'ottica molto pragmatica da una parte ma anche molto più rigorosa dei molti esempi a cui siamo abituati.

Le GMP: http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm.

Il corrispondente USA, ha sigla 21 CFR 11:
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm
ed è accompagnato dalle linee guida della DFA:
- http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm
- http://www.fda.gov/RegulatoryInformation/Guidances/ucm122046.htm

Molto diffuse in ambito farmaceutico sono le GAMP, pubblicate dalla ISPE:
http://www.ispe.org/cs/gamp_publications_section/gamp_publications_overview

Sul Risk Assessment, la bibliografia comprende l'Annex 20 delle GMP, il capitolo 5 e M3 della GAMP 5, una pubblicazione complementare delle GAMP 5, la ISO 14971:2009 (in vigore anche per i medical devices), oltre che le ISO 31000, ISO 31010 e ISO Guide 73.

Un'ultima nota: nel calcolo del livello di rischio, alle ben note variabili di impatto e probabilità (a sua volta funzione di minacce e vulnerabilità), viene aggiunta la rilevabilità.

****

07- Rapporto Melani (Svizzera)

Segnalo l'interessante dodicesimo rapporto semestrale MELANI (Centrale d'annuncio e d'analisi per la sicurezza dell'informazione)della Confederazione Svizzera.

La Svizzera non è l'Italia, ma almeno si tratta di uno studio più vicino a noi rispetto a quelli tipicamente USA.

http://www.melani.admin.ch/dienstleistungen/archiv/01123/index.html?lang=it

(Notizia ricavata dalla newsletter del Clusit).

Inoltre, sempre dalla Svizzera, segnalo il simpatico sito di divulgazione sulla sicurezza informatica Storie di Internet:
http://www.storiediinternet.ch/

****

08- Cloud computing e incidenti

Ecco qui un'ulteriore notizia di un incidente sui servizi cloud di Amazon:
http://www.informationweek.com/news/cloud-computing/infrastructure/229402385

In breve: sono stati distrutti diversi dati di clienti.

Commento: il servizio cloud non si discosta troppo da altri servizi erogati da fornitori. Se il contratto con Amazon non prevedeva il backup dei dati, era opportuno pensarci lo stesso.

Notizia segnalata da SANS NewsBites Vol. 13 Num. 34.

****

09- OMAT e gestione elettronica di documenti

Il 5 e 6 aprile 2011 si è tenuto a Milano il convegno OMAT (www.omat360.it).

Segnalo che le presentazioni del convegno sono disponibili su
http://milano2011.omat360.it/documentazione/omat.php (per accedervi bisogna essere iscritti al convegno).

Io ho trovato interessante soprattutto la presentazione di Atle Skjekkeland (in inglese) su come oggi sono gestite le informazioni aziendali e lo saranno. E' stato interessante capire come le diverse generazioni percepiscono "i dati" e le informazioni: i nuovi lavoratori comunicano via social network, i loro predecessori via email e così via. Diverse percezioni e diverse modalità con cui gestire le informazioni a cui forse non siamo pienamente preparati.

La presentazione, in cui è possibile trovare ulteriori spunti di riflessione, è disponibile anche su
https://aiimtaskforce.box.net/shared/zdfvxlvpa0.

****

10- Privacy Enhancing Technologies

Il 7 aprile, alla Statale di Milano, si è tenuta la lezione aperta dal titolo "Privacy Enhancing Technologies vs. Antiforensics" di Marco A. Calamari del Progetto Winston Smith. La lezione è stata molto interessante anche per l'estesa panoramica sugli strumenti di anonimizzazione per Internet disponibili.

Per saperne di più, consiglio di visitare il sito: http://www.winstonsmith.info/pws/index.html

****

11- Business Continuity e Incident Management

Nella newsletter di marzo, trattando del nuovo CAD, avevo segnalato come disgraziatamente si confonde la Business Continuity con la continuità dei soli sistemi IT e con il Disaster Recovery (termine utilizzato solo per i sistemi IT):
http://blog.cesaregallotti.it/2011/03/nuovo-cad-relazione-convegno-3-marzo.html

Un lettore (anonimo perché non gli ho chiesto se posso pubblicare il suo nome) mi ha fatto giustamente notare che l'approccio secondo cui la Business Continuity si deve occupare anche dei piccoli incidenti di continuità porta al fallimento delle iniziative di BCP (Business Continuity Plan).

Convengo, ma ho fatto qualche riflessione che voglio qui pubblicare:

1- la business continuity è un'attività del business e non dell'IT (questa spero sia una cosa ben chiara a tutti)

2- per fare l'analisi da cui elaborare i BCP, ossia la Business Impact Analysis o BIA, è necessario comprendere i tempi massimi di interruzione che il business può sopportare insieme alla ampiezza della interruzione (in molte realtà, un unico pc rotto per 1 settimana può avere impatti ben diversi di 100 pc per 1 ora). A seconda del business, i tempi massimi possono essere molto ridotti: deve essere la BIA a evidenziare questo parametro.

3- Quando avviene un incidente, a seconda dei tempi previsti di ripristino e dalla sua ampiezza si possono adottare diverse strategie.

4- Solitamente, quando si parla di BCP si intendono i piani da attuare nella peggiore delle ipotesi. L'unica cosa su cui riflettere è che, in realtà, negli altri casi si procede con la "normale" gestione degli incidenti (Incident Management o IM).

5- Io dico che i BCP-estremi (mi permetto di inventare questa definizione) e i piani di IM sono tutti dei BCP e la cosa fondamentale è stabilire quando bisogna adottare gli uni o gli altri (ossia, quando la prima valutazione di un incidente fornisce una previsione di interruzione compresa in un certo intervallo di tempo e una sua ampiezza di un certo tipo, si adottano le procedure A, B o C, che dispongono azioni specifiche tecniche e gestionali).

6- Il problema delle inziative di BCP è che solitamente riguardano solo i casi peggiori, per i quali è richiesta la collaborazione di persone poco preparate ad un certo tipo di riflessione e poco disposte a farle, visto che i casi sono rari. Ritengo che, in questi casi, è sufficiente trattare con loro solo della BIA e dei casi peggiori semplificando (giustamente, come dice il mio lettore) la teoria in favore della pratica.

Nella mia impostazione sono confortato dalla ISO/IEC 20000 che tratta in un unico capitolo la disponibilità dei sistemi e la continuità dei servizi e dalla ISO/PAS 22399 dal titolo "Guideline for incident management and operational continuity management".

Altri contributi alla discussione sono benvenuti.

****

12- Value Assessment Tool

Dall'articolo "Value Assessment Tool for ICT Projects at the European Commission" sul Volume 2, 2011 dell'ISACA Journal, segnalo il VAST, strumento messo a punto in seno alla EC per valutare le proposte di progetti ICT.

Evidentemente il tool è tarato per il business specifico della Commissione Europea, ma può essere un ottimo spunto per altre specializzazioni.

http://ec.europa.eu/dgs/informatics/vast/index_en.htm