****
IT SERVICE MANAGEMENT NEWS - Giugno 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- Novità Privacy (Banche, sanità, telefonia, customer satisfaction, Decreto Sviluppo)
02- Novità sugli standard serie ISO/IEC 27k
03- Infrastrutture critiche e Dlgs 61/2011
04- I primi dieci anni di applicazione del Decreto 231
05- APMG Ente di Accreditamento per la ISO/IEC 20000-1
06- Sul downtime di Aruba
07- Metriche FISMA
08- Report ENISA su resilienza e metriche
09- La natura frattale del ciclo PDCA
10- Internet e politica
11- Confindustria Digitale
12- Un contributo su Business Continuity e Incident Management

****
01- Novità Privacy (Banche, sanità, telefonia, customer satisfaction, Decreto Sviluppo)

--- Banche

Simone Tomirotti mi ha segnalato la pubblicazione delle "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011".

http://www.garanteprivacy.it/garante/doc.jsp?ID=1813953

Su questo documento ci sarebbero dei commenti da fare su un discorso che mi sta cuore su "Titolari e Responsabili esterni". Purtroppo neanche questo mese ho avuto la possibilità di studiare come si conviene (grazie al cielo ho dei lavori da fare e nei fine settimana ho fatto il Presidente del Seggio 300 a Milano). Ci riproverò per luglio.

Aggiungo che Simone ha anticipato di poche ore Andrea Praitano che gentilmente mi ha segnalato anche lui questa notizia.

--- Sanità

Daniela Quetti (DFA) ha segnalato la pubblicazione, da parte del Garante:
- del vademecum intitolato "Dalla parte del paziente. Privacy: le domande più frequenti".
http://www.garanteprivacy.it/garante/doc.jsp?ID=1812194
- delle "Linee guida in tema di trattamento di dati per lo svolgimento di indagini di customer satisfaction in ambito sanitario":
http://www.garanteprivacy.it/garante/doc.jsp?ID=1812910

Le linee guida potrebbero essere utili anche a chi conduce medesime indagini in altri ambiti.

--- Telefonia

Daniela Quetti (DFA) ha segnalato che sono stati prorogati i termini per la realizzazione delle misure previste per gli operatori telefonici e riportate nel provvedimento del 24 febbraio 2011, "Modelli di informativa e di richiesta di consenso al trattamento dei dati personali relativi agli abbonati ai servizi di telefonia fissa e mobile"
http://www.garanteprivacy.it/garante/doc.jsp?ID=1811916

--- Decreto Sviluppo e semplificazioni

A seguito della notizia "Privacy: ulteriori semplificazioni" (http://blog.cesaregallotti.it/2011/05/privacy-ulteriori-semplificazioni.html), segnalo una piccola analisi che ho effettuato in materia.

1- i dati dei clienti e fornitori non sono più oggetto della privacy se trattati unicamente per la gestione del rapporto di lavoro. In particolare, non è più necessario mandare loro l'informativa.

2- Attenzione però: questa esclusione sarà annullata laddove quei dati siano oggetto di trattamento per finalità commerciali, pubblicitarie e promozionali.

3- Altra esclusione: la richiesta di consenso preventivo per quanto riguarda dati contenuti nei curricula

4- Il Registro delle opposizioni vale anche per la posta cartacea (in altre parole, prima di fare mailing pubblicitario, bisogna fare uso del Registro delle Opposizioni, di cui ho già scritto in http://blog.cesaregallotti.it/2011/02/dpr-1782010-privacy-e-diritto-di.html)

5- la comunicazione di dati tra societa', enti o associazioni con societa' controllanti, controllate o collegate, nonchè tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalita' amministrativo contabili, non è più necessario il consenso. Però il fatto deve essere messo nell'informativa.

****

02- Novità sugli standard serie ISO/IEC 27k

Il 15 aprile si è tenuto a Singapore il meeting dell'SC 27 WG 1.

Questi i risultati:
- ISO/IEC 27000 (Vocabolario): sarà prodotto il 3WD (Terzo Working Draft; siamo indietro...)
- ISO/IEC 27001: è in circolazione il 1 CD (Committee Draft, più avanzato del WD);
- ISO/IEC 27002: sarà prodotto il 4 WD (la 27001 avrà ancora l'Annex A, anche se alcuni, tra cui io, volevano lasciare libertà di scelta per il SOA; verranno tolte alcune cose in materia di risk assessment e politiche già presenti sulla 27001)
- ISO/IEC 27005: è stata pubblicata la versione del 2011 che sostitusce quella del 2008 solo per allineare la terminologia alla ISO 31000:2009 (per il resto è rimasta invariata)
- ISO/IEC 27006 (la norma per gli organismi di certificazione) dovrebbe essere pubblicata entro metà 2012
- ISO/IEC 27007 (linee guida per gli audit): è uscito il Final Draft
- ISO/IEC 27008 (verifica dei controlli di sicurezza): dovrebbe essere conclusa
- ISO/IEC 27013 (relazioni tra 27001 e 20000-1): è in circolazione il 1 CD

Non ho ancora letto i draft in circolazione.

Dalla presentazione fatta da Fabio Guasconi per l'Uninfo, segnalo quanto segue:
- Numerosissimi commenti su 27001 e 27002
- la 27015 (sui Financial Services) è ferma in attesa di nuovi input

E' stata fatta una proposta per una norma specifica sul Cloud Computing. Voterò contro perché dovrebbe già essere coperta dalle norme sull'outsourcing (se i "servizi cloud" sono offerti dagli esterni) e dalle altre norme più tecniche (se i servizi cloud sono erogati internamente). Uninfo probabilmente voterà a favore.

L'aggiornamento della 27006 è dovuto soprattutto all'allineamento con la ISO/IEC 17021:2011 e quindi gli editor vorrebbero non avere altri argomenti da discutere. Rimane quindi il grosso problema dei tempi di audit proposti dall'Annex C (Informative) della 27006: attualmente sono esagerati (soprattutto per le PMI). L'allegato è solo informativo e questa è un'altra ragione per cui gli editor non vorrebbero discuterlo; purtroppo Accredia lo considera acriticamente come "normativo" e quindi siamo costretti ad avere audit troppo onerosi per le aziende e anche per gli auditor (che non sanno come giustificare il proprio tempo; per lo meno i molti che conoscono la materia... i tempi sono probabilmente tarati per i pochi che non la conoscono; più ignoranti ma più capaci a far pubblicare le cose).

PS: ringrazio Fabio Guasconi per aver corretto qualche errore di questo articolo. Quelli rimasti sono colpa mia.

****

03- Infrastrutture critiche e Dlgs 61/2011

Simone Tomirotti mi informa della pubblicazione del Dlgs 61/2011 dal titolo "Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessita' di migliorarne la protezione".

E' possibile leggere il Dlgs da www.normattiva.it.
E' possibile leggere la Direttiva da http://eur-lex.europa.eu/it/index.htm

Il Dlgs è interessante, anche se riguarda solo il settore energia e il settore trasporti. In particolare perché tratta compiutamente la sicurezza delle informazioni, stabilisce che il "funzionario di collegamento in materia di sicurezza" è anche il responsabile della sicurezza delle informazioni e, infine, nell'allegato B, illustra i "Requisiti minimi del piano di sicurezza dell'operatore (PSO)" in modo più convincente di quanto prescritto dal Codice Privacy.

Simone Tomirotti aggiunge: "la Regione Lombardia sembra intenzionata ad affrontare l'argomento Infrastrutture Critiche. E questo è già qualcosa. A giugno del 2010 c'era stato un incontro con alcuni gestori di Infrastrutture Critiche. Poiché in questa prima Direttiva la tematica interessa Trasporti ed Energia, all'incontro hanno partecipato società tipo AEM o A2A. A novembre 2011 ci sarà un incontro dal titolo inglese e un po' ambizioso: 1st International Workshop on Regional Critical Infrastructure Protection."

Il sito della protezione civile Regione Lombardia: http://bit.ly/iiDo8T

****

04- I primi dieci anni di applicazione del Decreto 231

Segnalo questo interessante articolo sul Dlgs 231 del 2011:
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2320

****

05- APMG Ente di Accreditamento per la ISO/IEC 20000-1

Tony Coletta mi ha segnalato come APMG sia ora il gestore delle certificazioni aziendali ISO/IEC 20000-1 su incarico di itSMF.

Maggiori informazioni su:
http://www.apmg-international.com/faq2.asp?category=ISO/IEC%2020000%20FAQs

Sarà interessante capire come saranno gestite le relazioni tra certificati aziendali accreditati APMG e quelli accreditati da altri organismi di certificazione quali Accredia (ex Sincert).

****

06- Sul downtime di Aruba

Uno dei casi più discussi di recente è il downtime di Aruba, perché tocca gli argomenti "infrastrutture", "continuità operativa" e "contrattualistica".

Segnalo qualche articolo interessante (dalla newsletter del Clusit):
- il commento di Claudio Telmon: http://blog.clusit.it/sicuramente/2011/05/considerazioni-sulla-vicenda-di-aruba.html
- il commento di Armando Leotta: http://blog.clusit.it/sicuramente/2011/04/aruba-downtime-osservazioni.html
- il commento di Andrea Draghetti: http://www.oversecurity.net/2011/04/30/incendio-nella-server-farm-di-aruba-comunicato-stampa/

PS: ci sarà anche da discutere sul downtime di Poste. Purtroppo non ho avuto il tempo per studiarlo. Vi invito a segnalare articoli in merito.

****

07- Metriche FISMA

Lo statunitense Federal Information Security Management Act (FISMA) richiede alle agenzie governative di rispondere periodicamente a dei questionari del Homeland Security Department sulla sicurezza informatica.

Per il 2011 è in circolazione un questionario di 11 pagine (pare però non ancora ufficiale) che sta riscontrando il favore degli analisti perché cerca di spingere le agenzie verso il "monitoraggio continuo" (senza però specificare cosa si intenda per "continuo").

Lascio ai lettori più pazienti la possibilità di valutare il questionario e l'applicabilità delle metriche alla propria organizzazione.

Un articolo piuttosto completo: http://www.govinfosecurity.com/articles.php?art_id=3707
Un articolo più critico: http://www.nextgov.com/nextgov/ng_20110606_5245.php?oref=topstory
Il questionario: http://www.sans.org/critical-security-controls/fisma.pdf

****

08- Report ENISA su resilienza e metriche

A febbraio, ENISA ha pubblicato il documento "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report" (ho visto la segnalazione sul blog del Clusit).

Ho trovato interessante la scelta delle metriche e il fatto che siano accompagnate dai loro valori "tipici".

La parte introduttiva è un po' troppo scolastica.

Il link:
http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report/at_download/fullReport

****

09- La natura frattale del ciclo PDCA

Da un Twitter della società di consulenza Lambda CT, segnalo questo articolo in inglese: http://is.gd/iTcILz.

La materia non è nuova, ovviamente. Preferisco altri testi dedicati al Kaizen (tra cui quelli editi da Guerini), ma forse questo articolo può essere d'aiuto ai tanti che non osservano con la dovuta attenzione gli argomenti relativi alla "vecchia" qualità.

Mi viene in mente la frase di un mio cliente che mi disse (con ironia e segnalando la criticità): "nella nostra azienda rilasciamo applicazioni e processi e procedure e moduli solo in versione 1".

Nota: il Twitter successivo di Lambda CT (http://is.gd/W7ogQ4) rimanda a un pdf sulle correlazioni tra sicurezza e ISO/IEC 25504, che è un modello decisamente (troppo) oneroso. Ogni volta mi stupisco di come certe cose così complesse e teoriche abbiano tanto successo: direi che probabilmente si tratta di vittorie delle grandi società di consulenza.

****

10- Internet e politica

A inizio maggio avevo segnalato una presentazione di Atle Skjekkeland sulle nuove modalità di comunicazione:
http://blog.cesaregallotti.it/2011/05/omat-e-gestione-elettronica-di.html

Le campagne elettorali sono molto interessanti perché dimostrano pubblicamente come alcuni mezzi sono utilizzati. Questo articolo, seppur dal titolo "di parte" e dal tono ironico, mi sembra equilibrato nell'illustrare come Pisapia abbia utilizzato Internet efficacemente, al contrario della Moratti. E ci dà anche altre indicazioni sull'attenzione da porre nell'uso di questi mezzi:
http://www.02blog.it/post/8170/the-social-letizia-moratti-una-serie-di-sciagure-riassunta-con-cura

****

11- Confindustria Digitale

Segnalo questo articolo di Computerworld Italia sulla nuova confederazione di aziende ICT e ringrazio Aldo Ceccarelli che l'ha pubblicato su LinkedIn:
- http://www.cwi.it/2011/06/13/confindustria-digitale-un-passo-avanti-ma-il-rischio-di-cadere-in-vecchi-errori/

****

12- Un contributo su Business Continuity e Incident Management

Maurizio Nastro mi ha inviato un contributo su Business Continuity e Incident Management (http://blog.cesaregallotti.it/2011/04/business-continuity-e-incident.html). Copio integralmente e segnalo in particolare la seconda parte con l'esempio della barca.

Riguardo la differenza tra Business Continuity (BC) e Disaster Recovery (DR), sulla base della mia esperienza, credo che si possa riassumere concettualemente in questi termini.

Il criterio caratterizzante è rappresentato dalla sopravvivenza di un'azienda.

I piani di BC si preoccupano di mantenere, a seguito di un incidente di Business Disruption, la continuità dei servizi critici di Business almeno ad un livello predefinito considerato accettabile.

[Un incidente di Business Disruption è un evento che può intaccare le attività a supporto di servizi critici minando potenzialmente la sopravvivenza aziendale. Ogni organizzazione deve definire la propria classificazione di incidenti; il confine tra ciò che rappresenta un incidente ordinario e uno di Business Disruption è labile, e fortemente dipendente sia dall'organizzazione che dalla realtà in cui opera. A tal riguardo, prendiamo come esempio una organizzazione che opera nel settore dei trasporti, ed un'altra nel

campo ICT con la maggior parte dei dipendenti che lavora da remoto via internet. E' evidente che un incidente (in questo caso legato ad un evento naturale) rappresentato da improvviso forte maltempo, che determina il formarsi di ghiaccio con conseguente inagibilità delle strade, assumerà contorni e valenza diversi per le due realtà aziendali.]

La BC è trasversale a tutte le tipologie di settori, potendosi applicare sia alle aziende erogatrici di servizi IT h24, sia, ad esempio, alle aziende manufatturiere che utilizzano laminatoi od altoforni, per le quali l'IT non rappresenta il core business.

I piani di Disaster Recovery si preoccupano di di mantenere, a seguito di un incidente (non necessariamente di Business Disruption), la continuità dei servizi erogati tramite l'infrastruttura IT almeno ad un livello predefinito considerato accettabile.

Qualora tali servizi (erogati tramite l'infrastruttura IT) siano anche servizi critici di Business, i piani di DR faranno parte dei piani di BC. Qualora, questo non avvenga, i piani di DR saranno fuori dai piani di BC. A tal riguardo, c'è però da dire che se l'infrastruttura IT non è a supporto di servizi critici, è presumibile che non vi sia neanche l'adozione di una soluzione di DR.

In altre parole, la BC si colloca ad un livello superiore rispetto al Disaster Recovery, che può essere visto come la parte tecnologica della Business Continuity, laddove l'infrastruttura IT copra un ruolo determinante per la sopravvivenza dell'azienda (in quanto a supporto di servizi critici).

Riguardo invece i piani di BC e i piani di Incident Management (IM) credo che un'analogia possa essere utile.

Se si pensa ad una piccola imbarcazione che improvvisamente presenti una falla che causi infiltrazioni d'acqua, il piano di IM, attuato dall'equipaggio, provvederà alle operazioni necessarie per tamponare la falla; il piano di BC è invece attuato dal personale adibito a scaricare fuoribordo l'acqua che entra durante le operazioni di tamponamento, per evitare che l'imbarcazione affondi.

Il piano di BC non è quindi finalizzato alla risoluzione del problema che ha causato l'incidente, ma a garantire la sopravvivenza dell'organizzazione per il tempo necessario a risolverlo.

Da quanto esposto si comprende come i piani di gestione incidenti e di BC siano diversi, ma, nel contempo, strettamente correlati. I responsabili dei due piani (che in realtà aziendali di piccole dimensioni possono anche essere in carico ad un'unica persona) devono mantenersi in stretto contatto al verificarsi di un incidente di Business Disruption. Se ci si accorge che il tempo trascorso nel tentativo di gestire a buon fine l'incidente, sommato a quello necessario per il ripristino dei servizi critici, rischia di diventare maggiore del massimo tempo tollerabile dall'azienda per la sua sopravvivenza, occorre procedere con l'attivazione dei piani di BC [attivarli subito, contestualemente ai piani di IM, non è detto che sia la soluzione migliore; questo perchè l'incidente potrebbe venire risolto per tempo, con conseguente vanificazione dei piani di BC (e costi conseguenti)].

PS di Cesare: giusto ieri mi è arrivata un'altra mail sull'argomento. Non ho avuto tempo di commentarla con il mittente. Quindi, anche questo argomento sarà ripreso nella newsletter di luglio.