****
IT SERVICE MANAGEMENT NEWS - DICEMBRE 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

****
00 - Auguri

Auguro a tutti i lettori delle buone feste e un buon 2012.

****
01- Standizzazione sicurezza - Famiglia ISO/IEC 270xx, ISO 22301 e altro

Famiglia ISO/IEC 270xx

A ottobre si è svolto il meeting del SC27 in Kenya.

Prima dell'elenco, ricordo che gli stati degli standard sono i seguenti (riassumo):
WD -> CD -> DIS -> FDIS -> Pubblicazione

- ISO/IEC 27001: ancora molto immatura: si è rimasti allo stadio di CD (è il secondo)
- la ISO/IEC 27002 è al primo CD
- la ISO/IEC 27007, come già sapete, è stata pubblicata

- ISO/IEC 27006 (per gli Organismi di Certificazione), approvata per pubblicazione; rispetto alla versione precedente, recepisce i soli aggiornamenti richiesti per allinearla alla ISO/IEC 17021:2011; un riesame sistematico partirà a maggio (rimane invariato l'Allegato C con le giornate uomo richiesta per gli audit di certificazione)
- ISO/IEC 27007, estensione della ISO 19011 sull'auditing dei sistemi di gestione, approvata per pubblicazione
- ISO/IEC 27008:2011, sull'audit dei controlli di sicurezza, già pubblicata
- ISO/IEC 27010, supplemento ai controlli della 27002 per lo scambio di informazioni, passata allo stadio di FDIS
- la ISO/IEC 27013 (rapporti ISO/IEC 27001 e ISO/IEC 20000-1) rimane allo stato di DIS
- ISO/IEC 27014, Governance of information security, passata allo stadio di DIS,
- ISO/IEC 27015 sui controlli di sicurezza per i servizi finanziari e assicurativi, è allo stadio di WD e sarà un TR e non un International Standard anche a causa delle perplessità degli inglesi
- la ISO/IEC TR 27016 (Organizational economics) è allo stato di terzo WD
- ISO/IEC 27017 sull'uso dei servizi cloud; approvato l'avvio dei lavori
- la ISO/IEC WD 27033-4 (Securing Communications between networks using security gateways) è al quarto WD
- la ISO/IEC 27034-1 (Application security — Part 1: Overview and concepts) è stata pubblicata
- ISO/IEC 27037 sulla digital forensics, lavori in corso
- ISO/IEC 27043: approvato l'avvio dei lavori per una norma su "Investigation principles and processes"
- avviati i lavori per uno standard sul Air traffic management

Per il passaggio da uno stato all'altro (quando non rimangono allo stesso stato), normalmente, devono passare almeno 6 mesi. Quindi, se calcolo correttamente, la nuova 27001 sarà pubblicata non prima del 2013.

Commenti sul CD della ISO/IEC 27001

Pubblico qui alcuni commenti di Fabio Guasconi, Presidente Commissione SC27, che ha partecipato al meeting SC27 a Nairobi.

- Il risk assessment sarà nel capitolo dedicato alle "Operations" e non al "Planning" perché si distinguono i rischi del sistema di gestione rispetto a quelli operativi
- il SOA non sarà più obbligatorio, dovranno però essere documentate e giustificate le esclusioni rispetto all'Allegato A
- sono state avanzate alcune proposte di modifica rispetto al testo della ISO Guide 83, ma non sono ancora pervenute risposte dal comitato specifico
- il rischio residuale dovrà essere approvato dalla Direzione
- non saranno esplicitati, come input al Riesame della Direzione, i risultati del risk assessment perché si ritiene che il testo attuale già lo richieda

ISO 22301

Al di fuori della famiglia ISO/IEC 270xx, ho avuto notizia che la ISO 22301 (Requisiti per il Business Continuity Management System) è allo stato di FDIS e la pubblicazione è prevista per metà del 2012. La corrispondente Linea Guida, ISO 22313 è prevista per fine 2012. Queste due norme sostituiranno, rispettivamente, la BS 25999-2 e BS 25999-1.

Altri standard di sicurezza

Il 25 novembre, Stefano Ramacciotti ha fatto un'interessante presentazione in Uninfo sui lavori di ottobre del Gruppo di Lavoro WG3 del SC27 di ISO/IEC JTC1.

Questi gli standard trattati dal Gruppo:
- ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008; ISO/IEC 15408-3:2008: si tratta dei Common Criteria e potete scaricarli da http://www.commoncriteriaportal.org/; le versioni attuali saranno riesaminate a partire dal 2013
- ISO/IEC 15292:2001 "ProtecHon Profile registraHon procedures": non è stato oggetto di discussione
- ISO/IEC TR 15443 "A framework for IT Security assurance": sarà rielaborata l'attuale versione del 2005
- ISO/IEC TR 15446:2009 "Guide for the producHon of ProtecHon Profiles and Security Targets": non è stato oggetto di discussione
- ISO/IEC 18045:2008 "Methodology for IT security evaluaHon", il CEM: sarà riesaminata dal 2013
- ISO/IEC 19790:2006 "Security requirements for cryptographic modules", corrispondente del NIST FIPS 140-2: ne è stato avviato il riesame
- ISO/IEC TR 19791:2010 "Security assessment of operaHonal systems": non è stato oggetto di discussione
- ISO/IEC 19792:2009 "Security evaluaHon of biometrics": non è stato oggetto di discussione
- ISO/IEC 21827:2008 "Systems Security Engineering - Capability Maturity Model® (SSE- CMM®)": non è stato oggetto di discussione
- ISO/IEC 24759:2008 "Test requirements for cryptographic modules", corrispondente al NIST DTR per la NIST FIPS 140-2: ne è stato avviato il riesame

Sono inoltre in corso dei progetti sulle seguenti norme:
- ISO/IEC 29147 "Responsible vulnerability disclosure": prevista la pubblicazione nel 2013
- ISO/IEC 29193 "Secure System Engineering Principles and Techniques": prevista la pubblicazione nel 2013

****

02- Standardizzazione - ISO Guide 83 - Common text for management system standards

Come avevo già detto parlando della nuova ISO/IEC 27001, l'ISO sta promuovendo l'uso di un modello comune per tutti gli standard dei sistemi di gestione (ISO 9001, ISO 14001, ISO/IEC 27001, eccetera).

La guida è denominata "ISO Guide 83" e la sua versione finale dovrebbe essere disponibile a febbraio 2012.

Per saperne di più, segnalo l'articolo dell'IRCA:
http://www.irca.org/inform/issue32/DSmith.html?dm_i=4VM,MN6H,HZSOT,1U0IS,1

****

03- Privacy: Limiti (ma non troppi) al telemarketing

Max Cottafavi di Reply mi ha fatto tornare sul comma 4 dell'articolo 130 del Codice Privacy. Il testo recita: "se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, puo' non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni".
Insomma, mi ha fatto notare (l'avevo rimosso dalla mia memoria) come in questo caso viga l'opt-out.
Per il telefono e la posta cartacea, vige quanto previsto dal comma 3-bis (quello sul Diritto di Opposizione che, tra l'altro, alcuni mi hanno segnalato non funzionare correttamente per le numerazioni non comprese nel solo elenco di Telecom Italia... ahinoi).

Il Garante, quasi contemporaneamente, ha segnalato nella sua newsletter un recente Provvedimento di divieto proprio perché una società si è "allargata" il significato del comma (già di per sé discutibile).

Il riassunto del Provvedimento: http://www.garanteprivacy.it/garante/doc.jsp?ID=1852586#1
Il Provvedimento completo: http://www.garanteprivacy.it/garante/doc.jsp?ID=1851415

****

04- Privacy - Corte di Giustizia UE: Opt-in e Diritto di Opposizione

Poco dopo aver visto le due notizie sopra riportate, ho avuto notizia di questa sentenza della Corte di Giustizia UE:
- http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=3487

Arrivo direttamente alla conclusione (cancellando qualche inciso che ne rende la lettura quasi impossibile):
"La Direttiva del Parlamento europeo 95/46/CE osta ad una normativa nazionale che, in assenza del consenso della persona interessata e per autorizzare il trattamento dei suoi dati personali, richiede che i dati in parola figurino in fonti accessibili al pubblico"

Spero di poter tradurre così: il comma 3-bis dell'articolo 130 del Codice Privacy ("il trattamento dei dati su pubblici elenchi, mediante l'impiego del telefono e della posta cartacea per le finalita' di invio di materiale pubblicitario e' consentito nei confronti di chi non abbia esercitato il diritto di opposizione") è contrario a quanto previsto dalla Direttiva Europea e, pertanto, dovrà essere eliminato.

A questa speranza, aggiungo quindi la speranza che qualcuno porti avanti questa richiesta.

****

05- Internet, stampa e controllo dell'editore

Da Interlex riporto questo testo:
Un periodico on line non può essere considerato "stampa". La nuova sentenza della Corte di cassazione (Sentenza n. 44126 del 28.10.2011) conferma i precedenti orientamenti, ma lascia aperte diverse questioni sulla responsabilità di chi immette contenuti on line.
- http://www.mcreporter.info/giurisprudenza/cass11_44126.pdf

Aggiungo che l'evento riguarda un post inserito da un lettore, non un articolo del giornale stesso.

****

06- Nuovo Codice di Autodisciplina per le aziende quotate

A dicembre 2011 è stato pubblicato il nuovo "Codice di Autodisciplina" rivolto a "ogni società italiana con azioni quotate".

Il Codice è focalizzato sui controlli di garanzia contabile e finanziaria. Però, la lettura dell'articolo 7 "Sistema di controllo interno e di gestione dei rischi", può accendere qualche lampadina a chi si occupa di sicurezza delle informazioni (materia collegata ai rischi operativi, trattati dal Codice).

In particolare, il nuovo Codice stabilisce i ruoli e le caratteristiche del consiglio di amministrazione, di una figura di riferimento detta "amministratore incaricato del sistema di controllo interno e di gestione dei rischi", di un comitato controllo e rischi, dell'internal audit.

E' possibile scaricare il Codice da:
- http://www.borsaitaliana.it/borsaitaliana/regolamenti/corporategovernance/corporategovernance.htm
Il link diretto è:
http://www.borsaitaliana.it/borsaitaliana/regolamenti/corporategovernance/codicecorpgov2011clean_pdf.htm

Ho trovato la notizia sulla newsletter di Protiviti, di cui do il link per altri approfondimenti:
- http://hqp-as-prdaut01:95/it-IT/Insights/Newsletters/Insight%20-%20Newsletter-di-Protiviti-Italia/Documents/Newsletter_35%20-%20Dic_2011.pdf

****

07- Virus blocca un ospedale negli USA

Dalla newsletter SANS Newsbyte del 13 dicembe 2011, trovo la notizia di un ospedale bloccato per due giorni causa virus IT. E' una delle tante storie dell'orrore sulla sicurezza delle informazioni e questa mi pare degna di essere segnalata.

Un articolo (in inglese): https://www.ajc.com/news/gwinnett/ambulances-turned-away-as-1255750.html

****

08- Digital Forensics - Video di introduzione e digital profiling

Video digital forensics

Segnalo i primi due video di Marco Mattiucci sulla Digital Forensics.

Molto interessanti:
- Definizioni: http://www.ustream.tv/recorded/18774982
- Digital forensics e digital investigation: http://www.ustream.tv/recorded/18925489

Sulla rete e in letteratura si trovano moltissimi contributi per l'ambito penale. Purtroppo, ho trovato pochissimo per l'ambito civile. Se qualcuno ha segnalazioni, sono le benvenute.

Digital profiling

Segnalo l'articolo "Digital Profiling" di Clara Maria Colombini.

Il Digital Profiling rappresenta uno strumento di indagine informatica mirato all'estrazione di informazioni utili all'identificazione di soggetti, dall'analisi dei dati contenuti nella memoria di un qualsiasi dispositivo digitale.

L'articolo è molto interessante, anche per chi non si occupa di Digital Forensics.

Link: http://www.marcomattiucci.it/CMColombini.art.02.v1.0.pdf

****

09- Standardizzazione - ISO 13053 - Quantitative methods in process improvement - Six Sigma

Il 1 settembre 2011 sono state pubblicate le prime due parti della ISO 13053 "Quantitative methods in process improvement — Six Sigma". In particolare:
- ISO 13053-1:2011: DMAIC methodology
- ISO 13053-2:2011: Tools and techniques

Si tratta, in sostanza, del recepimento da parte dell'ISO della metodologia Six Sigma.

La lettura è interessante, soprattutto del secondo documento, dove sono illustrati brevemente 31 strumenti per la qualità.

Per chi non abbia a disposizione i documenti ISO, segnalo comunque la presenza di molto materiale su Internet. Un buon punto di partenza è Wikipedia:
- italiano: https://it.wikipedia.org/wiki/Sei_Sigma
- inglese: https://en.wikipedia.org/wiki/Six_Sigma

****

10- Standardizzazione - UNI 11200 e UNI EN 15838 del 2010 per i Contact Center

La UNI 11200 e la UNI EN 15838 sono due norme, tra loro collegate, sulla qualità dei Centri di Contatto. In Italia, era stata pubblicata nel 2006 la prima norma in materia (UNI 11200:2006), con la quale era possibile certificare un Centro di Contatto.

A novembre del 2009, il CEN ha pubblicato la norma europea EN 15838 ("Centri di contatto - Requisiti del Servizio"), recepita in Italia come UNI EN 15838:2010 nel luglio del 2010. Sempre a luglio, la UNI ha emesso la norma italiana UNI 11200.

Questa seconda norma (come leggo dal sito dell'UNI www.uni.com) "definisce i parametri di riferimento dei requisiti di servizio fornito dai centri di contatto (come indicati dalle appendici A e B della UNI EN 15838:2010), al fine di garantire una valutazione oggettiva del livello di qualità del servizio medesimo, indipendentemente dal modello organizzativo o dalla tecnologia utilizzati". Forse, potevamo fare a meno di una ulteriore norma nazionale (non ho trovato, leggendo la EN 15838, alcuna richiesta di emissione di ulteriori norme). Forse, alle persone che hanno lavorato sulla UNI 11200:2006 dispiaceva perdere le esperienze maturate.

A parte queste riflessioni, la norma EN 15838 riprende molti concetti della precedente UNI 11200. Soprattutto, a differenza di altre norme, i requisiti sono molto specifici, fino ad elencare gli indicatori (KPI) che un Centro di Contatto deve tenere sotto controllo. La UNI 11200:2010 richiede ulteriori KPI e impone anche le soglie di attenzione ("valori di riferimento").

Aggiungo che queste due norme hanno anche degli approfondimenti sulla sicurezza dei dati dei clienti e delle persone contattate e hanno anche dei requisiti su come deve essere gestito correttamente il rapporto di lavoro con i collaboratori (sappiamo che in Italia la situazione non è sempre buona).

Si raccomanda quindi la lettura della norma a quanti si occupano di Centri di Contatto.
Ringrazio Deborah Monaco di Quint per avermi segnalato l'uscita della UNI 11200:2010.

****

11- Business Continuity - DR delle PA e BSI PAS 200

Linee guida per il DR delle PA

Il 23 novembre 2011, è stata pubblicata la versione definitiva delle "Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni". Questo in ottemperanza a quanto disposto dall'articolo 50-bis del Dlgs 82 del 2005, così come aggiornato nel 2010.

- La pagina della DigitPA: http://www.digitpa.gov.it/altre-attivit/linee-guida-disaster-recovery-delle-pubbliche-amministrazioni
- Il link al documento in pdf: http://www.digitpa.gov.it/sites/default/files/notizie/LINEE%20GUIDA%20PER%20IL%20DISASTER%20RECOVERY%20DELLE%20PA.pdf

Note polemiche:
- non mi sembra ben delineata la differenza tra Business Continuity (Continuità Operativa) e Disaster Recovery; sebbene le definizioni fornite siano corrette, in alcuni punti del documento si rileva un utilizzo non rigoroso di questi termini
- malgrado quanto specificato nella sezione 4.10 dello stesso documento, questo è pubblicato senza data e senza versione
- avrei preferito un documento più schematico.

A parte queste piccolezze, ho trovato interessante la lettura del documento e ho individuato alcuni interessanti spunti.

Altri elementi di interesse:
- insieme alle Linee Guida, è possibile scaricare dalla pagina della DigitPA anche anche un "tool di autovalutazione" (lo chiamerei "tool per una BIA in ambito non-profit")
- l'appendice D, con le caratteristiche di un sito di DR (certamente da estendere anche al sito primario)
- il capitolo 8 sulle Infrastrutture Critiche (anche se i riferimenti bibliografici non sono disponibili)
- i capitoli 2 e 5 con i riferimenti giuridici

Ringrazio Franco Guidi per la segnalazione della pubblicazione delle Linee Guida.

BSI PAS 200 sul Crisis Management

Il BSI segnala la pubblicazione della PAS 200 sul Crisis Management.
Questa è una materia molto importante quando si parla di di gestione degli incidenti e di Business Continuity.

Ovviamente, il suo ambito non è solo ristretto a questi due processi, ma può riguardare ogni genere di evento "critico" per un'azienda (e non solo; penso a Zapatero che ha vinto le elezioni 7 anni fa perché Aznar non ha saputo gestire una crisi e le ha perse pochi giorni fa perché a sua volta non è riuscito a gestire un'altra crisi, anche se diversa).

Attualità a parte, il documento costa 100 sterline e potete trovarlo al link sottostante.
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030252035&utm_source=QUALL-NA&utm_medium=et_mail&utm_content=2497212&utm_campaign=QUALL-NA_24_November_2011&utm_term=PAS+200

Per i più parsimoniosi, l'indice può già essere d'aiuto.

****

12- Standardizzazione - ISO 19011:2011 sulla conduzione degli audit

Per primo, Attilio Rampazzo mi ha segnalato la pubblicazione, in data 15 novembre 2011, della ISO 19011:2011 dal titolo "Guidelines for auditing management systems".

La precedente versione era del 2002 e riguardava solo i sistemi di gestione per la qualità e per l'ambiente (ISO 9001 e ISO 14001). Oggi la norma è estesa a tutti i sistemi di gestione (inclusi quindi quelli per la sicurezza delle informazioni e per i servizi IT). Per alcuni schemi, sono state emesse norme specifiche per la conduzione degli audit e bisognerà fare riferimento a tutte e due le norme (ricordo che è stata pubblicata la ISO/IEC 27007 "Guidelines for information security management systems auditing", già allineata con la nuova versione della ISO 19011).

La nuova vesione è molto allineata con la precedente. Ho notato l'aggiunta di considerazioni in merito ai rischi di audit e alla sicurezza delle informazioni trattate durante le verifiche. Ci sono anche molti altri dettagli ulteriori rispetto alla precedente edizione e suggerisco quindi la lettura di questo standard a quanti devono condurre audit.

L'IRCA ha emesso un commento ad agosto, basato sulla bozza finale:
http://www.irca.org/downloads/ISO%20FDIS%2019011%202011%20Briefing%20Note.pdf

****

13- Errata Corrige - DPS: nessun addio

Daniela Quetti e Vito Losacco mi hanno segnalato il fatto che il Patto di Stabilità 2012 non riporta l'eliminazione dell'obbligo del DPS. La notizia data in precedenza è quindi non più attuale
http://blog.cesaregallotti.it/2011/10/dps-addio.html

Il DPS rimane quindi un obbligo normativo (tranne le semplificazioni già introdotte nel 2008. Questo per la gioia dei pochi che lo ritengono utile, dei tanti consulenti che ci guadagnano soldi e di quanti hanno ancora qualcosa di cui lamentarsi (l'innocente DPS, mentre possono evitare di affrontare punti più complessi della normativa in vigore).

Vito Lo Sacco mi ha anche segnalato il seguente articolo:
http://www.federprivacy.it/index.php?option=com_content&view=article&id=423:dps-nulla-e-cambiato-gli-obblighi-rimangono-le-sanzioni-anche&catid=4:il-punto-di-vista&Itemid=9

****

14- Miei prossimi interventi (24 gennaio sulla sicurezza del Cloud Computing)

Il 24 gennaio, a Milano, in occasione di un evento organizzato da Assintel e il Cloud Security Alliance parlerò di sicurezza e cloud computing. L'evento sarà libero e gratuito e spero che molti dei miei lettori abbiano l'opportunità di partecipare.

Maggiori dettagli il mese prossimo.