Cesare Gallotti

From: it_service_management-news-bounces@mailman.cesaregallotti.it on behalf of IT Service Management NewsLetter [it_service_management-news@mailman.cesaregallotti.it]
Sent: Monday, 15 December, 2008 18:49
To: Mailing list
Subject: [IT Service Management] Newsletter del 15 dicembre 2008
Attachments: ATT189473.txt

****
IT SERVICE MANGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile diffonderla a chiunque; è possibile iscriversi, disiscriversi e modificare le proprie opzioni, oltre a vedere l'informativa sul trattamento dei dati personali, all'indirizzo
http://mailman.ipnext.it/mailman/listinfo/it_service_management-news

****
Indice

****
0- Auguri

Auguri di buone feste a tutti.
Cesare

****
1- ISO/IEC 27031 - Business Continuity

Mi hanno segnalato (Paola Generali, Getsolution) la ISO/IEC 27031. Ho visto anche interventi che la mitizzavano come "recepimento della BS 25999 da parte della ISO).

Fabio Guasconi, che segue i lavori dell'UNINFO, mi ha risposto che "la 27031 (Guidelines for ICT readiness for business continuity) è attualmente allo stadio di 2nd Working Draft e in mano al WG4 del SC27".

Dal sito della ISO (www.iso.ch), la ricerca per "27031" non dà alcun risultato.

Dal titolo del documento in elaborazione ricavo le seguenti informazioni:
1- si tratta di "guidelines" e non di "requirements", quindi non si tratterà di uno standard "certificabile"
2- è focalizzato sull'ICT e non sulla business continuity, a differenza della BS 25999

Sono dell'idea che su questa materia si stiano spendendo troppi "standard" e troppi bit.

****

2- Siti web: informativa privacy e Partita IVA

Il Garante informa su recenti sanzionamenti per informative incomplete sui siti web che raccolgono dati personali.

In particolare, segnala di aver sanzionato un'azienda perché non aveva considerato come dati personali le e-mail e i recapiti telefonici.

L'azienda ha fatto ricorso

Mi permetto due commenti:
- un'azienda che fa ricorso perché in disaccordo con l'interpretare come dati personali le e-mail e numeri di telefono o ha una sensibilità da elefanti non più in linea con i tempi, o i suoi avvocati hanno la pretesa di essere così intelligenti (cioè, stupidi) per poter convincere il Garante di ciò?
- mi è capitato troppe volte di vedere analisi del rischio che considerano come informazioni le configurazioni dei sistemi o i manuali di installazione e poi tra gli asset non trovo i "dati dei clienti" o i "dati aziendali"; forse questo non è un esempio di stupidità, è solo un sintomo della deriva che sta prendendo la sicurezza delle informazioni, di come si stia guardando il dito e non la luna.

Ricordo inoltre che sui siti web aziendali deve essere riportata la Partita IVA dell'azienda.

Spero che il mio sito sia a posto...

****

3- Sicurezza - Attacchi
(da SANS Newsbyte)

In 3 ospedali londinesi, il virus Mytob ha bloccato i sistemi informatici per più di 3 giorni. Se state conducendo delle risk analysis, questo è sicuramente un esempio di "caso peggiore".

http://www.theregister.co.uk/2008/11/19/hospital_computer_virus_shutdown_update/
http://software.silicon.com/malware/0,3800003100,39348158,00.htm?r=8

****

4- Giusrisprudenza - Firma digitale

Vi segnalo questo articolo di filodiritto sulla giurisprudenza in tema di firma digitale
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1092

****

5- Sicurezza - documenti interessanti

Da Cryptogram di novembre, ho trovato un link ad una guida dell'ANSI per la sicurezza informatica orientata al personale amministrativo-legale.
http://webstore.ansi.org/cybersecurity.aspx

In questa pagina, poi, sono disponibili altri link ad altri document interessanti come questo Information Security Management Maturity Model (ISM3)
http://www.ism3.com/index.php?option=com_docman&task=doc_download&gid=4&Itemid=9

Il NIST (ente USA che ha il mandato, tra gli altri, di emettere linee guida sulla sicurezza per le agenzie governative), segnala l'emissione della SP 800-64 Revision 2 "Security Considerations in the System Development Life Cycle" e della SP 800-66 Revision 1 "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule".

Le linee guida del NIST sono molto interessanti sia per chi vuole iniziare a conoscere un argomento (cosa sono le HIPAA?) sia per chi vuole approfondirlo.

Le trovate su http://csrc.nist.gov/publications/PubsSPs.html

****

6- Gli atti della conferenza ITSMF

Disponibili gli Atti della Quinta Conferenza Annuale dell'ITSMF, dal titolo "Making IT - I servizi IT: risorsa strategica per lo sviluppo", tenuta a Milano il 12 Novembre 2008.
http://www.itsmf.it/index.php?method=zoom_conferenze&id=114

****

7- Microsoft Operation Framework (MOF)

Il Microsoft Operation Framework potrebbe essere presentato come una traduzione di ITIL da parte della Microsoft, con una maggiore focalizzazione agli aspetti pratici. La Microsoft, però, non parla di "service management" e di "service lifecycle" ma di "IT practices and activities" e "IT lifecycle".

La versione 4.0 del 2008 del MOF, notevolmente modificata rispetto alla precedente, è disponibile gratuitamente all'indirizzo
http://technet.microsoft.com/en-us/library/cc506049.aspx

La Exin mi segnala che è stato elaborato uno schema di certificazione delle competenze in ambito MOF
http://www.exin.org/content/news/new-microsoft-operations-framework-foundation-exam.aspx

****

8- Errata Corrige

Andrea Praitano di Business-e SpA mi segnala che la EXIN gestisce le certificazioni PRINCE2 solo per il mercato olandese, mentre a livello mondiale le gestisce APMG.

Inoltre, nella segnalazione del mese scorso, mi sono accorto di aver lasciato intendere che la proposta Exin è la sola non rivolta a Lead Auditor in materia di norme della serie ISO/IEC 27000. Questo non è vero, ma la segnalo comunque perché mi sembra una buona iniziativa.

****

9- ISO 9001:2008

Due link ulteriori dell'IRCA (in italiano e in inglese) sulle differenze tra la ISO 9001:2000 e la ISO 9001:2008.

Non ne darò più: le modifiche sono così insignificanti che ho già speso abbastanza bit per segnalarle.

http://www.irca.org/downloads/IRCA633.pdf
http://www.irca.org/downloads/IRCA633IT.pdf

****

10- CNIPA - “Analisi di Fattibilità per l'acquisizione delle forniture ICT”
(dalla newsletter dell'AIEA)

CNIPA annuncia la pubblicazione della versione definitiva delle Linee Guida “Analisi di Fattibilità per l'acquisizione delle forniture ICT”.
http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Qualit%c3%a0_delle_forniture_ICT/Manuali/

Questo è l'ottavo manuale CNIPA. Segnalo anche gli altri, focalizzati sul ciclo di vita delle forniture ICT: strategie di acquisizione, modelli organizzativi, studio di fattibilità, stipula del contratto, governo e valutazione del contratto. Utili come spunto anche per il settore privato.

****

11- Inglese giuridico, diritto delle obbligazioni e dei contratti
(Da Filodiritto)

Vi segnalo questi articoli della Dott.ssa Serena de Palma sull'inglese giuridico.

http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1107
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1078

****

Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italy)
+39.02.58.10.04.21 (Office)
+39.349.669.77.23 (Mobile)
www.cesaregallotti.it
cesaregallotti@cesaregallotti.it