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: Tuesday, 28 October, 2008 16:27

To: it_service_management-news@mailman.cesaregallotti.it

Subject: [IT Service Management] Newsletter "beta" del 27 ottobre 2008

Categories: Studio

Attachments: ATT00028.txt

****

IT SERVICE MANGEMENT NEWS

****

Indice

****

0- Presentazione

Buongiorno,
ringrazio tutti per questa partecipazione alla newsletter "beta".

Per chi non avesse partecipato alla "alfa": ho migrato da yahoogroup al servizio gestito tecnicamente da www.IPNext.it (scusate, ma un minimo di pubblicità bisogna farla, sennò dovevo pagare) perché gli antispam bloccano yahoogroups, dovrei essere riuscito ad attivare la funzione di archvio delle mail mandate e questa potrebbe essere consultata da http://mailman.ipnext.it/mailman/listinfo/it_service_management-news.

Per la prossima volta dovrei inserire l'informativa Privacy sulla pagina della newsletter, dovrei integrarla nel mio sito che metterò in manutenzione e dovrei migliorare questa stessa mail inserendo alla fine le istruzioni per gestire la propria iscrizione a questa newsletter.

Per intanto mi scuso per il ritardo con cui vi ho inviato questa mail, visto che oggi e lunedì 27 e non venerdì 24. Per maggiori dettagli, vedete l'ultimo articoletto di questa mail. Dal prossimo mese dovrei riuscire ad inviare il tutto intorno al 15 del mese.

Vi ricordo che potete collaborare a questa newsletter. Ogni contributo sarà opportunamente accreditato.

Cesare

****

1- Standard: novità ISO 20000-1

La ISO 20000-1 è in fase di revisione e ha recentemente cambiato stato: dal 17 ottobre è un "Commitee Draft". Ci vorrà ancora diverso tempo prima che venga pubblicata.

Sono ancora in corso molte discussioni per migliorare lo standard. La versione precedente, come noto, presentava molte ambiguità e incoerenze. Allo stato attuale lo standard presenta la stessa impostazione di quello pubblicato nel 2005, anche se migliorato nella terminologia nell'intento di togliere le incoerenze precedenti. Non sembra però che ci sia il necessario consenso per esplicitare meglio il processo di

progettazione del servizio e dei processi che lo sostengono.

Lo standard rimange ancora molto legato al concetto di "gestione dell'infrastruttura", senza uno sviluppo completo e coerente del ciclo di Deming.

****

2- Standard: novità ISO 9001

Come molti sanno, nel 2008 dovrebbe uscire la nuova versione della ISO 9001 "Sistemi di Gestione per la Qualità". Dal 9 ottobre è in stato di "in fase di pubblicazione" e dovrebbe pertanto essere pubblicata a breve.

La nuova versione non presenta alcuna novità rilevante. Rispetto alla precedente ISO 9001:2000 sono state aggiunte note di chiarimento e alcuni paragrafi sono stati revisionati perché presentavano alcune disomogeneità rispetto ad altri.

Dopo le preoccupazioni iniziali per una norma molto diversa dalla precedente (come già successo dalla versione del 1994 a quella del 2000), si vede che non c'è nulla da temere.

Rimangono delle perplessità, leggendo le note: se è stato necessario specificare che per ciascuna procedura obbligatoria non è obbligatorio prevedere uno e un solo documento, vorrà dire che qualcuno l'ha interpretata in questo modo. E questo può gettare luce sul perché alcuni vedono la ISO 9001 come norma "burocratica" e "inutile".

Va invece detto che, se ben applicata, la ISO 9001 è un'ottimo strumento di gestione basato sul ciclo di Deming plan-do-check-act e che specifica i punti di controlli minimi per garantire una qualità costante e corrispondente ai requisiti del cliente.

Maggiori novità sono da prevedere per la ISO 9004 "Managing for the sustained success of an organization -- A quality management approach", che sarà dedicata alla sostenibilità di un'organizzazione. Essendo una linea guida, non sarà certificabile, ma sicuramente una buona lettura. Dal 31 luglio è però ancora in versione "Draft", che prevede la votazione finale, prima del passaggio alla versione FDIS, entro il 31 dicembre. Per questa norma, pertanto, bisognerà prevedere la pubblicazione non prima del 2009.

Un altro articolo in merito, lo trovate su: http://www.irca.org/inform/issue19/CCoxJHele.html

****

3- Standard: gli standard di business continuity e IT Service continuity

Come promesso, mi sono letto:
- ISO/IEC 24762:2008 "Guidelines for information and communications technology disaster recovery services"
- BS 25999-1:2006 e BS 25999-2:2007 "Business continuity management".
- BS 25777 "Code of practice for information and communications technology continuity"
- NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems"

Lo standard dell'ISO è risultato pragmatico, con diversi esempi, senza però indicazioni su come condurre una Business Impact Analysis.

La BS 25999 è più orientata alla parte gestionale, ossia su come gestire il ciclo Plan-Do-Check-Act o, come indicato dal documento, un "Business Continuity Programme". Non mi è sembrato che possa essere di aiuto a chi voglia sviluppare e gestire un Business Continuity Plan. Mancano esempi o riferimenti per poter approfondire le possibili metodologie da adottare per la messa in opera. Va comunque notato che la parte 2 dello standard presenta le "specifiche"; è quindi uno standard sviluppato più che altro come base per uno schema di certificazione.

La BS 25777 mi è sembrata molto molto molto inutile. E' ancora meno ricca di esempi della BS 25999. In effetti, basterebbe applicare la BS 25999 per un business di "information and communications technology" ed ecco applicata anche la BS 25777.

La linea guida del NIST è quanto di più utile (e gratuito) per chi volesse avere esempi su come sviluppare e gestire una BIA e un Business Continuity Plan.

Un ulteriore articolo che indica altri standard, lo trovate su
http://www.irca.org/inform/issue19/ATomkinson.html

****

4- Normativa: sentenza della Cassazione sull'accesso abusivo a sistema informatico
(dal Numero 278 del 6 ottobre 2008 della newsletter di www.filodiritto.it)

Commette il reato di accesso abusivo ad un sistema informatico o telematico (articolo 615 ter Codice Penale) l'associato di associazione professionale che quand'anche parte di detta associazione si introduca nel sistema informatico dell'associazione ed effettui copia dell'elenco clienti allo scopo di sviare la clientela verso una nuova realtà professionale in via di costituzione.

Lo ha stabilito la Cassazione con una pronuncia nella quale ripercorre le teorie dottrinarie e la giurisprudenza in merito all'articolo 615 ter Codice Penale nella vecchia formulazione precedente alle novità introdotte dalla Legge 18 marzo 2008, n.48 di Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno. Tuttavia è bene precisare che la pronuncia mantiene il proprio rilievo anche con riferimento alla nuova formulazione della norma.

http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1218

Una mia nota. Ottima sentenza, di cui trovo interessante il passaggio: "il dato rilevante non sarebbe tanto la introduzione quanto la permanenza nel sistema informatico al fine di estrarne copia dei dati per fini estranei alla associazione". In altre parole: anche se si hanno i diritti "informatici" di accesso ad un sistema, è comunque necessario che le finalità perseguite siano in linea con le volontà di chi del sistema legittimamente dispone.

****

5- Normativa: privacy e tessere di riconoscimento
(da www.filodiritto.it)

Il Ministero del Lavoro ha risposto all'istanza di interpello formulata dall'ANIE - Federazione Nazionale Imprese Elettrotecniche ed Elettroniche, in merito ai dati da pubblicare nelle tessere di riconoscimento ed in particolare "se rispetto all'esigenza che i dati riportati su detta tessera consentano l'identificazione del lavoratore l'indicazione della data di nascita non risulti sproporzionata e possa, pertanto, essere omessa, risultando sufficiente l'indicazione degli altri elementi indicati dalla circolare n. 29/2006 (fotografia, nome e cognome del lavoratore, nome o ragione sociale del datore di lavoro)".

http://www.filodiritto.com/index.php?azione=archivionews&idnotizia=1562

Una nota: questa vicenda è interessante perché presenta come neanche il legislatore si ricordi sempre della legge sulla Privacy.

Ci ricorda inoltre come le misure di sicurezza debbano essere sempre proporzionate alla realtà e mai eccessive. In questo caso la sproporzione non ha arrecato inefficienze specifiche, ma troppe volte l'effetto è che si viene a creare un sistema inefficiente che, in breve tempo, diventa anche inefficace.

****

6- Computer forensics
Segnalo la buona lettura "SANS Top 7 New IR/Forensic Trends In 2008". L'articolo riassume le considerazioni fatte nel corso del Forensic Summit organizzato dal SANS institute
http://forensics.sans.org/community/top7_forensic_trends.php

Per chi volesse avvicinarsi alla materia, il SANS propone anche diversi white papers
http://forensics.sans.org/community/whitepapers.php

****

7- Sicurezza: un esempio da ricordare

Molte volte sento e vedo aziende che non si curano di gestire le password di amministrazione dei propri sistemi informatici in modo che ciascun amministratore possa utilizzare solo delle utenze personali (per quanto di amministrazione).

In molti casi viene detto che si ha fiducia nel proprio personale, in altri casi vengono presentati problemi tecnici "insormontabili". La verità è che il rischio non viene percepito come tale.

Un esempio, viene dato da Terry Childs, un amministratore di sistema di una società che gestisce la rete IT di San Francisco. Childs, a seguito di un'azione disciplinare, ha modificato tutte le password di amministrazione dei sistemi, impedendo l'accesso a tutti gli altri.

Childs è stato arrestato e verrà probabilmente condannato. L'azienda ha previsto una spesa straordinaria di oltre 1 milione di dollari per manutenzione.

Un buon esempio per ricordare che anche le password di amministrazione vanno gestite considerando la sicurezza.

http://www.theregister.co.uk/2008/09/10/rogue_sf_sysadmin_may_cost_sf_1m/print.html
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114479&source=rss_topic17

****

8- Un articolo sulla gestione della crisi

Dalla newsletter del Clusit, viene segnalato un articolo sulla gestione della crisi che ricorda che quando si hanno incidenti, non bastano le misure tecnologiche per una loro chiusura efficace. Anche i processi gestionali e di comunicazione (verso l'interno e verso l'esterno di un'organizzazione) sono fondamentali per garantire il completo recupero con il minimo di impatti consequenziali.

L'articolo presenta un caso positivo di gestione di una crisi presso BestWestern.
http://blog.quintarelli.it/blog/2008/08/best-western-e.html

****

9- Business continuity: un piccolo esempio negativo (e personale)

Avendo deciso di fare il libero professionista, ho dovuto adeguare i miei sistemi informatici a tale realtà. Tra le altre cose, ho quindi chiamato Telecom per modificare il mio contratto ADSL da "tariffa a consumo" a "tariffa flat".

Venerdì, senza avvisarmi, Telecom ha quindi staccato la mia linea ADSL per le necessarie manutenzioni.
Per questa ragione io non sono riuscito ad inviarvi questa e-mail.

Qualche lezione:

1- pur avendo un Business Continuity Plan (modem PSTN a 56k) non l'ho avviato. I piani non vanno solo fatti, vanno anche avviati quando necessario. In questo caso la pigrizia del venerdì sera e l'arrabbiatura hanno giocato un ruolo frenante. Inoltre, non sono riuscito a trovare i cavi per la connessione: avrei dovuto testare periodicamente il piano!

Se questa situazione può far sorridere perché si tratta di una singola persona, viene però naturale pensare che in un'azienda è ancora più necessario testare i piani: il coordinamento di più persone è sempre più oneroso e le possibili perdite economiche maggiori.

2- Telecom non mi ha avvisato, dimostrando una grande mancanza di "orientamento al cliente". Ecco quindi che una delle lezioni di IT Service Management non è stata applicata: avvisare sempre gli utenti e mantenere un contatto costante con loro.

3- alla fine, chi ha fatto una brutta figura sono solo e soltanto io. Anche se Telecom ci ha messo lo zampino. Questo ricorda un'altra lezione fondamentale: la responsabilità finale rimane sempre in capo all'organizzazione che offre il servizio; l'uso di outsourcer e fornitori esterni non può toglierle tale responsabilità.

_____

Cesare Gallotti
Quint Wellington Redwood Group
Via Vincenzo Monti 8
20123 Milano (Italy)
http://www.quintgroup.com
+39.02.46.71.25.32 (Office)
+39.02.48.01.32.33 (Fax)
+39.349.669.77.23 (Mobile)
c.gallotti@quintgroup.com