****
IT SERVICE MANAGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque secondo la licenza http://creativecommons.org/licenses/by-nc/2.5/it/

E' possibile iscriversi o disiscriversi
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/newsletter.htm.
Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Business Continuity

NFPA 1600

Segnalo, dal sito del Disaster Recovery Institute Italy, lo standard "NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs - 2010 Edition".

La NFPA è la National Fire Protection Association (USA) e lo standard è di tipo generale, non occupandosi dei soli rischi di incendio.

Degno di nota è l'allegato A in cui sono approfonditi i requisiti (come se avessero fatto la BS 25999-1 e 25999-2 in un solo documento).

Si può scaricare dal sito del DRI (http://www.dri-italy.com/public/NFPA16002010.pdf) o direttamente da quello della NFPA (http://www.nfpa.org/assets/files//PDF/NFPA16002010.pdf)

NIST SP 800-34

Il NIST ha pubblicato la revisione 1 della "Contingency Planning Guide for Federal Information Systems".
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf

Ritengo che le guide del NIST siano tra le migliori fonti di informazione sulla sicurezza delle informazioni: rigorose dal punto di vista teorico, pragmatiche e con poco fuffaware (in linea con la migliore tradizione USA).

Notizie

Dal SANS Newsbyte segnalo quanto riportato dalla survey 2010 della Symantec "State of the Data Center Report": 1/3 delle aziende di media dimensione non hanno riesaminato il proprio Disaster Recovery Plan nell'ultimo anno e 1/3 asserisce che il proprio DRP è "insufficiente". Faccio notare che questi sono risultati ottenuti da interviste: sempre più ottimistici delle realtà (infatti, anche a fronte di quanto sopra esposto, l'80% degli intervistati ha comunque fiducia nel proprio DRP!)
http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sdcreport2010

****

02- ROSI
(da Mauro Cicognini)

A seguito della mia segnalazione del mese scorso sul lavoro "Return On Security Investment: un approccio pratico" reperibile da http://rosi.clusit.it, il co-autore Mauro Cicognini mi ha inviato una risposta che copio e incollo.

Ciao Cesare,

ti ringrazio per la recensione del nostro lavoro sul ROSI, che, vista la fatica che ci ha richiesto, considero già un traguardo raggiunto nonostante le numerose manchevolezze che sono ben note anche a noi stessi del gruppo di lavoro.

In particolare, mi permetto di renderti noto che il gruppo di lavoro sta proseguendo il suo impegno, cercando di produrre una versione 2.0 (od anche solo 1.1 ;) entro l'estate, arricchendola soprattutto là dove fin dall'inizio si è previsto che il lavoro potesse e dovesse essere "espanso" ovvero nella sezione di Case Study ed aggiungendo alcuni Pattern.

Temo poi che non siamo stati sufficientemente chiari durante la presentazione: il metodo "classico" del risk management è assolutamente cardinale nel lavoro di costruzione di un ROSI, perlomeno nell'approccio che abbiamo chiamato "Top-Down". Forse non è sufficientemente evidente, e senz'altro non è abbastanza formalizzato (ne stiamo cercando di scrivere la WBS proprio in questi giorni), ma ti assicuro che c'è ed anzi buona parte delle tabelle (quelle che trovi scaricabili dal sito) servono proprio a quello.

Abbiamo però aggiunto a questo metodo, che è tipicamente deduttivo - e, proprio per questo, poco congeniale ad una parte non trascurabile di persone - un secondo approccio, assolutamente induttivo, che se vogliamo potremmo definire come "Bottom-Up", e che nel testo trovi chiamato "Verify".

In questo secondo metodo si parte presentando un caso concreto, nel quale, con un po' di fortuna e fatti i debiti aggiustamenti, è ragionevole pensare che qualcuno si possa identificare, perché riconosce in parte la sua situazione, ritrova dei temi di cui qualcuno gli ha già parlato, intravede delle soluzioni che gli sembra di aver capito. In questo modo gli si fornisce una griglia da riempire per verificare queste sue intuizioni, griglia che lo favorisce nella sistemazione analitica di un insieme di conoscenze che verosimilmente già possiede ma che fa fatica ad incasellare, e lo guida (speriamo) nel raccogliere i dati rilevanti per costruire e presentare il suo business case a chi di dovere.

****

03- Libro "Manuale di sicurezza aziendale"

Giulio Carducci e Alberto Berretti, "Manuale di sicurezza aziendale", bit.book editore, 2010, Roma

Questo libro può essere considerato l'aggiornamento del precedente "La tutela dei dati nelle aziende e nelle istituzioni" edito da FrancoAngeli nel 2003 (http://www.ibs.it/code/9788846446862/carducci-giulio/tutela-dei-dati-nelle.html).

Infatti, ne mantiene l'impostazione: introduce la sicurezza delle informazioni (motivazioni, norme legali, standard), descrive cos'è una metodologia di risk assessment e in particolare presenta Migra (l'evoluzione della precedente Defender), elenca e approfondisce le misure da prevedere per la sicurezza delle informazioni. Il capitolo finale ha il titolo programmatico di "Prospettive e futuro".

Mi è parso molto ben fatto. Ovviamente, non posso fare a meno di leggere un libro sulla sicurezza delle informazioni senza pensare a qualche critica o a qualcosa che farei in modo diverso (per esempio, avrei dato più spazio agli standard della serie ISO/IEC 27001 e meno a quelli sulla certificazione della sicurezza dei prodotti e dei sistemi).

Ma si tratta di sciocchezze. Quello che veramente importa è che in questo libro trovate idee e opinioni (a differenza di tanti libri e articoli che presentano i "soliti" modelli copiandoseli l'un l'altro).

Ne consiglio quindi la lettura, anche (e non solo) per raccogliere il punto di vista di 2 consulenti della sicurezza delle informazioni e per aggiornarsi sulle misure di sicurezza oggi disponibili sul mercato.

Il libro è reperibile da www.bitbook.it

Nota: Giulio Carducci è stato il mio primo Amministratore Delegato, è stato il primo (insieme a Maurizio Bedarida) a darmi fiducia e ad offrirmi un posto di lavoro presso Securteam. Il mio debito di riconoscenza è molto alto, ma non ha influito su questo giudizio.

****

04- Sicurezza ISP

Da SANS NewsBites Vol. 12 Num. 45, segnalo la pubblicazione del Cyber Security Code per gli ISPs Australiani.

Il documento segnala alcune pratiche che gli ISPs dovrebbero seguire per rilevare computer infetti e agire di conseguenza.

L'iniziativa è interessante e mi ha fatto pensare alle molte aziende in cui i fornitori possono connettersi ai servizi interni (file server, console di configurazione, eccetera) senza che ne siano verificati i pc (in compenso nessuno mette a disposizione una connessione solo web per i consulenti!). Prendessero iniziative minimali, come quelle previste da questo codice, sarebbe sicuramente meglio.

http://iia.net.au/images/resources/pdf/icode-v1.pdf

****

05- Novità ISACA (Monitoring Controls; Implementing IT Governance

Monitoring of Internal Controls and IT

Il 25 marzo è stato pubblicato il draft del documento dedicato al monitoraggio dei controlli IT.

Ci sono diverse buone idee, riprese dalla qualità in merito alla misurazione dei processi.

www.isaca.org/itmonitoring

Implementing and Continually Improving IT Governance

Il framework "Implementing and Continually Improving IT Governance" è composto di files Word, Excel e PowerPoint utili ad implementare l'IT Governance in un'impresa.

Il download è per i soli soci ISACA
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-and-Continually-Improving-IT-Governance1.aspx

****

06- Computer Forensics

Pasquale Stirparo segnala (via Associazione Digital Forensics Alumni, www.perfezionisti.it) il blog dedicato al Windows Forensics Environment (la distribuzione forense di Windows).

http://winfe.tk/

****

07- Assessment

Da ITSM News segnalo l'interessante articolo "Quality ITSM Assessments".
(http://itsmadviser.com/portal/index.php?option=com_wrapper&view=wrapper&Itemid=4)

Tratta su come fare dei buoni assessment considerando i servizi, i processi organizzativi e i tool utilizzati. Fa notare anche le possibili difficoltà causate dagli obiettivi dello sponsor, quando questi spingono verso "certi" risultati.

Condurre un assessment non è facile, anche perché le persone coinvolte non danno molta disponibilità, spesso perché impegnate in "cose più importanti". La soluzione più facile, seguita da molti, è fare gli assessment attraverso "interviste in sala riunioni".

Inoltre, chiunque sia l'assessor e chiunque sia lo sponsor, c'è sempre un pelo di diffidenza nei confronti di coloro che fanno domande e quindi "fare le interviste ai tecnici presso le loro postazioni" (il metodo più efficace per raccogliere informazioni) è sempre molto difficile se il consulente non è ancora introdotto completamente nell'azienda.

****

08- KISSS

Segnalo l'articolo (su segnalazione di ITSM News) "CRM Success Sealed with a KISSS". (http://www.cio.com/article/595409/CRM_Success_Sealed_with_a_KISSS?taxonomyId=3000)

E' una analisi su come i progetti di CRM (io aggiungerei anche gli ERP) siano quasi sempre condotti secondo la logica "tutto e subito" per poi scoprire che il "subito" è "tra diversi mesi" e "tutto" è "una serie di funzionalità complesse, di scarsa usabilità e spesso non coerenti con le aspettative".

L'aritcolo quindi ricorda la bontà del principio "KISS" (fallo semplice e stupido) e ne propone l'evoluzione KISSS ("fallo piccolo, semplice e modulare").

****

09- IT Governance e CIO

Sempre da ITSM News segnalo l'articolo "CIOs Running IT Governance: A Lose-Lose Scenario" (http://advice.cio.com/thomas_wailgum/10488/cios_running_it_governance_a_lose_lose_scenario?source=rss_Blogs_and_Discussion_Enterprise_Software_Unplugged)

Tratta del fatto che l'IT dovrebbe essere governato (nel senso di "governance" non di "gestito") da tutta la Direzione, non solo dal responsabile IT. L'articolo è impostato secondo la logica del "è ovvio, perché parlarne?".

Io dico: è ovvio, ma bisognerebbe avere dei dirigenti formati in un certo modo. In caso contrario o fanno dei danni (senza tirare in ballo le vignette di Dillbert sui dirigenti, sappiamo tutti come le persone con minime competenze informatiche dicono troppo spesso che i progetti IT sono "semplici") o subiscono la governance del CIO.

In definitiva, è mio parere che per avere una IT Governance efficace e condivisa tra i dirigenti di un'impresa, sono necessari investimenti in tempo e denaro per la formazione (dei dirigenti, non dei loro sottoposti!).

_____

Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italy)
Web: http://www.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it