****
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' 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- Breve editoriale (nuovo sito) e auguri
02- Standardizzazione famiglia ISO/IEC 27000 (27001, 27002, 27031)
03- Standardizzazione famiglia ISO/IEC 20000 (20000-1, 20000-4)
04- Novità legali (Dlgs 198/2010, Privacy, Decreto Pisanu
05- Corso di Perfezionamento Computer forensics a Milano
06- Club di Cyberspazio e Diritto
07- Val IT 2.0 in italiano
08- "At your service", magazine di itSMF
09- Lasciatemi il mio PC!
10- BS 8878:2010 "Web accessibility. Code of practice"
11- Fascicolo Sanitario Elettronico
12- Wikileaks
13- Minacce e vulnerabilità: Utente "sconosciuto" su HP MSA2000 G3
14- Velocità di trasmissione
15- Mie presentazioni
****
01- Breve editoriale (nuovo sito) e auguri

Mi scuso per il ritardo di questa uscita: volevo prima mandare on-line il mio nuovo sito con nuova grafica. Cosa successa ieri sera. Un grazie ad Anita Franchella per aver fatto il 90% del lavoro di ideazione e di riscrittura, avendo a che fare con un pessimo cliente come me che contestava tutto (le cose che non vi piaceranno, saranno lì per quel mio 10%!)

Vi chiedo quindi di farmi avere i vostri commenti e critiche (da refuso, al bad english o mauvais francais, all'impostazione generale).

Vi faccio quindi i miei migliori auguri di Buone Feste e... arrivederci al 2011!

****

02- Standardizzazione famiglia ISO/IEC 27000

Stanno ora circolando i draft delle seguenti norme:
- ISO/IEC 27000 (2o draft)
- ISO/IEC 27001 (4o draft)
- ISO/IEC 27002 (3o draft)
- TR ISO/IEC 27008 - "Guidelines for auditors on information security controls" (Draft)
- ISO/IEC 27010 - "Information security management for intersector and inter-organisational communications" (Committee draft)
- ISO/IEC 27013 - Relazioni tra 27001 e 20000 (3o draft)
- ISO/IEC 27014 - Governance of information security (Committee draft)
- ISO/IEC 27016 - Organizational economics (1o draft)
- ISO/IEC 27033-3 - Reference networking scenarios -- Threats, design techniques and control issues (Final Draft)

Di alcune seguono i miei commenti, di altre tratterò il mese prossimo, altre ancora le ignorerò in quanto non le ritengo interessanti.

WD4 ISO/IEC 27001

Siamo al quarto draft della 27001.

L'aspetto da notare è che ora è impostata secondo il modello "JTCG 8 Common Structure and Identical Text for management system standards". La 27001 sarà la prima norma ad adottare questo modello e le altre (9001, 14001, 20000) dovrebbero seguire.

La norma, di per se stessa, non cambia molto soprattutto per quanti ne hanno dato delle interpretazioni corrette da un punto di vista formale e sostanziale. Ne riparleremo le prossime volte, quando si sarà più stabilizzata.

In realtà, il nuovo modello introduce almeno tre aspetti che al momento mi lasciano perplesso. Non mi sono ancora imbattutto in disquisizioni in merito sulla rete per capirli fino in fondo, ma ne lascio qui un piccolo elenco:
1- viene introdotta la necessità di pianificare il sistema di gestione tenendo in conto, seppure in modo sfumato ma esplicito, i rischi di impresa; se questa non è una novità per la 27001, certamente lo è per altre norme; il problema è che li chiama "issues" e questo potrà creare qualche confusione in chi si occuppa di "risks"
2- non ci sono più "procedure documentate" e "registrazioni", ma "documented information"; questo genera dei giri di parole non sempre semplici da assimilare
3- la richiesta di procedure documentate e registrazioni (quindi, di informazioni documentate) obbligatorie si è di molto ridotta, lasciando ulteriore margine all'utilizzatore; questo potrebbe creare qualche difficoltà per gli auditor che potrebbero trovarsi con sempre meno punti di appoggio per "capire" cosa auditare

Ripeto: non ho ancora valutato fino in fondo questi aspetti e mi riserverò di farlo dopo il prossimo draft.

WD3 ISO/IEC 27002

La 27002 è invece al terzo draft.

Le cose non sono molto cambiate per i capitoli dal 5 al 9. Segnalo che è stato introdotto un controllo sui progetti e uno sull'inserimento di nuovo personale.

C'è invece molta manovra sui capitoli successivi. Quelli attuali presentano infatti molte ridondanze, disomogeneità di tecnicità (si va dai molto generici ai molto specifici) e non sempre sono al posto giusto (perché il mobile computing e il teleworking sono nel capitolo dedicato al "controllo accessi" e non alle "operations"?).

Una lettura del testo mi ha fatto capire che ogni controllo del capitolo 10 non deve essere visto solo come collegato all'IT, ma anche a tutte le tipologie di "informazioni". Ho quindi chiesto di esplicitarlo meglio.

La situazione è al momento talmente "fluida" che non mi sembra il caso di fare ulteriori commenti.

FDIS ISO/IEC 27031

La ISO/IEC 27031 "Guidelines for information and communication technology readiness for business continuity" è ora allo stadio di final draft.

Si tratta di linee guida (quindi non "certificabili") che riprendono i concetti espressi dalla BS 25777 sulla relazione tra IT e Business Continuity.

Alcune cose interessanti:
- viene detto che bisogna segnalare quando i sistemi IT non possono soddisfare i requisiti di business in materia di tempi e metodi di ripristino, in modo da valutare se accettare la situazione attuale o intraprendere opportune azioni; troppo spesso si vede come il business stabilisca invece i propri obiettivi sulla base delle prestazioni dell'IT e come non siano evidenziati eventuali disallineamenti affinché siano consapevolmente accettati
- sono ben descritte le varie tipologie di test praticabili
- vi sono utili esempi di misurazioni quantitative (ve ne sono anche sulle misurazioni qualitative che non mi convincono)

Punto debole è l'eccessiva considerazione degli RTO a scapito di altri requisiti come gli RPO e altri controlli di sicurezza, oltre all'assenza del parametro relativo alle prestazioni (spesso ridotte rispetto a quelle normali) previste in caso di emergenza.

Alessandro Cerasoli (NIS - Network Integration and Solutions), durante le discussioni in seno all'Uninfo, ha fatto anche notare la mancanza del concetto di MTPoD (Maximum Tolerable Period of Distruption), ossia il limite massimo degli RTOs.

****

03- Standardizzazione famiglia ISO/IEC 20000

FDIS ISO/IEC 20000-1

La ISO/IEC 20000-1 è ora allo stadio di FDIS. Questo non vuol dire che sarà approvata, ma a questo punto è molto probabile che nel 2011 sarà emessa la nuova versione della norma.

La nuova versione è molto meglio scritta della precedente, anche se si notano ancora alcune inesattezze e imprecisioni deprecabili quando si tratta di uno standard internazionale. Sembra quasi che troppi standardizzatori improvvisati siano all'opera.

A parte ciò, i requisiti, in definitiva, sono molto simili agli attuali (ho fatto una verifica veloce) e soprattutto la parte di "New or changed services" ha ora un senso. Inoltre, molti requisiti sono simili all'attuale ISO 9001 di modo che anni di sviluppo non sono andati dimenticati ;-)

Mi ha molto interessato il lavoro fatto sul miglioramento continuo, ora esplicitamente non collegato alle sole azioni correttive e preventive.

Rimane infine un dubbio: perché continuare a chiamare "Known errors" gli incidenti di cui è nota la causa, quando nella realtà (e in modo a mio parere più significativo) si usa questo termine per gli incidenti di cui è noto uno o più workarounds?

ISO/IEC TR 20000-4:2010

E' stata pubblicata la quarta parte (non certificabile!) della 20000 dal titolo "Information technology — Service management — Part 4: Process reference model".

In poche parole, si tratta di una riscrittura della attuale 20000-1 (prima edizione) e del draft della seconda edizione seguendo il modello della ISO/IEC 15504-1.

Che dire? Si tratta di un esercizio di stile, forse interessante ma che non approfondirò. A questo aggiungo che non sono riuscito a capire il perché di questa operazione ora, a poco tempo dalla riemissione della norma. Infine, non sono riuscito a capire a quale draft della seconda edizione faccia riferimento.

****

04- Novità legali

Decreto Legislativo 198 del 2010 sull'installazione di reti IT

Dal blog di Luca De Grazia (http://lucadegrazia.postilla.it/2010/11/29/installare-da-soli-un-router-o-una-chiavetta-umts-sara-illegale/) ho trovato la notizia che il 15 dicembre entrerà in vigore il Dlgs 198 del 2010 che manderà in pensione tra un anno la Legge 109 del 1990 e il DM 314 del 1992.

Il Dlgs: http://www.normattiva.it/dispatcher?service=213&fromurn=yes&datagu=2010-11-30&annoatto=2010&numeroatto=198&task=ricercaatti&elementiperpagina=50&redaz=010G0219&newsearch=1&classeprv=1&paginadamostrare=1&tmstp=1292571461591

La lettura del dispositivo non chiarisce le idee, così come non le chiarivano i precedenti. Ad una lettura "intransigente", sembrerebbe che tutte le reti (anche interne di una casa, ufficio o azienda) debbano essere installate, collaudate e manutenute solo ed esclusivamente da aziende inserite in un apposito registro.

Rimane il punto f) del comma 2 dell'articolo 2 che prevede che vengano stabilite delle semplificazioni (chissà...).

Un'interpretazione più condivisa, però, prevede che il Dlgs si rivolga ai soli installatori e agli operatori di TLC, regolandone l'accesso al mercato. A questo va però aggiunto il fatto che il rappresentante legale di un'azienda potrebbe incorrere in qualche sanzione relativa alla sicurezza dei lavoratori (Articolo 80 del Dlgs 81 del 2008) perché, se non dovesse chiamare un installatore qualificato, non potrebbe dimostrare che "le installazioni e gli impianti elettrici ed elettronici sono stati progettati, realizzati e costruiti a regola d'arte". Questo anche se si tratta di tirare un solo cavo di TLC sotto il pavimento flottante.

Concordo con Luca De Grazia dicendo che il Dlgs è scritto male e può essere fonte di confusione.

Ogni contributo in merito sarà gradito.

Privacy: modificato il Codice per i funzionari pubblici

Dalla newsletter della DFA (www.perfezionisti.it) giro la notizia della modifica al Dlgs 196/2003 relativa agli "addetti ad una funzione pubblica".

In particolare sono stati modificati l'articolo 1 e 19.

La versione consolidata del Dlgs si trova su http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248

Abolizione Decreto Pisanu sulle wi-fi libere

Dalla newsletter della DFA (perfezionisti.it) riprendo la notizia dell'approvazione del Pacchetto Sicurezza da parte del Consiglio dei Ministri, che prevede il non rinnovo del Decreto Pisanu.

Il Decreto Pisanu, lo ricordo, imponeva diverse limitazioni alle connessioni su Internet, imponendo la rintracciabilità dell'utente. In modo molto semplicistico, si può quindi dire che ora i bar potranno offrire la connessione wi-fi gratuita.

L'articolo di riferimento: http://www.zeusnews.com/index.php3?ar=stampa&cod=13408

Luca De Grazia, nel suo blog, esprime un parere non allineato con quello più diffuso (tanto per intenderci:

quasi tutti vogliono "la wi-fi libera") e per questo vale la pena di analizzarlo:
http://lucadegrazia.postilla.it/2010/11/18/sprint-finale-per-il-wi-fi-libero-in-italia/

Io continuo a pensare che stiamo dibattendo senza dati: è servito a qualcosa il Decreto Pisanu o no? Finora, ancora nessuno mi ha risposto e quindi non mi pronuncio. Egoisticamente, lo ammetto, accetterò la comodità di potermi connettere alle wi-fi libere con gioia.

****

05- Corso di Perfezionamento Computer forensics a Milano

Sono state avviate le iscrizioni per il Corso di Perfezionamento in "Computer forensics e investigazioni digitali" dell'Università di Milano. Il corso è costituito da cinque giornate formative, al giovedì, dal 27 gennaio al 24 febbraio 2011.

Per info: http://forensics.typepad.com/ e infogiuremi@gmail.com

Mi permetto di segnalare l'evento perché io ho partecipato come studente alla seconda edizione e l'ho trovata molto interessante.

Purtroppo penso che questa segnalazione vi arrivi in ritardo (il termine per le iscrizioni era il 9.12).

Ad ogni modo, il 20 gennaio ci sarà la "Lezione zero" aperta, anche se consiglio di informarsi presso l'associazione Digital Forensics Alumni info@perfezionisti.it.

****

06- Club di Cyberspazio e Diritto

E' stato attivato il forum di discussione "Club di Ciberspazio e Diritto", come mi è stato segnalato da Giovanni Ziccardi.

Al momento ci sono 5 segnalazioni molto interessanti per chi vuole capire di più la materia.
https://groups.google.com/group/ciberspazioediritto/topics?hl=it

Ho trovato particolarmente interessante il riferimento ad un articolo in cui sono stati analizzati (e criticati) più di 400 casi nei quali sentenze statunitensi hanno citato Wikipedia.
http://www.yjolt.org/files/peoples-12-YJOLT-1.pdf

****

07- Val IT 2.0 in italiano

L'AIEA ha pubblicato la traduzione in italiano di Val IT 2.0 ed è scaricabile dall'area download di www.aiea.it.

Il framework estende i concetti di quello che in ITIL è il processo di Service Portfolio. E' un'ottima lettura.

Per i più pigri, spaventati dalle 128 pagine, suggerisco di leggere almeno fino a pagina 19, dove si trovano due perle:
1- "I programmi sono selezionati sulla base non solo della desiderabilità ma anche sulla capacità dell'organizzazione di portarli a termine".
2- "La presenza di metodologie in azienda è meno importante del loro effettivo utilizzo da parte dei business managers".

A pagina 20 si trova la figura 9, con illustrati i domini del Val IT e i corrispondenti processi. Il primo processo "Istituire una leadership informata e responsabilizzata" potrebbe dare materia di riflessione.

****

08- "At your service", magazine di itSMF

Su ITSM News di novembre si trova la notizia sulla prima uscita del magazine dell'itSMF "At your Service", dedicato all'IT Service Management e a ITIL.

Particolarmente significativo è l'articolo di IT Skeptic, utile per capire come è evoluto ITIL nel passato e come probabilmente evolverà.

Purtroppo, il sito ufficiale dell'itSMF non dà grande risalto al magazine, né dà informazioni sulle prossime uscite (quando saranno e come esserne aggiornati).
http://www.itsmfi.org/content/new-itsmf-international-magazine-your-service-launched

****

09- Lasciatemi il mio PC!

Sulla newsetter della società Ready Informatica (temo si tratti di spam...), si trova un articolo dal titolo "Lasciatemi il mio PC!". In poche parole, l'articolo si pone la domanda "Come far fronte alla marea di dispositivi personali e non tradizionali sul lavoro?" e risponde proponendo la soluzione di Citrix.

Al di là dell'aspetto commerciale che non intendo approfondire anche perché non l'ho studiato né nello specifico, né in rapporto ad eventuali concorrenti, è opportuno riflettere sulla pertinenza della domanda: oggi si vedono innumerevoli dipendenti che usano smartphones e tablet personali e anche il pc di casa per accedere alla rete aziendale. Per non parlare dei fornitori che si collegano alla stessa rete con dei pc incontrollati.

Le risposte "semplici" sono facili: non permettere questo genere di comportamenti, non permettere l'accesso alla rete aziendale dall'esterno, dare l'accesso ai fornitori solo attraverso computer aziendali. Ma è vero che il mondo è ormai cambiato e sta cambiando sempre più e noi dobbiamo prenderne atto e cambiare le scelte di trattamento di questi rischi.

L'articolo: http://www.ready.it/lasciatemi_il_mio_pc.html

****

10- BS 8878:2010 "Web accessibility. Code of practice"

Il BSI annuncia la pubblicazione della BS 8878 "Web accessibility. Code of practice".

Questo ci fa ricordare della necessità di pensare ad un tema apparentemente marginale: un sito "accessibile" non è solo necessario a chi è portatore di handicap, ma è anche più facilmente fruibile dai cosiddetti normodotati (alla fine degli anni '90, una delle richieste di accessibilità riguardava gli scivoli strada-marciapiede che ora si rilevano utili per tutti).

La pubblicazione dello standard inglese ricorda sì questi aspetti, ma costa 100 sterline (120 Euro) per 90 pagine. Per chi volesse approfondire la materia gratuitamente, un punto di accesso è la pagina della DigitPA (http://www.digitpa.gov.it/content/accessibilit%C3%A0) da cui accedere anche ad interessanti risorse on line.

Il CNIPA gestiva il sito http://www.pubbliaccesso.gov.it con una buona Biblioteca (link ad altre risorse) e ha pubblicato nel lontano 2005 il quaderno 4 sull'accessibilità (http://www.cnipa.gov.it/site/it-IT/La_Documentazione/Pubblicazioni/Quaderni_dell'accessibilit%c3%a0/).

Un altro importante riferimento sono le "Linee guida per l'accessibilità ai contenuti del Web" del W3C, ora alla versione 2.0: http://www.w3.org/Translations/WCAG20-it

****

11- Fascicolo Sanitario Elettronico

Segnalo l'interessante pagina sul Fascicolo Sanitario Elettronico (http://fse.clusit.it), da cui è possibile scaricare una breve analisi della normativa vigente e delle best practices applicabili.

Sono inoltre disponibili le modalità per richiedere ulteriore materiale al gruppo di lavoro.

****

12- Wikileaks

Credo che la faccenda Wikileaks sia stata sufficientemente coperta da diversi media e commentatori. Quindi non ritengo di doverne discutere molto.

Si potrebbero anche fare delle riflessioni su "come si diffondono le notizie", vere o false che siano. Ma su questo, credo che Quarto Potere di Orson Welles e l'ultimo libro di Eco siano sufficientemente illuminanti.

Rimane il problema della sicurezza. Visto che nessun uomo è un'isola, è necessario dare un certo livello di fiducia a amici, clienti, collaboratori e fornitori. In altre parole, è necessario dare loro un tot di informazioni.

Sono dei rischi che corriamo, a fronte di innegabili benefici (umani, sociali, economici, professionali).

Possiamo (e dobbiamo!) realizzare tutte le misure tecniche o organizzative che vogliamo (dal SANS Newsbyte, la reazione dei militari USA http://www.wired.com/dangerroom/2010/12/military-bans-disks-threatens-courts-martials-to-stop-new-leaks/), possiamo monitorare il personale (qualcuno, in barba allo Statuto dei Lavoratori ha anche proposto la macchina della verità!), possiamo limitare il più possibile l'accesso di ciascuno alle informazioni, ma avversari, delusi e ricattabili ci saranno sempre.

In conclusione: cogliere il segnale è un bene, ma ricordarsi sempre che la sicurezza al 100% non è raggiungibile e che la parola chiave è "bilanciamento" (tra i rischi, le esigenze efficienza e il budget).

Rimane la massima applicabile a tanti contesti: "se non vuoi che non sia pubblicato, non scriverlo, non dirlo, non fotografarlo".

A fronte di una serie di commenti inutili, ridondanti o addirittura sciocchi, mi permetto di suggerirne uno buono di Andrea Monti, dove viene anche ricordato il caso del dossier Mitrokin:
http://www.ictlex.net/?p=1211

PS: qualche tempo fa, mi è capitato di vedere una mail di risposta ad un creditore. Il debitore accampava delle belle scuse per ritardare il pagamento o, addirittura, per non farlo. Peccato che si fosse dimenticato di cancellare dalla mail tutta la propria corrispondenza interna, da cui si capiva chiaramente che le scuse erano costruite ad arte.
Questo per dire: il caso Wikileaks è solo un segnale pubblico di cose che accadono quotidianamente e non diffuse.

PS2: mi è tornato in mente un progetto in cui il cliente, per necessità di riservatezza, non mi voleva dare accesso ad una serie di documenti. Gli ho fatto notare che senza documenti non avrei potuto fare nulla. Questo per dire: anche la paranoia non porta da nessuna parte

PS3: Hervé Schauer, nella sua newsletter, premette un editoriale molto più corto di questo (e senza Post scriptum...) segnalando solo che la vicenda ci ricorda due vulnerabilità da tenere in conto: 1) le chiavi USB permettono di trasmettere più informazioni della rete IT; 2) le persone nate nell'era dell'informatica distinguono sempre meno tra vita professionale e vita privata.

****

13- Minacce e vulnerabilità: Utente "sconosciuto" su HP MSA2000 G3

Dal SANS Newsbyte, giro la notizia "sulle macchine HP StorageWorks MSA G3 P2000, è presente un utente non rilevabile attraverso i normali strumenti gestionali e con password standard"

La HP ha già pubblicato le specifiche per risolvere il problema.
http://isc.sans.edu/diary.html?storyid=10090
http://www.securityweek.com/backdoor-vulnerability-discovered-hp-msa2000-storage-systems

Come Stuxnet, anche questo caso sottolinea come i concetti base della sicurezza IT siano sconosciuti ai più.

****

14- Velocità di trasmissione

Andrea Rui (Tecnoindex S.p.A.) mi ha segnalato questa divertente notizia (come se avesse letto l'editoriale di Hervé Schauer):
per inviare un messaggio nella zona di Durban (Sudafrica) è più veloce il piccione dell'Adsl.
http://www.tgcom.mediaset.it/mondo/articoli/articolo459872.shtml

****

15- Mie presentazioni

In novembre ho tenuto due interventi, di cui è possibile scaricare il materiale:

- “IT Governance: scelte e soluzioni”, intervento per il convegno "Stanco di fare l'equilibrista - Lasciatevi condurre sul cammino sicuro verso una corretta IT Governance" organizzato da ECS (pdf, 363KB).

- “Appréciation conjointe ISO 27001 et ISO 20000-1”, intervento tenuto in francese a Parigi per il Club 27001 (www.club-27001.fr); (pdf in inglese, 700KB).