****
IT SERVICE MANAGEMENT NEWS - FEBBRAIO 2012
****

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

****
01- Novità legali - Privacy (DL Crescita, Semplificazione, Regolamento UE)

Mese impegnativo per chi si occupa di Privacy. Come potete notare dalle tante notizie.

Il D.L. Crescita Italia diventa Legge

Con la Legge 214 del 22 dicembre 2011, il Decreto Legge 201/2011 "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici" è stato convertito in Legge, con modificazioni.

I punti di interesse:
- art.29-bis: introduce, all'articolo 68 del Codice dell'Amministrazione Digitale (Dlgs 82 del 2005), la categoria del software libero accanto ai programmi a codice sorgente aperto tra le opzioni che hanno le PA per scegliere i programmi informatici
- art. 40 comma 2: esclude dall'applicabilità del Codice Privacy le persone giuridiche, enti e associazioni (aumentando l'impatto di quanto già stabilito dal DL 70 del 2011, convertito in Legge dalla Legge 106 del 2011).

(Su segnalazione di Daniela Quetti della DFA)

DL Semplificazione: DPS addio (ma meglio stare attenti ancora un po')

E' stato pubblicato in Gazzetta Ufficiale il D.L. n. 5 del 2012 "Disposizioni urgenti in materia di semplificazione e di sviluppo" dove, all'articolo 45, viene eliminato il DPS.

Ovviamente, per essere sicuri sicuri, dovremo aspettarne la Legge di conversione, che potrebbe recare modifiche o farlo decadere. Dovremo aspettare al massimo 60 giorni per avere certezze definitive. E quindi tali certezze potrebbero arrivare dopo il 31 marzo, data di "scadenza" per i DPS... chissà se conviene farlo o no?

Se dobbiamo poi discutere se si tratta di una semplificazione, guardo nel mio palazzo (un artigiano, uno studio di ingegneria, uno studio di un professionista - io, due medici che però non hanno lo studio privato) e posso dire che almeno 4 o 5 DPS inutili non sono più obbligatori.

Se però penso ad alcuni miei clienti (tra le cui attività vi sono: trattamento paghe e stipendi di persone, gestione donazioni per scopi religiosi, ricerche di mercato, selezione del personale, conservazione cartelle mediche) e ad alcune realtà fortemente sindacalizzate e se penso anche ai tanti reclami al Garante da sindacati e consumatori, allora mi viene da pensare che a molti conviene predisporre, in ottica preventiva, nel caso in cui dovessero essere coinvolti in un procedimento giudiziario o da una verifica da parte del Garante, un documento che dimostri in qualche modo l'attuazione delle misure di sicurezza minime e idonee previste (ancora...) dal Codice Privacy.

Non dimentichiamoci infine che i Titolari devono dimostrare il controllo sulle attività dei Responsabili, che devono fornire loro delle istruzioni, che devono verificare l'operato degli Amministratori di Sistema e che rimangono responsabili penalmente per alcuni inadempimenti. Sicuramente, molte aziende dovranno produrre ancora dei documenti in merito e una sorta di "lista di riscontro", come poteva essere inteso il DPS, sarà sempre utile.

Insomma, io suggerirei a queste imprese di continuare a farlo (e non solo per mie finalità economiche di bieco consulente!), anche se ora non bisognerà più pensare alla scadenza del 31 marzo, potrà essere redatto in modo diverso, forse migliore, e potrà essere nominato "Manuale Privacy" o "Pippo" e non più "DPS".

Ultima nota: con l'eliminazione del punto 19.6 dell'Allegato B, non c'è più una misura minima la formazione al personale. Ho già discusso altrove come questa misura sia mal scritta e mal posizionata all'interno del Codice. Ora mi chiedo: è veramente furbo non prenderla più in considerazione?

Attilio Rampazzo mi ha suggerito anche il seguente articolo, che condivido quasi completamente:
- http://www.federprivacy.it/index.php?option=com_content&view=article&id=469&Itemid=8
(per i curiosi: non condivido quanto detto sul ruolo del Responsabile della Sicurezza, né sull'inutilità dei riferimenti a nomine e informative sul DPS; quest'ultimo punto non l'ho mai preso in carico, ma ora che il DPS è facoltativo lo trovo utile perché così neanche questi aspetti sfuggono alla lista di riscontro).

Ringrazio Max Cottafavi di Spike Reply per avermi dato la notizia per primo e Daniela Quetti per avermi segnalato per prima la sua pubblicazione ufficiale. Si può trovare su Normattiva:
- http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2012-02-09&atto.codiceRedazionale=012G0019¤tPage=1

Regolamento UE sulla Privacy (forse il DPS resusciterà)

Grazie a Uninfo, ricevo notizia sull'attuale bozza del possibile futuro Regolamente Privacy a livello europeo.

Detto in poche parole, questo regolamento, una volta approvato, entrerà in vigore per tutti gli stati UE. Le proposte sono sottoposte, ora, al Parlamento europeo e agli Stati membri dell'Unione (riuniti in sede di Consiglio dei Ministri) per discussione e, una volta adottate, non entreranno in vigore prima di due anni. Quindi: c'è tempo.

Il link: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Ho trovato molto interessante la lettura della bozza e scrivo qui alcuni punti:
- articolo 26: stabilisce chiaramente che se il Responsabile (Processor) tratta i dati senza opportune istruzioni del Titolare (Controller), allora deve essere considerato Titolare Congiunto (Joint Controller). Osservo che il trasferimento ad altri da parte del Processor è vietato, se non dopo autorizzazione da parte del Controller: il 99% degli attuali Responsabili Esterni saranno quindi Joint Controller
- articolo 28: il DPS è morto da poco ma, se passa questo articolo, risorgerà forse più molesto di prima; saranno esentate le aziende con meno di 250 addetti (ma bisognerà capire come tradurre "employing fewer than 250 persons")
- articolo 30: bisogna ancora fare una "valutazione dei rischi"
- articoli 31 e 32: gli incidenti con impatto sui dati personali dovranno essere comunicati al Garante e agli interessati
- articolo 33: la notifica al Garante viene un poco trasformata; anzi... bisognerà anche fare un "impact assessment"
- articolo 35 e seguenti: le aziende con più di 250 persone dovranno nominare un Data Protection Officer
- articolo 39: potrà esistere una "certificazione privacy"; ne vedremo delle belle... temo.

Copiando un intervento di Daniela Quetti, segnalo anche:
- il riferimento ad un'unica autorità nazionale di protezione dei dati nel paese dell'Unione in cui imprese e organizzazioni hanno il proprio stabilimento principale;
- l'introduzione del diritto all'oblio: chiunque potrà cancellare i propri dati se non sussistono motivi legittimi per mantenerli;
- le norme UE si applicheranno anche ai dati personali trattati all'estero da imprese che sono attive sul mercato unico e offrono servizi ai cittadini dell'Unione;
- le autorità nazionali indipendenti di protezione dei dati avranno maggiori poteri.

Segnalo anche un articolo segnalato da Attilio Rampazzo che mette in relazione la sorte del DPS con il Regolamento UE:
- http://www.federprivacy.it/index.php?option=com_content&view=article&id=468:passa-il-decreto-semplificazioni-il-dps-e-stato-abolito&catid=40:flash-news&Itemid=64

Altro di interessante c'è. Per chi volesse: buona lettura!

La Direttiva collegata al Regolamento riguarda solo il trattamento dei dati da parte delle autorità addette a prevenire, investigare, rilevare e perseguire crimini.

****

02- Standard - Pubblicata la ISO/IEC 27007

E' stata pubblicata la ISO/IEC 27007 dal titolo "Guidelines for information security management systems auditing". E' un'estensione della ISO 19011, applicabile agli audit di prima e seconda parte.

Non aggiunge molto rispetto ai requisiti della ISO 19011 e da questo punto di vista non è interessante. Può essere però interessante la lettura dell'allegato A (informativo) "Practice Guidance for ISMS Auditing", dove è quasi proposto un manuale di auditing molto dettagliato.

****

03- Standard - UNI EN ISO 19011 (in italiano) - Linee guida per gli audit di gestione

E' stata appena pubblicata la versione in italiano della ISO 19011.

Ho già commentato la versione in inglese: http://blog.cesaregallotti.it/2011/11/iso-190112011.html

Aggiungo solo che la 19011 si applica ai soli audit di prima parte (audit interni) e di seconda parte (ai fornitori o ai partner). Per gli audit di terza parte (audit degli organismi di certificazione), bisogna fare riferimento alla ISO/IEC 17021 e alle norme che da essa discendono (per esempio la ISO/IEC 27006).

La norma è interessante, soprattutto se consideriamo come sono svolti alcuni audit (rilievi non discussi con il personale, rapporti inviati dopo settimane o mesi, eccetera).

****

04- Elenco degli standard di sicurezza ICT

Da Uninfo, che ha girato il verbale del primo incontro del "CEN-CENELEC-ETSI Cyber Security Coordination Group (CSCG)", ricevo il link a "una lista di tutti gli standard relativi alla sicurezza ICT", curata dall'ITU: http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

La pagina è decisamente interessante e, a sua volta, indirizza ad altre 6 pagine. I riferimenti sono tanti e dovrebbero soddisfare quasi ogni esigenza.

****

05- Computer forensics e processo civile

Uno degli argomenti normalmente meno dibattuti in ambito di computer forensics è "la prova nel processo civile". La cosa, invece, da profano ma con interessi nella materia, mi interessa molto.

Provo qui a raccogliere gli elementi in merito:
- nell'ordinamento italiano, i mezzi di prova sono "tipici", ossia devono essere quelli stabiliti dalla Legge (prova documentale, prova testimoniale, presunzioni, confessione, giuramento)
- le prove possono essere legali (il giudice è vincolato a prenderne atto) o liberamente apprezzabili (la Legge non attribuisce loro alcuna predeterminata valenza probatoria)
- le prove possono essere piene (dimostrano con certezza la veridicità dei fatti cui si riferiscono), di verosomiglianza (ritenute sufficienti dalla Legge) oppure possono essere "argomenti di prova" (offrono alcuni elementi di valutazione)

Per quanto riguarda la prova informatica:
- le riproduzioni informatiche hanno la medesima valenza probatoria delle riproduzioni meccaniche disciplinate dall'articolo 2712 del Codice Civile: la prova è piena se colui contro il quale sono prodotte non le disconosce; se contestate, devono essere considerate argomenti di prova
- il Codice dell'Amministrazione Digitale (CAD, Dlgs 82 del 2005, più volte modificato), nella versione attuale, definisce il valore giuridico del documento informatico come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"; ricordiamo che il CAD stabilisce anche che tale mezzo di prova è liberamente valutabile in giudizio se firmato elettronicamente oppure costituisce se firmato digitalmente

Per l'acquisizione e presentazione delle prove, non vi sono regole esplicite. Si consiglia però, anche per motivi prudenziali, di acquisire e presentare i documenti con le stesse procedure tecniche del penale, documentando le modalità seguite e la catena di custodia.

Ovviamente, poi, i casi reali possono essere piuttosto variegati. Segnalo quindi questa presentazione trovata sul web:
- http://www.slideshare.net/gbellazzi/la-gestione-legale-delle-prove-digitali

Ulteriori segnalazioni in materia sono gradite.

****

06- Computer forensics - Video Marco Mattiucci

Segnalo i notevoli video di Marco Mattiucci sulla Computer Forensics:

Video 3: "Incertezza nel Digital Forensics"
Video 4: "Aree del Digital Forensics"
Video 5: "Computer Forensics"
Video 6: "I problemi nel Digital Forensics"
Video 7: "Mobile forensics"

I primi due video, li avevo segnalati precedentemente.

Sono tutte delle lezioni base, anche se con diverse complessità. Fa eccezione il video 3 che propone una lezione di buona complessità, utile però a far capire che, prima di cimentarsi nella materia, è necessario aver seguito un buon percorso di formazione (teoria, pratica, affiancamento in situazioni reali).

Per accedere ai video, il punto di partenza è una pagina del sito di Marco Mattiucci:
- http://www.marcomattiucci.it/myvideodf.php

****
07- Telelavoro e sicurezza (riferimenti legali)

Dalla circolare dello Studio Tributario "Borioli & Colombo Associati", riporto che il comma 5 dell'articolo 22 della legge 183/2011(Legge di stabilità 2012) interviene sul tema del telelavoro con la finalità di favorirne l'utilizzo, oggi poco diffuso. Tale tipologia di lavoro subordinato non è rinvenibile in alcuna norma di legge ma, nel settore privato, è contenuta in vari accordi aziendali o di settore, fino a trovare il suo sbocco più generale nell'accordo interconfederale del 9 giugno 2004 che ha recepito l'accordo quadro europeo del 16 luglio 2002.

Ovviamente, non è questo il luogo dove discutere della Legge di Stabilità, ma degli impatti sulla sicurezza. E per questo è interessante leggere l'accordo in questione. Ecco alcuni punti che evidenzio:
- Articolo 1 - Definizione: Il telelavoro costituisce una forma di organizzazione del lavoro che si avvale delle tecnologie dell' informazione, in cui l'attività lavorativa, che potrebbe anche essere svolta nei locali dell'impresa, viene regolarmente svolta al di fuori dei locali della stessa
- Articolo 2: il datore di lavoro provvede a fornire al telelavoratore le relative informazioni scritte
- Articolo 4 - Protezione dei dati: Il datore di lavoro ha la responsabilità di adottare misure appropriate, in particolare per quel che riguarda il software, atte a garantire la protezione dei dati utilizzati ed elaborati dal telelavoratore per fini professionali.
- Articolo 6 - Strumenti di lavoro: Di regola, il datore di lavoro è responsabile della fornitura, dell'installazione e della manutenzione degli strumenti necessari ad un telelavoro svolto regolarmente, salvo che il telelavoratore non faccia uso di strumenti propri; In caso di guasto o malfunzionamento degli strumenti di lavoro il telelavoratore dovrà darne immediato avviso alle strutture aziendali competenti

Io ho trovato l'accordo su:
https://www.cliclavoro.gov.it/informarmi/comefarepercit/Conciliarefamigliaelavoro/Documents/accordo_telelavoro2004.pdf

****

08- Certificati digitali invalidati?

La notizia è che le firme digitali utilizzate da ottobre 2011 da noi utenti potrebbero essere non ritenute valide. Il motivo è che per la generazione dei certificati digitali (e, quindi, per garantire la validità della firma digitale) è necessario utilizzare dei meccanismi certificati dall'OCSI. Ovviamente, come al solito, Le scadenze sono state di volta in volta posticipate fino ad arrivare al pasticcio. Ora sembra che solo i certificati rilasciati da un unico operatore siano validi. E gli altri?

L'articolo del Corriere della Sera:
- http://archiviostorico.corriere.it/2012/gennaio/23/pasticcio_delle_firme_digitali_ce_0_120123076.shtml

L'articolo di pc professionale:
- http://www.pcprofessionale.it/2012/01/27/il-far-west-delle-firme-digitali-8-milioni-di-certificati-fuorilegge/

Il commento dello Studio Legale Lisi:
-
http://www.studiolegalelisi.it/notizia.php?titolo_mod=376_Il_pasticcio_italiano_dei_dispositivi_automatici_di_firma__le_firme_digital

Insomma, di qualunque materia si tratti, pare che le certificazioni non siano sempre apprezzate dalle aziende italiane...

La notizia me l'ha data mio padre per primo, Franco Ferrari del DNV poi e infine Daniela Quetti della DFA. L'ho trovata anche sulla newsletter dello Studio Legale Lisi.

****
09- I 20 controlli per un'efficace difesa informatica

Sulla newsletter Sans NewsByte del 13 gennaio si trova la notizia che il Governo UK ha rilasciato un documento dal titolo "20 critical controls for effective cyber defence".
- http://www.cpni.gov.uk/advice/infosec/Critical-controls/

Questo sono a loro volta un riassunto dei "20 Critical Security Controls - Version 3.1" dello stesso SANS. Meglio leggere questi, con molte linee guida in più (come la mancanza del controllo può essere sfruttata per un attacco, come realizzare il controllo, come misurarne l'efficacia, procedure e strumenti per realizzare il controllo, quali test condurre).
- https://www.sans.org/critical-security-controls/

Per gli appassionati di metriche, di cui la guida del SANS fornisce molti esempi, segnalo che la bozza della ISO/IEC 27001 ora in circolazione richiede, in modo più generico dell'attuale versione del 2005, di "misurare l'efficacia del Piano di Trattamento del rischio".

****

10- Sostenibilità e responsabilità sociale

Un tema interessante è quello della sostenibilità. La sua accezione più ampia parte dal presupposto che "un'economia sostenibile a livello globale dovrebbe combinare la profittabilità a lungo termine con la giustizia sociale e la cura dell'ambiente".

Le organizzazioni possono quindi misurare e diffondere le proprie prestazioni in merito alla sostenibilità (a livello globale).

Per elaborare questi report, sono disponibili diverse linee guida o manuali.

Ho trovato interessante il link segnalatomi da Antonio Astone del DNV Italia:
http://www.globalreporting.org/

Qui, nella sessione "Get started" è possibile trovare le "Sustainability Reporting Guidelines", utili per chi volesse iniziare a produrre il proprio report.