****
IT SERVICE MANAGEMENT NEWS - NOVEMBRE 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.

IT Service Management News è rilasciata sotto la Creative Commons Attribution 3.0 Unported License (http://creativecommons.org/licenses/by/3.0/deed.it). Bisogna attribuire il lavoro a Cesare Gallotti con link a http://www.cesaregallotti.it/Newsletter.html

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- Standardizzazione: Stato delle norme ISO/IEC 270xx -- ottobre 2012

Dal 22 al 26 ottobre, si è tenuto a Roma il plenary meeting del WG1 dell'SC27, ossia del gruppo responsabile delle norme ISO/IEC 270xx. Io vi ho partecipato come delegato per l'Italia.

Ricordo il percorso delle norme: si parte da WD (working draft) e poi si hanno i CD, i DIS, i FDIS (final draft) e infine la pubblicazione.

Questi i risultati:
- ISO/IEC 27000: sarà pubblicata a breve la nuova versione; si è comunque stabilito di riaprire i lavori per una nuova versione (early revision) anche a seguito di quanto uscirà dai lavori sulla ISO/IEC 27001 e 27002
- ISO/IEC 27001: è stata proposta per il passaggio a DIS, procedendo quindi nel cammino che dovrebbe concludersi a ottobre 2013 con la pubblicazione della nuova sua versione; ulteriori dettagli nel seguito
- ISO/IEC 27002: è stata proposta per il passaggio a DIS, procedendo quindi nel cammino che dovrebbe concludersi a ottobre 2013 con la pubblicazione della nuova sua versione; gli editor dovrebbero preparare un documento con indicate le modifiche principali; ulteriori dettagli nel seguito
- ISO/IEC 27003 sull'implementazione di un ISMS: si è stabilito di riesaminare la norma anche in funzione delle future versioni di ISO/IEC 27001 e 27002
- ISO/IEC 27004 sulle misurazioni: si è stabilito di avviare dei lavori preliminari alla sua revisione; in particolare, si è stabilito di effettuare delle indagini sulle misurazioni necessarie per la valutazione di efficacia dei controlli e/o dell'ISMS

- ISO/IEC 27006: sono proseguiti i lavori; gli elementi di maggior interesse, per lo meno dal mio punto di vista, hanno riguardato la pubblicazione sul certificato della versione del SOA (l'Italia è stata contraria a questa opzione, e se ne discuterà ancora) e una nuova tabella per le giornate di audit necessarie per la certificazione, ricertificazione e sorveglianza di un sistema di gestione per la sicurezza delle informazioni
- ISO/IEC 27015 sui financial services dovrebbe essere pubblicata a breve
- ISO/IEC 27016 su "Organizational economics" è stata proposta per il passaggio a PDTR (equivalente allo stato di DIS)
- ISO/IEC 27017 e 27018 sul cloud computing: sono proseguiti i lavori
- ISO/IEC 27019 "Information Security within Smart Grid Environments": dovrebbe essere approvato a breve sulla base di una norma tedesca e verrà poi sottoposto ad early revision
- sono partiti i lavori per un nuovo standard dal titolo "Use of ISO/IEC 27001 for Sector-Service Specific Third Party Accredited Certifications"
- sono state discusse norme e iniziative sui modelli di maturità di un ISMS, sui sistemi di gestione per la privacy e PIMS, sulla certificazione delle persone sulla sicurezza delle informazioni

PS: Ringrazio Fabio Guasconi, Presidente SC27 dell'Uninfo per la segnalazione di alcune integrazioni.

****

02- Standardizzazione: Sulla futura ISO/IEC 27001

Durante il meeting di Roma del WG1 dell'SC27, sono continuati i lavori sulla nuova ISO/IEC 27001, che dovrebbe uscire a ottobre 2013. Si osservi però che la versione attualmente in bozza è oggetto di parecchie critiche (personalmente, ne condivido solo una parte) e non è detto che la nuova norma verrà pubblicata.

La Polonia si è lamentata, tra le altre cose, che nella discussione nessuno ha fatto riferimento al proprio mercato di riferimento e alle sue richieste. Ciò mi ha fatto riflettere e ho pensato quali potrebbero essere le richieste del mercato italiano (accetto contributi):
- semplificazione dei requisiti del metodo di risk assessment perché la sua elaborazione, secondo lo schema del 2005, richiede troppe risorse togliendole ad altri progetti e non fornisce risultati sempre utili perché troppo di dettaglio
- irrobustimento delle garanzie per i clienti delle aziende che si certificano ISO/IEC 27001
- migliore leggibilità per garantire corrette relazioni tra organizzazioni certificate e auditor

Procedo quindi nel dare notizia delle novità più rilevanti.

Scopo dell'ISMS
Rimane il requisito generale di descrivere lo scopo dell'ISMS (da non confondere con la frasetta sul certificato), senza ulteriori specificazioni (ad esempio, "includendo le caratteristiche del business, dell'organizzazione, della localizzazione, dei beni e delle tecnologie") perché ritenute implicite; rimane il requisito di descrivere i confini dell'ISMS e le sue relazioni con entità esterne.
Il Giappone (e anche l'Italia) sono stati molto contrariati da questa scelta; personalmente, mi chiedo perché non voler esplicitare qualcosa di implicito, se questo può migliorare la leggibilità dello standard e ridurre incomprensioni tra imprese e auditor.
Anche in altre situazioni, l'Italia ha promosso l'aggiunta di testo esplicativo per migliorare la leggibilità dello standard e ridurre incomprensioni tra imprese e auditor. Purtroppo è prevalsa la linea della "eleganza": dove il requisito è implicito, non si aggiunge testo.

Direzione
Molto dibattere si è fatto sulle responsabilità della Direzione. In particolare, l'Australia ha voluto ridurle. Questo aspetto mi è risultato incomprensibile perché, a mio avviso, la norma attuale prevede (sintetizzo) che la Direzione garantisca la realizzazione dell'ISMS e comunichi l'importanza della sicurezza delle informazioni. Non mi sembrano compiti gravosi.
E' vero che molte Direzioni si disinteressano della sicurezza delle informazioni tranne quando c'è l'audit (e neanche questo caso si verifica sempre), ma fornire loro una giustificazione per farlo mi sembra scorretto. Tra l'altro, è ben noto che, se la Direzione si disinteressa della sicurezza delle informazioni, il resto dell'impresa farà altrettanto, con ovvi risultati.
Un'ultima riflessione: ogni articolo o conferenza ribadisce il concetto dell'importanza della Direzione: mi piacerebbe vedere ben sviluppati gli argomenti di chi è contrario, sempre che ciò sia possibile.

Processi e attività di business
Il testo "comune" alla future norme sui sistemi di gestione prevedeva frasi come "attività di business" o "processi di business". Su proposta dell'Italia è stata tolta la dizione "di business", in parte perché bisognerebbe capire quali sono le attività "non di business" e in parte perché, quali esse siano, la sicurezza delle informazioni si applicherebbe anche a loro.

Metodo di risk assessment
L'attuale ISO/IEC 27001 del 2005 sviluppa una metodologia di risk assessment: individuare gli asset, le minacce e le vulnerabilità; valutare la verosimiglianza delle minacce e i loro potenziali impatti sugli asset. Tutto questo è stato eliminato: non si fa più riferimento agli asset, alle minacce o alle vulnerabilità. Si fa riferimento ai rischi che riguardano le informazioni.
Non mi pare sia un male: seppure implicitamente, si richiede di individuare le informazioni e i rischi che incombono su di esse, senza imporre metodologie che nella pratica sono troppo onerose e non utili. Sarà poi agli "esperti" sviluppare un metodo che garantisca di aver individuato (al giusto livello di granularità) tutti i rischi. Agli auditor, esattamente come oggi, viene solo richiesto di verificare la coerenza (o la "validità", come si è deciso) del metodo di risk assessment e dei suoi risultati.
Il Giappone si è dichiarato contrario a questa impostazione.
Personalmente, mi pare una buona soluzione, ma devo ancora rifletterci: probabilmente qualche indicazione in più potrebbe essere utile (per la cronaca: Fabio Guasconi, Presidente dell'SC 27 di Uninfo è solidale con il Giappone).

Misurazione dei controlli
Con mia grande gioia (anche perché la proposta era mia), è stato eliminato il concetto di misurazione dei controlli. Rimane il fatto che l'organizzazione deve valutare l'efficacia del proprio ISMS grazie ad attività di monitoraggio o misurazione, secondo quanto necessario.
Questo includerà sicuramente la misurazione dell'efficacia di alcuni controlli, ma se qualcuno vorrà misurare cose inutili, almeno non avrà la scusa dello standard.

Riesame della Direzione
Su proposta dell'Italia, è passato senza quasi discussione il fatto che la Direzione, nel riesame periodico, deve anche riesaminare i risultati del risk assessment e lo stato del piano di trattamento del rischio. Interessante che ciò sia successo dopo che si era detto che la stessa Direzione non poteva svolgere troppi compiti.

Statement of Applicability e Annex A
E' stato confermato il requisito che richiede l'elaborazione di un SOA collegato all'Annex A della norma. Come Italia siamo lievemente a favore della sua eliminazione. Personalmente, credo che sia un bene che rimanga il SOA collegato all'Annex A, perché impone al mercato l'adozione di una terminologia e di uno schema unico (insomma, impone l'adozione di uno standard!).

Risk assessment: nella pianificazione o nelle operation?
Ho lasciato per ultimo l'argomento più difficile.
Si è molto dibattuto su: i requisiti sul risk assessment vanno nel capitolo "planning" o nel capitolo "operation"?
L'Italia (con la maggioranza) ha votato per la prima ipotesi perché il risk assessment fornisce i risultati necessari alla scelta dei controlli di sicurezza e alla loro pianificazione.
Altri dicono che il capitolo planning riguarda il solo sistema di gestione che ha altri rischi rispetto alla sicurezza delle informazioni.
Personalmente, vedo come molto pericolosa questa seconda impostazione perché prevede che il "sistema di gestione" sia una cosa e la sicurezza delle informazioni sia un'altra cosa, buttando all'aria tanta letteratura e pratica sul fatto che la sicurezza delle informazioni debba essere vista come un insieme integrato di tecnologia e processi. La norma, comunque, riguarda il "sistema di gestione per la sicurezza delle informazioni" (e non un generico "sistema di gestione") di cui i controlli di sicurezza sono parte integrante. Pertanto, pianificare il sistema di gestione per la sicurezza delle informazioni implica necessariamente la scelta dei controlli di sicurezza, da fare con il risk assessment. Altra mia obiezione è: quale rischio al "sistema di gestione" vedete che non è applicabile al "sistema di gestione per la sicurezza delle informazioni"? La risposta è sempre stata una sola: "indisponibilità della Direzione" e mi pare un po' pochino.

Il problema è che il common text presenta alcuni requisiti che creano confusione: nella pianificazione si richiede di considerare rischi e "issues" (in italiano, "questioni"), e qui c'è chi distingue tra rischi strategici e operativi (ma questo ragionamento non toglie nulla alla necessità di avere il risk assessment dell'ISMS nel planning); nelle operation si fa comunque riferimento alla pianificazione delle attività, ma qui si dovrebbe fare riferimento ai piani di dettaglio o ai piani di produzione (per esempio, il piano di verifica dei backup, secondo le politiche stabilite in fase di scelta del controllo di sicurezza).

Mi piacerebbe ricevere pareri in merito (anche a favore!), sul blog o via email.

****

03- Standardizzazione: Sulla futura ISO/IEC 27002

Durante il meeting di Roma del WG1 dell'SC27, sono continuati i lavori sulla nuova ISO/IEC 27001, che dovrebbe uscire a ottobre 2013. La bozza attuale è meno criticata della bozza della 27001, ma i miei commenti non devono intendersi come definitivi, visto che neanche la norma lo è.

Premetto che non ho seguito i lavori perché impegnato sulla 27001. Le riflessioni che seguono riguardano solo lo stato di alcuni controlli:
- alcuni molto tecnici sono stati elminati (per esempio, quello sulla limitazione della connessione, visto che incorporato in altri sulla sicurezza della rete)
- molti controlli sono stati spostati di capitolo (per esempio, quello sul riesame indipendente di terze parti è stato accorpato con gli altri controlli sugli audit attualmente al A.15.2; il controllo sul ritiro degli asset è stato spostato nel capitolo sulla strumentazione e tolto dalla gestione delle risorse umane); non tutte le scelte mi sembrano convincenti (per esempio, il capitolo sulle comunicazioni è incastrato tra capitoli relativi a controlli informatici, quando le comunicazioni non sono necessariamente IT), ma in definitiva mi sembra che alcune cose siano migliorate (la separazione dei compiti è ora nell'organizzazione)
- si sono migliorate alcune dizioni (per esempio, non si parla più di mobile computing, ma di Mobile device policy)
- nuovi controlli con impatto sostanziale sono: Information security in project management, Restrictions on software installation, Secure development policy, System security testing (che sostituisce un controllo precedentemente meno orientato alla sicurezza), ICT Supply chain, Redundancies
- i capitoli sono dal 5 al 18 (la versione attuale va dal 5 al 12), ma solo in virtù di una diversa collocazione dei controlli
- non ho fatto il conto dei controlli previsti, rispetto ai 133 della versione del 2005.

Fabio Guasconi, Presidente SC27 di Uninfo, che ha seguito un po' i lavori, anche compatibilmente con il suo ruolo di ospite visto che l'incontro si è svolto a Roma, ha fatto i seguenti commenti:
- tantissimi commenti sono stati scartati (e nonostante ciò ci sono voluti 2 meeting per indirizzarli tutti);
- ci sono molti controlli nuovi e tanti con contenuti rivisti e aggiornati.

In definitiva, mi pare che verrà richiesto un certo sforzo nel rinumerare e rinominare i controlli degli attuali SOA, ma poco altro. Chi finora ha fatto un lavoro "furbo" (e spero l'abbia fatto, visto che l'esperienza di transizione dalla versione del 2000 a quella del 2005 dovrebbe essere servita) non dovrà dedicarci troppo tempo.

****

04- Standardizzazione: Verso la ISO 9001:2015. La posizione italiana

Franco Ferrari mi ha girato questo articolo sulla posizione italiana sulla futura ISO 9001, per la quale i lavori sono partiti a giugno 2012:
- http://www.uni.com/index.php?option=com_content&view=article&id=1686:verso-la-iso-90012015-la-posizione-italiana&catid=111:generale&Itemid=546

La posizione dell'UNI è, in sintesi, la seguente:
- il SGQ dovrebbe considerare l'intero sistema di esigenze ed aspettative, includendo temi relativi all'ambiente, alla sicurezza, alla responsabilità sociale, alla gestione dell'energia, alla privacy, eccetera; per questo dovrebbe essere più flessibile
- introdurre elementi di gestione del rischio;
- introdurre un approccio socialmente responsabile: aggiungere, oltre alla soddisfazione dei clienti, anche quella di altri stakeholder (la comunità, i dipendenti dell'impresa…).

Per una migliore applicabilità della norma, l'UNI propone le seguenti linee guida:
- riferimento nella politica per la qualità al contesto di riferimento e all'approccio generale alla qualità come parte degli orientamenti adottati nei confronti delle aspettative espresse dalle specifiche parti interessate;
- migliorare la semplicità e chiarezza
- introdurre un'appendice informativa che spieghi il significato e i motivi di ogni requisito

Ho riassunto parecchio e forse ho lasciato qualche spunto interessante. Ho comunque idea che molti degli argomenti ci siano già, tranne la considerazione di altri stakeholder e dei rischi. Questi temi dovrebbero essere introdotti grazie all'uso dell'Annex SL delle Direttive ISO per i sistemi di gestione.

Trovo che le riflessioni dell'UNI siano comunque interessanti. Purtroppo, come dice lo stesso documento dell'UNI in modo meno diretto, l'uso dello standard a mero scopo certificativo ha spinto le imprese ad adottarlo in modo rigido con esiti, in alcuni casi, dannosi. La colpa? Di tutti (imprese, consulenti, auditor), ovviamaente.

****
05- NIST SP 800-30 rev1 "Guide for conducting risk assessments"

Il NIST ha annunciato a fine settembre la pubblicazione della revisione 1 della NIST SP 800-30 dal titolo "Guide for conducting risk assessments".

La guida è molto interessante soprattutto perché stabilisce i diversi livelli a cui si possono condurre i risk assessment: strategico, tattico e operativo. Purtroppo l'ho letta dopo il meeting di Roma sulla ISO/IEC 27001, forse avrei avuto idee più chiare sul dibattito "Risk assessment nel planning o nelle operations?". Credo infatti che si confonda il ciclo PDCA con il modello di un'azienda a 3 livelli.

La guida, inoltre, promuove l'analisi dei rischi basata su minacce e vulnerabilità, mentre si prevede che la ISO/IEC 27001 ne farà a meno. Forse questa guida segnala che quest'ultima non sta prendendo la direzione giusta.

Mi piace molto anche il fatto che si consiglia di valutare la verosimiglianza delle minacce a partire dai loro agenti e dalle loro caratteristiche di interesse, capacità e obiettivi.

Ho segnato anche il punto sul riconoscimento dell'incertezza dell'analisi, da considerare e valutare opportunamente. Viene anche segnalato come la soggettività è sempre presente in questo campo e il fatto che la ripetibilità delle analisi qualitative può essere garantita dalla esplicitazione e documentazione delle ragioni per cui sono stati attribuiti certi valori (concetto che ho espresso in più occasioni io stesso; credo di averlo inconsciamente mutuato dagli stessi documenti a cui si è ispirato il NIST).

Al paragrafo 2.3.3, la guida descrive 3 possibili approcci: basati sulle minacce, sugli asset e gli impatti, sulle vulnerabilità. E' interessante, soprattutto perché le metodologie che vedo solitamente utilizzate sono del primo tipo.

****

06- Legale: Privacy e comunicazioni elettroniche: imprese ancora tutelate

Daniela Quetti mi ha segnalato il Provvedimento 262 del 20 settembre 2012 del Garante Privacy che afferma che, nonostante il Codice Privacy sia ora applicabile alle sole persone fisiche, il capo 1 del titolo X del Codice rimane applicabile anche alle persone giuridiche.

I requisiti del Capo 1 del Titolo X del Codice riguardano gli operatori di TLC e i loro abbonati (meglio: contraenti). In particolare, sono normati: la riservatezza dei dati dell'utente e gli apparati utilizzati, l'uso dei dati di traffico; la fatturazione di dettaglio; la visibilità o invisibilità del numero chiamante; i dati relativi all'ubicazione; il contrasto alle chiamate di disturbo; gli elenchi di abbonati.

Un ultimo aspetto è regolato da quel Capo: il registro delle opposizioni. Quindi, tale registro è valido anche per le imprese.

Per leggere il comunicato del Garante e il Provvedimento:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2094796
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2094932

****

07- Legale: DL 179/2012 per la crescita

Il 18 ottobre è stato approvato il DL 179/2012 "Ulteriori misure urgenti per la crescita del Paese" e si può scaricare da www.normattiva.it. Come tutti i Decreti Legge dovrà essere esaminato dalle Camere per la sua adozione definitiva e ciò potrà introdurre dei cambiamenti al testo attuale.

Tra gli aspetti più interessanti, a mio avviso, sono delle modifiche al Dlgs 82/2005 (il CAD o Codice dell'Amministrazione Digitale):
- il domicilio digitale del cittadino: "è facoltà di ogni cittadino indicare alla pubblica amministrazione un proprio indirizzo di posta elettronica certificata, quale suo domicilio digitale."
- l'obbligo per le pubbliche amministrazioni di accettare pagamenti via comunicazioni telematiche

Ci sono poi tanti altri temi, tra cui "Attuazione dell'Agenda digitale italiana", "Trasmissione telematica delle certificazioni di malattia nel settore pubblico", promozione per il trasporto pubblico dei sistemi di bigliettazione elettronica interoperabili a livello nazionale, "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario", "Giustizia digitale".

****

08- Legale: Certificazioni e avvalimenti

Un avvalimento, detto in poche parole, permette ad un'azienda che partecipa ad una gara di non avere tutti i requisiti richiesti, perché può indicare altre aziende "amiche" che li hanno al posto loro.

Detta così non sembra una procedura condivisibile, soprattutto se si parla di certificazioni di sistemi di gestione. E infatti, l'Autorità di Vigilanza sui Contratti Pubblici ha chiarito la sua posizione in questo senso.

La Determinazione dell'Autorità:
- http://www.avcp.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=5146

Il riassunto di Accredia:
- http://www.accredia.it/news_detail.jsp?ID_NEWS=986>emplate=default.jsp&ID_AREA=10

Ringrazio l'organismo di certificazione NQA per la notizia.

****

09- L'audit non aggiunge valore

Finalmente qualcuno che scrive che l'audit ISO 9001 non fornisce valore aggiunto. Io sono un vile e mi limito a dirlo a pochi intimi:
- http://www.irca.org/en-gb/resources/INform/archive/Issue37/opinion/?utm_source=Email&utm_medium=Inform&utm_campaign=Nov_12

Cosa dice, in sostanza, l'autore David Hutchins:
- l'audit è condotto verificando che processi e attività siano condotti secondo quanto prescritto; trovare disallineamenti non vuol dire "aggiungere valore"
- il significato attribuito a "valore aggiunto" dall'auditor può non coincidere con lo stesso significato attribuito dagli altri stakeholder
- è ridicolo pensare che, nei ridotti tempi di audit e con competenze spesso inadeguate, l'auditor abbia la pretesa di dare valore aggiunto.

Ormai, perso ogni freno inibitore, lo dico: sono d'accordo!

****
10- COIT, BYOD, strumenti mobili: rapporti di ENISA e FBI

Dalla newsletter del Clusit, leggo la notizia che ENISA ha pubblicato il report "Consumerization of IT: Top Risks and Opportunities".

Da questo ho imparato che la "Consumerization of IT (COIT)" o "IT aziendale guidato dal consumatore" riguarda l'uso per attività aziendali di strumenti hardware e software personali e che il BYOD (bring your own device) ne è una parte, perché riguarda solo l'uso di hardware personale. Dal BYOD sono esclusi, per esempio, gli account personali Facebook, LinkedIn o Dropbox utilizzati per raccolta o trasmissione di informazioni aziendali o per conto dell'azienda.

ENISA ha quindi elencato i rischi maggiori del COIT (riassumo):
- danneggiamento dell'immagine aziendale per uso non controllato di servizi IT
- aumento dei costi di manutenzione degli strumenti IT a causa della loro disomogeneità
- perdita degli strumenti
- potenziali cause con il personale a causa della non chiara distinzione tra dati aziendali e dati dell'utente
- perdita di riservatezza delle informazioni a causa di errori degli utenti nell'uso di applicazioni di sharing
- perdita di riservatezza delle informazioni a causa di accesso non autorizzato di malintenzionati

Per chi volesse approfondire:
- https://www.enisa.europa.eu/media/press-releases/workplace-it-enisa-sees-opportunities-and-risks-in-201cbring-your-own-device201d-trend

Su Nòva 24Ore è anche apparsa la notizia che l'FBI ha emesso delle linee guida per la protezione dei dispositivi mobili.

Trovate l'articolo del 24 Ore e un riassunto delle linee guida dell'FBI a questo indirizzo:
- http://www.ilsole24ore.com/art/tecnologie/2012-10-27/quei-virus-compagni-viaggio-172025.shtml?uuid=AbHpjSxG

La pagina web dell'FBI con la notizia dovrebbe essere questa:
- https://www.fbi.gov/sandiego/press-releases/2012/smartphone-users-should-be-aware-of-malware-targeting-mobile-devices-and-the-safety-measures-to-help-avoid-compromise

****

11- Vulnerabilità alla IEEE

Questa notizia me l'ha data Sandro Sanna:
- http://www.ilsole24ore.com/art/tecnologie/2012-09-26/falla-sistema-sicurezza-ieee-192130.shtml?uuid=AbSioBkG

In breve: su un ftp server erano conservati dei log con anche delle user-id e password non cifrate.

Purtroppo, il solito mix di incompetenza, disattenzione e superficialità.

Il fatto che sia coinvolta la IEEE dà solo più colore alla notizia. Il cui significato finale rimane quello di dover sensibilizzare l'IT.

****
12- Firme digitali: SHA-3

Il "nuovo" algoritmo per le firme digitali, che sostituirà lo SHA-2, è nato e si chiama in modo poco originale SHA-3:
- http://csrc.nist.gov/groups/ST/hash/policy.html

Il punto di riferimento è lo statunitense NIST. Ha dato l'annuncio della scelta dell'algoritmo di hashing (Keccak) a inizio ottobre:
- http://csrc.nist.gov/groups/ST/hash/sha-3/winner_sha-3.html

Come si vede dalle pagine del NIST, non c'è ancora la necessità di migrare al nuovo algoritmo.

La notizia l'ho avuta dalla newsletter Crypto-Gram, in cui Bruce Schneier fa anche notare come l'attuale SHA-512 sia ancora da considerare sicuro:
- https://www.schneier.com/blog/archives/2012/09/sha-3_will_be_a.html