



Associazione Italiana
Information Systems Auditors



Ottobre 2009

Il trentesimo anniversario della nostra Associazione

Questa newsletter sarà in distribuzione proprio nella settimana nella quale ricorre il 30° anniversario. Come già annunciato, i soci potranno ritrovarsi nelle tre sedi (Milano, Roma e Torino) per festeggiare insieme in occasione delle Sessioni di Studio contemporanee.

Nell'augurare ad AIEA un futuro denso di iniziative, ringraziamo tutti i nostri soci che, collaborando con noi, permettono all'Associazione di intraprendere sempre nuove iniziative.

Come già anticipato, la data sarà "celebrata" con tre Sessioni di Studio, contemporanee, tenute nelle sedi di Milano, Roma e Torino. Le sessioni, oltre ad essere l'occasione di ascoltare relatori di alto livello che parleranno su temi ed esperienze attuali, permetteranno di festeggiare e brindare tutti insieme! Nel corso della sessione, ai soci sarà consegnata una maglietta (polo) con il logo del 30°!

Ha avuto, inoltre, un buon riscontro l'iniziativa promozionale, avviata da AIEA in occasione del 30° anniversario, dello sconto del 30% sulle quote di iscrizione ai corsi CISA, CISM

AIEA parteciperà.....

Il Vicepresidente Orillo Narduzzo interverrà all'incontro promosso da AUSED sul tema "L'evoluzione dei framework ITIL e COBIT e loro utilizzo innovativo nelle aree della compliance e del risk assessment" con una relazione sullo stato dell'arte del framework COBIT® e sulle sue recenti evoluzioni.

L'incontro avrà luogo a Milano, giovedì 22 ottobre 2009 alle ore 14.

Per ulteriori informazioni consultare il sito www.apsed.org.

Il prossimo 26 ottobre a Milano, AIEA terrà una relazione per una delegazione di 18 auditor cinesi, funzionari della pubblica amministrazione. L'iniziativa è frutto di un accordo con ASIAPROMOTION, struttura che si occupa della promozione di contatti culturali e lo sviluppo delle relazioni tra paesi europei ed asiatici. La delegazione è organizzata dal governo cinese nell'ambito del programma di formazione di esperti in paesi stranieri ed è interessata ad approfondire l'impostazione dell'audit in Italia (norme di riferimento, modelli organizzativi adottati nelle aziende, strumenti di supporto utilizzati, ecc.). La relazione sarà tenuta dal nostro socio Luigi Vedani.

Il nuovo Consiglio Direttivo

Il 31 dicembre scade il mandato dell'attuale CD e, quindi, a breve daremo inizio alla procedura di rinnovo e raccoglieremo le candidature.

Distribuzione guide

Nella sessione dell'8 ottobre è stata distribuita la nostra guida n.ro 6 "Business Continuity Management & Auditing", frutto dell'impegno del Gruppo di Ricerca, coordinato, con grande impegno, dal nostro socio Massimiliano Nulli o Rinalducci. Al Gruppo hanno partecipato anche soci di Aused e Anssaif.



La guida si propone di contribuire ad affrontare la tematica della continuità operativa, lato gestione e lato audit, con un approccio basato, principalmente, sull'esperienza dei relatori, e con un doveroso riferimento alla normativa e agli standard presenti in materia.

Tra qualche settimana sarà disponibile anche la guida n.ro 5 "I legami tra gli obiettivi aziendali e i processi secondo il framework COBIT". Lo studio formalizza la ricerca, commissionata nel 2008 da AIEA a Bocconi, che ha visto la partecipazione di Protiviti

Gruppi di Ricerca

Gruppo di Lavoro "Traduzione Cobit 4.1"

In questi mesi è stato sottoscritto con ISACA un accordo per pubblicare la traduzione di COBIT 4.1 sul sito di ISACA, assieme a quelle in Spagnolo e in Russo rilasciate nel mese di luglio 2009. Stiamo pertanto rivedendo l'editing secondo le indicazioni di ISACA e completando l'attività di controllo qualità. Nell'Area Download del sito si trovano l'"Executive Summary" ed alcuni processi

CobIT e legge 262

Il Gruppo di Ricerca AIEA è articolato in 6 sottogruppi chiamati Focus Group.

I partecipanti alla ricerca sono ben 17 soci divisi in 6 Focus Group i cui Relatori sono:

Alessandro Arca (FG5)

Giuliano Flesia (FG4)

Luca Nurisso (FG1 e FG6)

Dino Ponghetti (FG3)

Luca Turri (FG2)

Le tematiche dei Focus Group sono le seguenti:

FG1: Introduzione e normativa di riferimento

FG2: Dimensionamento delle verifiche e analisi dei rischi

FG3: Controlli generali

FG4: Controlli applicativi

FG5: Campionamenti

FG6: Valutazione del sistema di controllo e attestazioni finali

Le relazioni dei Focus Group 1, 2, 3, 4 e 6 sono giunte alla finalizzazione, come da programma, entro l'estate ed ora passano alla fase di convalidazione fra tutti i partecipanti al GdR; tale fase dovrà concludersi entro due mesi lavorativi e pertanto entro l'autunno, considerato il periodo di ferie estive. L'attività del Focus Group 5 è in svolgimento e si prevede che sarà ultimata essa pure entro l'autunno

Gruppo di Lavoro "Traduzione Val IT 2.0"

Sta lavorando, con il coordinamento di Guido Leone, il Gruppo di Lavoro che si occupa della traduzione della versione aggiornata di Val IT 2.0. In particolare delle seguenti pubblicazioni:

Enterprise Value:Governance of IT Investments - The Business Case



Associazione Italiana
Information Systems Auditors



Enterprise Value: Governance of IT Investments - Getting Started with Value Management
Enterprise Value: Governance of IT Investments - The Val IT Framework 2.0
Sono stati rilasciati, in occasione del convegno di Pisa, i primi due documenti.

Dopo il rilascio, in occasione del convegno di Pisa, dei primi due documenti, ora è in corso la traduzione del terzo ("The Val IT Framework 2.0"), il rilascio della quale è previsto per l'ultimo trimestre dell'anno.

La traduzione è entrata nella fase finale di controllo qualità.

La traduzione completa costituirà una **nuova Guida AIEA**

Riceviamo da ISACA

Renew your 2010 ISACA Membership online – easily & securely

Da:
"ISACA_News" <sbalazs@isaca.org>

ISACA is pleased to announce that online renewals are now available for the upcoming year - 2010! Members requested that renewals open earlier than normal to take advantage of available existing corporate funds.

2010 promises to be a very exciting year with the debut of a completely updated and dynamic ISACA.org web site where you can strengthen your professional knowledge and connections.

Get a jump on 2010 and ensure your member benefits continue uninterrupted through 31 December 2010 - Renew today!

To renew online - simply and securely, please login to www.isaca.org with your personalized login credentials. This will place you within "My ISACA" where a link to "My Renewals" is provided in the left-hand navigation menu. You will also have the opportunity to renew your certification during this process. For login assistance, please visit www.isaca.org/login.

Thank you.



Calendario Eventi AIEA

Ottobre 2009

8.....Milano – Roma – Torino: sessioni di studio
20-21.....Roma – Corso base COBIT

Novembre 2009

16-17.....Roma – Corso avanzato COBIT

I prossimi eventi di AIEA

Calendar of Events

Dates of conferences/events are indicated in **RED**; other dates and deadlines are indicated in **BLACK**.

October

14-16 October **IT Governance, Risk and Compliance Conference**,
Henderson, Nevada, USA

November

2-6 November **ISACA Training Week**, San Francisco, California,
USA
9-11 November **Information Security and Risk Management Conference**,
Amsterdam, The Netherlands

I prossimi eventi ISACA:

Avviso ai soci 1

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo, azienda di appartenenza o altro...) di comunicare i nuovi dati in segreteria aiea@aiea.it. La mancanza di tali comunicazioni potrebbero impedire, al socio, la ricezione delle comunicazioni.

Avviso ai soci 2

E' in linea, sulla homepage del sito, il calendario degli eventi AIEA.

Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2009 sia nelle Sessioni di Studio sia in Workshop.

Chi volesse dare il proprio contributo, è pregato inviare una mail a aiea@aiea.it, specificando, nell'oggetto "ARGOMENTI DI INTERESSE"

In una successiva newsletter provvederemo ad elencare tutti i temi proposti.

Partecipazione di soci ad eventi

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da segnalare ad esempio nella newsletter.



Associazione Italiana
Information Systems Auditors



In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIEA. La partecipazione dell'Associazione ad un evento “deve” però essere decisa dal Consiglio Direttivo: siete quindi pregati di contattare il CD con ragionevole anticipo! In caso non fosse possibile la partecipazione a nome AIEA, vi invitiamo ad indicare, nel profilo professionale la vostra appartenenza ad AIEA, Capitolo di ISACA

Bibliografia

E' on line il nuovo numero di InterLex (<http://www.interlex.it>)

Vi informiamo che sul sito www.cnipa.it sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo che alla stesura di numerosi documenti hanno partecipato diversi nostri soci e che inoltre CNIPA organizza incontri o seminari aperti anche ai soci AIEA.

Le Newsletter delle altre Associazioni

- ✚ E' disponibile on line, la **Newsletter CLUSIT** del 30 settembre 2009 (disponibile in PDF all'indirizzo www.clusit.IT/newsletter_30_09_09.pdf)
- ✚ Sono disponibili e qui allegate le Newsletter n.ro 338 del Garante Privacy
- ✚ E' disponibile on line, la **Newsletter ANSSAIF** all'indirizzo www.anssaif.it
- ✚ E' disponibile on line, la **Newsletter AIPSI** all'indirizzo www.aipsi.org/newsletter



- BANCHE: DATI DEI CLIENTI PIU' PROTETTI
- NO A DATI SANITARI ON LINE
- DISABILI: PER IL BUONO SOCIALE SOLO DATI INDISPENSABILI
- NO ALLE TARGHE DELLE AUTO NELLA BACHECA CONDOMINIALE

Banche: dati dei clienti più protetti

Gli accessi non autorizzati devono essere tempestivamente comunicati al titolare del conto

La banca deve proteggere con particolare attenzione i dati della clientela e deve dare immediata notizia al titolare del conto di eventuali accessi ingiustificati, anche se effettuati da propri dipendenti, alle informazioni riguardanti il conto corrente.

E' quanto ha stabilito il Garante per la privacy, con un provvedimento di cui è stato relatore Mauro Paissan, affrontando il caso di una signora che lamentava il trattamento illecito dei suoi dati personali da parte della propria banca. Nell'ambito di una causa di separazione, il marito aveva infatti prodotto una memoria contenente informazioni, relative a un conto corrente, che solo la donna stessa o il personale della filiale presso la quale aveva aperto il conto potevano conoscere.

Alla scoperta della violazione, la cliente si era subito rivolta all'istituto di credito per chiedere chi avesse avuto accesso ai dati, comunicandoli poi all'esterno. L'istituto bancario aveva inizialmente negato i fatti e solo in seguito a ulteriori richieste della donna, ammetteva che un dipendente aveva prima consultato senza giustificate "esigenze operative" i conti correnti della segnalante e poi inoltrato i dati a un altro funzionario del gruppo bancario. A causa del loro comportamento, entrambi i lavoratori erano stati temporaneamente sospesi dal lavoro.

La donna si era nel frattempo rivolta anche al Garante. Gli accertamenti dell'Autorità hanno messo in luce che la banca aveva sì adottato misure di sicurezza ma non sufficienti a impedire il trattamento non consentito dei dati del conto corrente. L'istituto di credito, inoltre, pur avendo rilevato l'accesso non autorizzato ai conti della sua cliente, non l'aveva tempestivamente avvertita, con ciò violando il principio di correttezza. La tempestiva informazione avrebbe, infatti, potuto consentire alla correntista perlomeno di ridurre i rischi derivanti dall'indebita divulgazione dei dati del suo conto.

L'Autorità ha prescritto al gruppo bancario di adottare misure di sicurezza idonee a garantire la scrupolosa vigilanza sull'operato degli incaricati, e di sensibilizzare i

funzionari al rigoroso rispetto delle norme sulla privacy attraverso attività di formazione. Ha inoltre stabilito che la banca, una volta acquisita la conoscenza di accessi non autorizzati ai dati della clientela, inclusi quelli eventualmente effettuati dai suoi dipendenti, è tenuta a comunicarlo tempestivamente agli interessati.

L'Autorità ha infine disposto la trasmissione del provvedimento alla Procura della Repubblica per le valutazioni di competenza riguardo a eventuali illeciti penali commessi.

No a dati sanitari on line

Il Garante blocca la diffusione dei dati di una dipendente pubblicati sul sito di una provincia

Il Garante privacy blocca la diffusione di dati sanitari di una dipendente provinciale pubblicati sul sito dell'ente locale e liberamente reperibili in Internet.

Il provvedimento di blocco (relatore Giuseppe Fortunato) è scattato a seguito della segnalazione della dipendente che, attraverso un motore di ricerca, aveva rinvenuto on line alcuni atti della provincia in cui erano riportati i suoi dati anagrafici e delicate informazioni sul suo stato di salute, la cui diffusione è vietata dal Codice privacy. Risultato confermato dagli accertamenti del Garante: due delibere del responsabile delle risorse umane della provincia relative ad una richiesta di riconoscimento di infermità per causa di servizio avanzata dalla donna erano, infatti, non solo direttamente visualizzabili sul sito istituzionale dell'ente ma erano anche liberamente accessibili attraverso il motore di ricerca. Uno dei documenti riportava, inoltre, accanto al nome e cognome della dipendente, il giudizio medico legale con il tipo di infermità riscontrata.

Nel disporre il blocco dei dati sanitari trattati in modo illecito, l'Autorità ha ribadito il principio che le amministrazioni locali, fermo restando il rispetto degli obblighi di legge sulla trasparenza delle deliberazioni dell'ente, devono selezionare con estrema attenzione i dati personali da diffondere, non solo alla luce dei principi di pertinenza, non eccedenza e indispensabilità rispetto alle finalità perseguite dai singoli provvedimenti, ma anche in relazione al divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Disabili: per il buono sociale solo dati indispensabili

Il Garante fa “sanare” un bando prima della chiusura del procedimento

Una persona anziana o un disabile che presenta una domanda per l’assegnazione di un “buono sociale” erogato dal comune non deve essere costretto a specificare le malattie di cui soffre, i ricoveri e gli esami effettuati. Per poter partecipare alla selezione è sufficiente certificare solo il grado di invalidità e il livello di indipendenza nello svolgere le attività elementari della vita quotidiana.

E’ bastato l’avvio di un’istruttoria da parte del Garante per far sì che un’azienda che gestisce i servizi socio sanitari per un insieme di enti locali, modificasse nei termini indicati, il bando per l’erogazione di “buoni sociali” a favore di categorie svantaggiate. Il caso era stato segnalato al Garante da un cittadino che aveva espresso dubbi sulla legittimità delle procedure indicate nel bando. Per poter partecipare alla selezione, infatti, anziani e disabili dovevano inoltrare una domanda al proprio comune di residenza corredata dalla copia del verbale di riconoscimento di invalidità civile, completa della relativa documentazione (patologie, diagnosi, ricoveri, esami) e da una valutazione analitica del livello di indipendenza della persona, accertata dal medico curante attraverso dei test. La documentazione veniva poi trasferita dai comuni all’azienda.

Nel corso degli accertamenti il Garante ha ribadito che gli enti che perseguono finalità di rilevante interesse pubblico, siano esse aziende socio-sanitarie, socio-assistenziali o socio-educative, sono tenuti a richiedere e ad utilizzare dati sanitari solo se pertinenti e indispensabili allo svolgimento delle proprie funzioni istituzionali ed ha quindi sollecitato l’azienda a rivedere il tipo di dati richiesti.

L’azienda ha assicurato al Garante la modifica del regolamento dei bandi futuri e che, di conseguenza, agli interessati verranno richiesti solo la percentuale di invalidità e il punteggio complessivo raggiunto nella valutazione del livello di indipendenza.

No alle targhe delle auto nella bacheca condominiale

Nella bacheca condominiale accessibile al pubblico non possono essere affissi avvisi contenenti dati che rendano identificabili anche indirettamente i condomini, come ad esempio le targhe delle automobili.

È il principio ribadito dal Garante nell’accogliere la segnalazione di alcuni residenti in un condominio milanese che lamentavano un’indebita divulgazione di dati personali dovuta all’affissione nella bacheca del

palazzo di un avviso di rimozione delle auto ancora parcheggiate nel cortile comune, area destinata da una delibera assembleare alla costruzione di posti auto interrati. Nella bacheca oltre all’avviso, che conteneva targhe e numero dell’area di sosta assegnata a ciascuno dei condomini, erano state affisse anche le foto delle autovetture. Un insieme di dati, secondo i segnalanti, in grado di renderli identificabili sia dagli altri residenti che da terzi in transito nelle aree comuni. I condomini contestavano, inoltre, il fatto che una serie di informazioni ad essi riferite, tra cui la loro condizione di inadempienza alla delibera assembleare, fossero state riportate dall’amministratore in una lettera inviata all’avvocato di fiducia del condominio ed alle ditte incaricate di svolgere i lavori.

L’Autorità, con un provvedimento di cui è stato relatore Giuseppe Fortunato, ha prescritto all’amministrazione condominiale di utilizzare comunicazioni individuali per gli avvisi relativi alla gestione comune che non siano di carattere generale. Il Garante ha infatti ritenuto l’esposizione in bacheca dell’avviso contenente informazioni relative ai condomini una modalità eccessivamente invasiva e non giustificata dalle esigenze di contenimento di spesa adottate dall’amministratore, oltre che non conforme a quanto previsto dalla disciplina in materia di protezione dei dati personali. L’Autorità ha inoltre vietato al condominio l’ulteriore comunicazione a soggetti terzi di dati personali riferiti ai segnalanti ad eccezione di quella destinata al legale di fiducia.

L’attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall’Autorità

Fascicolo sanitario elettronico: il Garante approva le Linee guida – Comunicato del 11.8.2009

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it