



Associazione Italiana  
Information Systems Auditors



### **Convocazione di Assemblea**

Nei giorni scorsi, i soci sono stati informati dell'Assemblea convocata, a Milano, per il giorno 13 febbraio (seconda convocazione).

La convocazione di una Assemblea, anche in aggiunta rispetto a quella annuale di fine esercizio, è un obbligo statutario che incombe sul Consiglio Direttivo quando il Consiglio intenda dare corso ad una iniziativa che rappresenti per l'AIEA un evento che per rilevanza sia definito attività di straordinaria amministrazione. L'ordine del giorno indica i due argomenti importanti e urgenti che l'Assemblea è chiamata a valutare: il progetto di ricerca sull'IT Governance e l'opportunità di investire talune risorse liquide disponibili in modo più remunerativo.

Relativamente al progetto di ricerca, abbiamo il piacere di anticipare ai soci che, secondo le linee strategiche indicate da ISACA, il Consiglio Direttivo intende dare corso alle attività di sviluppo AIEA nell'IT Governance, con una iniziativa e connesso investimento che qualifichi la nostra Associazione come leader nel mercato italiano. La ricerca, per complessità e visibilità, dovrà essere commissionata a primario istituto di ricerca accademico e impone una partenza immediata al fine di concludere l'anno 2008 con un risultato tangibile e idoneo a costituire base per le nostre future attività formative e informative su tale comparto.

L'Assemblea sarà anche un'occasione per partecipare ad una "edizione speciale" di una Sessione di Studio, con due interessanti relazioni, al termine della quale, ai soci presenti, sarà distribuito il secondo volume della collana di pubblicazioni "Guide AIEA": Valore d'impresa: la governance degli investimenti nell'IT.

### **Il prossimo Convegno Nazionale**

Possiamo confermare quanto anticipato nelle settimane scorse: il **convegno annuale AIEA** sarà tenuto, quest'anno, a Parma, nei giorni 29 e 30 maggio.

### **Notizie dai Gruppi di Lavoro**

#### ***Gruppo di lavoro "SOX2"***

Il Gruppo di Lavoro "Sarbanes Oxley 2" ha concluso i lavori. Il documento originale è stato completamente tradotto ed è terminato anche il controllo qualità. Il documento è in fase di stampa e sarà reso disponibile ai soci entro questo mese.

#### ***Gruppo di Ricerca "COBIT 4.1 - Iso 27001"***

Il Gruppo di Ricerca ha concluso i lavori ed il documento finale è in fase di "controllo qualità". Di seguito viene brevemente descritto lo scopo del documento.

*Negli ultimi anni si è assistito ad una crescente proposta di metodologie e standard che rispondono all'obiettivo di individuare le 'best practices' e le regole dell'area oggetto di studio.*

*Il documento si propone di contribuire ad un confronto fra COBIT 4.0 e ISO 27001 e si caratterizza per il ricorso ad una tecnica di valutazione quantitativa, ritenuta indispensabile*



*per garantire un metodo condiviso, obiettivo e ripetibile di valutazione e per l'inclusione, ai fini del confronto, dei Cap. 4-8 di ISO 27001, che costituiscono una parte essenziale dello standard.*

*Le novità introdotte da COBIT 4.1 rispetto a COBIT 4.0 influenzano in modo molto marginale la mappatura attuale che quindi, in attesa di una revisione, può essere ritenuta valida anche per CobiT 4.1.*

#### **Gruppo di Lavoro "Traduzione COBIT 4.1"**

La traduzione è stata ultimata e sono in corso sia il controllo qualità sia l'editing finale.

Non è stato possibile concludere il lavoro entro il 2007, come da pianificazione iniziale, sia a causa di altri impegni dei componenti il gruppo, sia per la lunga discussione che si è creata su alcuni termini.

Per rendere fruibile il lavoro quanto prima, il documento verrà rilasciato per Domini.

#### **Disponibile il documento "White Paper "COBIT® e ITIL®, due framework compatibili".**

E' stato pubblicato il white paper "COBIT® e ITIL®, due framework compatibili". Il documento, risultato della collaborazione attiva tra AIEA, itSMF Italia e SDA Bocconi, è un'utile guida per comprendere come utilizzare congiuntamente e proficuamente due tra i più importanti ed affermati framework per il governo e la gestione dell'IT. In particolare identifica chiaramente le aree di sinergia e, per esse, illustra quali parti dei modelli utilizzare in modo integrato e con quale approccio.

Utili esempi pratici, sviluppati per specifiche aree di processo, completano lo sviluppo teorico degli argomenti. Il documento è anche un'utile guida per chi desidera una panoramica dei principali framework per la gestione dell'IT, oltre a COBIT e ITIL, e fornisce per questi ultimi una guida introduttiva per chi si avvicinasse ad essi per la prima volta.

Hanno contribuito per AIEA: Orillo Narduzzo, Andrea Pederiva, Stefano Niccolini.

Il white paper è disponibile solo per gli associati, chi lo desidera può inviare la richiesta alla segreteria AIEA presso [aiea@aiea.it](mailto:aiea@aiea.it).

#### **Esame CISA e CISM**

Ricordiamo che i risultati dell'esame saranno comunicati, direttamente agli interessati, entro il mese di febbraio.

Sul sito [www.isaca.org](http://www.isaca.org) è già possibile l'iscrizione on-line all'esame di giugno 2008.

#### **AIEA è presente a...**

Per il sesto anno consecutivo, AIEA si è svolta a Lugano, in collaborazione con ATED e il chapter svizzero, una Sessione di Studio sul tema IT Governance., nella quale Silvano Ongetta ha aperto i lavori. Ottimi relatori e buona la partecipazione, anche di soci provenienti dalla Lombardia. Ricordiamo che erano preseni quasi tutti i soci svizzeri che aderiscono all'AIEA. Le relazioni, come sempre, sono a disposizione dei soci sul sito di AIEA.



## I prossimi eventi di AIEA

### Calendario Eventi AIEA

#### Febbraio

- 11 ..... Milano - Inizio corso Lead Auditor
- 13 ..... Milano - **Sessione di Studio**
- 22 ..... Milano - Inizio corso CISA
- 22 ..... Torino - Inizio corso CISA
- 29 ..... Roma - Inizio corso CISA
- 29 ..... Roma - **Sessione di Studio**

#### Marzo

- 3 ..... Milano - Inizio corso ITIL Foundation
- 11 ..... Milano - Inizio corso COBIT Base
- 13 ..... Torino - **Sessione di Studio**

#### Aprile

- 1 ..... Roma - **Sessione di Studio**
- 2 ..... Milano - **Sessione di Studio**
- 4 ..... Milano - Inizio corso CISM
- 7 ..... Roma - Inizio corso ITIL Foundation
- 10 ..... Torino - **Sessione di Studio**
- 14 ..... Milano - Inizio corso COBIT Avanzato
- 18 ..... Roma - Inizio corso CISM

## Notizie da ISACA

Riceviamo da ISACA:

### ISACA Benefit of the Month



#### Member Benefit of the Month: **JournalOnline**

JournalOnline (JOnline) is the online-only counterpart to the *Information Systems Control Journal*. Articles included in JOnline undergo the same rigorous peer-review process as those in the print version of the *Journal*. JOnline articles are available exclusively to ISACA members for one year. JOnline is updated bimonthly on the first business day of the month in which no print *Journal* is released (February, April, June, August, October and December). Members receive an e-mail announcing the articles' availability once they are posted. All JOnline articles are available in HTML and PDF at [www.isaca.org/journalonline](http://www.isaca.org/journalonline).



## Calendar of Events

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

### February

- 13 February ..... Early-bird registration deadline for June 2008 CISA and CISM exams and 2008 North America CACS
- 25-29 February ..... **ISACA<sup>®</sup> Training Week**  
Atlanta, Georgia, USA
- 28 February ..... Deadline to submit nominations for 2008-09 International BoD

### March

- 9-12 March ..... **EuroCACS**  
Stockholm, Sweden
- 21 March.....Deadline to submit articles for consideration for vol. 4, 2008, of the *Information Systems Control Journal*
- 28 March.....Deadline to submit Invitation to Participate application

Ricordiamo i prossimi eventi ISACA:

### ISACA e Balanced Score Card

ISACA ha messo a punto e divulgato ai vari Capitoli il contenuto del Chapter BSC (Balanced Score Card) Otto sono gli obiettivi strategici con vari sotto obiettivi. Per ciascun obiettivo, è stato messo a punto un sistema per misurarne l'implementazione. Tutti i Capitoli, quindi, avranno sia un sistema unico di reporting ad ISACA, sia uno strumento per una migliore pianificazione interna. Tutto il CD sta già lavorando per la compilazione della documentazione che dovrà essere fornita, ad ISACA, il prossimo luglio.

### Il sito AIEA

Continua la nostra lettura di chi, come e quando, accede al nostro sito. Le visite totali sono arrivate a 82.000.

Questa volta abbiamo paragonato l'andamento degli ultimi 6 mesi

Media giornaliera Visite	42	(lun-ven): 52	(sab-dom): 14
--------------------------	----	---------------	---------------

### Dettagli

Mese	Visite	Variazione	Mese	Visite	Variazione
<a href="#">Agosto 2007</a>	865		<a href="#">Dicembre 2007</a>	967	-33,7%
<a href="#">Settembre 2007</a>	1.390	+60,7%	<a href="#">Gennaio 2008</a>	1.563	+61,6%
<a href="#">Ottobre 2007</a>	1.552	+11,7%	<a href="#">Febbraio 2008</a>	278	
<a href="#">Novembre 2007</a>	1.459	-6,0%			

Di seguito la percentuale dei paesi di provenienza, sul totale degli accessi di gennaio:



■ Italia	90,20 %
■ Regno Unito	3,92 %
■ Germania	1,96 %
■ Stati Uniti d'America	1,96 %
■ Svizzera	1,96 %

### **Avviso ai soci**

Con l'obiettivo di coinvolgere nella vita associativa tutti i soci, invitiamo i lettori a fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2008 sia nelle Sessioni di studio sia in Workshop.

Chi volesse dare il proprio contributo, è pregato inviare una mail a [aiea@aiea.it](mailto: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.

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!

### **Bibliografia**

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

Vi informiamo che sul sito [www.cnipa.it](http://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.



AIPSI - Associazione Italiana Professionisti di Sicurezza Informatica

**ESTRATTO Newsletter numero 18, 29 gennaio 2008**

Disponibile in PDF all'indirizzo

[http://www.aipsi.org/newsletter/Aipsi\\_NewsLetter-19-2008\\_1.pdf](http://www.aipsi.org/newsletter/Aipsi_NewsLetter-19-2008_1.pdf)

-----  
## Attività dell'Associazione ##  
-----

- AIPSI a CiscoExpo 2008 - Milano, 26 e 27 febbraio 2008 presso: ATA Quark Hotel, via Lampedusa 11/a

AIPSI, come lo scorso anno offre il proprio patrocinio a CiscoExpo, partecipandovi con la propria presenza. L'evento avrà luogo presso l'ATA Hotel Quark a Milano nei giorni 26 e 27 Febbraio. CiscoExpo è una due giorni dedicata ad aziende e professionisti del settore ICT con focalizzazione su aspetti business e tecnologici. La traccia di Sicurezza, nella giornata del 26 febbraio, offre la possibilità di guadagnare punti (CPE) atti al mantenimento delle certificazioni professionali. I crediti possono essere richiesti a [info@aipsi.org](mailto:info@aipsi.org).

La partecipazione alla manifestazione è gratuita previa registrazione sul sito: [www.ciscoexpo.it](http://www.ciscoexpo.it)

- SICUREZZA INFORMATICA: RISCHI E CONTROMISURE

Ferrara, Sala Estense, 15 marzo 2008, h 10.00

AIPSI, con il patrocinio del Comune di Ferrara e dell'Ordine e Fondazione degli Ingegneri di Ferrara, organizza il convegno: SICUREZZA INFORMATICA: RISCHI E CONTROMISURE

- Sicurezza e Assicurazioni:

Nell'ambito di incontri con professionals del settore Assicurativo è emersa la possibilità di offrire ai soci AIPSI la: - Polizza di Tutela Legale per i professionisti ed i consulenti dell'IT, da studiare con ISI Insurance del Gruppo Assicurativo Arca (compagnia specializzata nella Difesa Legale): un prodotto assicurativo di Tutela Legale studiato per le necessità del settore.

- Gruppo AIPSI su LinkedIn

I membri AIPSI possono aderire al gruppo AIPSI su LinkedIn.

Il link da seguire è il seguente:

<http://www.linkedin.com/e/gis/37056/73BAA1072F68>

-----  
## ISSA News ##  
-----

- Win a Full Conference Pass to RSA: Enter By January 31 for 1st Drawing ISSA International has 4 complimentary full conference passes available for active ISSA members to attend RSA USA, scheduled for April 7-11 in San Francisco. You can enter to win one of these passes by



---

Associazione Italiana  
Information Systems Auditors

---



completing the entry form on the ISSA website, <https://www.issa.org/Members/RSAContest.php>.  
Your ISSA ID number and password are required for log in.

Drawings will take place on February 1, 15 and 29 with a single winner on each of the first two dates and two winners on February 29. You only need to enter once to be included in all subsequent drawings. Those selected will receive email notification from ISSA International following each drawing. Results will be announced in eNews. Winners will be responsible for their own transportation, lodging and incidental expenses.



CLUSIT ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA  
31 gennaio 2008 – ESTRATTO Newsletter CLUSIT - [www.clusit.it](http://www.clusit.it)

[disponibile in PDF all'indirizzo  
[www.clusit.it/newsletter\\_31\\_01\\_08.pdf](http://www.clusit.it/newsletter_31_01_08.pdf)]

=====

## CYBERCRIME

=====

Il worm Storm si evolve.

L'attacco del worm Storm prosegue, e si conferma come uno degli worm più persistenti degli ultimi anni.

Come riportato da Network World

[[www.networkworld.com/news/2007/122807-storm-switches-tactics-third-time.html](http://www.networkworld.com/news/2007/122807-storm-switches-tactics-third-time.html)], Storm continua ad evolvere aggiungendo nuove minacce (in particolare un rootkit) ed incrementando la propria pericolosità.

Per quanto, come scrive NW, il rootkit installato da Storm è relativamente "vecchio", e quindi rilevabile da alcuni software di sicurezza (anche se non si dice da quali, e quali versioni), non è un problema da sottovalutare.

Invitiamo quindi nuovamente i nostri lettori alla massima cautela, e a trattare i messaggi di posta elettronica "sospetti" con grande attenzione.

(Autore: Mauro Cicognini)

-----

Campioni del mondo ma perdenti nel quotidiano. Un incidente informatico al Tribunale di Genova riporta alla cruda realtà: vinciamo i campionati del mondo di security ma non difendiamo le risorse preziose che abbiamo attorno a noi.

L'ho detto su Nova100

<http://gigitagliapietra.nova100.ilsole24ore.com/2008/01/e-se-non-fo>

sser.html), si dice "intrusione di hacker" ma ho l'impressione che sia un "semplice" worm che si diffonde per la mancanza di regole minime di sicurezza, per mancanza di formazione di chi usa i sistemi, per mancanza di consapevolezza dell'importanza che ha la difesa dei sistemi informativi per la nostra vita di tutti i giorni.

Cosa mi fa dire che non penso si tratti di una intrusione di hacker? Perché ho grande rispetto dei "nemici", se fossero stati hacker, che sono sì dei banditi ma sono bravi, preparati, intelligenti, determinati, il sistema sarebbe stato devastato.

(Autore: Gigi Tagliapietra)

-----

Email di phishing: la situazione attuale.

Lo spamming sta aumentando l'intensità dei suoi picchi (anche di nove volte in raffronto al precedente), la tipologia di email è la stessa da mesi, tranne, come vedremo, che per il phishing. Ad oggi, le email di spamming si possono dividere nelle seguenti categorie:

- phishing (tese ad ottenere le credenziali di accesso al proprio conto on line);
- vendita di prodotti (medicinali, orologi, ecc.);
- scommesse;
- suggerimenti (es: investimenti in azioni, interventi per migliorare le "prestazioni", opportunità di lavoro, ecc.);



- richieste di contatto (ragazza russa sola, erede unico di un'ingente fortuna, ecc.);
- vincite alla lotteria;
- saluti (biglietti augurali, messaggi vocali, ecc.).

A volte le email pervengono ad ondate successive. In alcuni casi, inondano con centinaia o migliaia di email i domini di una determinata Azienda o Ente, in modo da provocare un forte rallentamento nella ricezione della posta e riempire le caselle, se non prontamente svuotate dalla email spazzatura.

Anche quelle di phishing, una volta più discrete, ora arrivano a gruppi e, molto spesso, con il risultato che il ricevente nemmeno le legge, e le cancella tutte in un colpo solo. Infatti, risultano pervenire da quattro o cinque banche diverse, come se tutti avessero più rapporti di conto on line con così tante banche!

Sul fronte della tipologia di messaggi, da pochi giorni si nota qualche novità nella speranza, per il criminale, di riuscire ad ingannare qualche utente.

Possiamo raggruppare le email di phishing in base alla tipologia di messaggio che viene inviato, vuoi positivo (ad esempio, per prevenire atti criminali o per premiare), o negativo (ad esempio, perché l'utente ha sbagliato più di tre volte l'immissione della password).

Vediamo le diverse tipologie:

#### POSITIVI:

la banca o Ente emittente la carta di credito è attento alla sicurezza; con la email inviata chiede la verifica dei dati per l'accesso online, oppure per attivare un rapporto di conto (in alcuni casi la email dice che il codice dispositivo arriverà via posta, ma per attivarlo bisogna digitare le credenziali, e quindi il codice dispositivo! Ciò è interessante, in quanto sembra che con queste email i criminali sembrano puntare a clienti con qualche problema di comprensione o fortemente distratti, e tutto ciò fa riflettere sulla reale composizione dell'universo degli utilizzatori di funzionalità offerte dal mondo finanziario e sulla possibile percentuale di utenti con ridotte capacità critiche); un addebito sul conto è andato a buon fine; se il Cliente ha qualche rimostranza, acceda al conto digitando le note credenziali (è ovvio che, nella mente dell'ignoto criminale, il Cliente sprovveduto accede subito per vedere di che si tratta!); il Cliente è stato premiato per la sua fedeltà all'accesso online: per ottenere la vincita (da 350 a 500 euro a seconda dell'Azienda) si deve accedere al conto digitando le credenziali, ovviamente!

#### NEGATIVI:

la banca o Ente è intervenuto bloccando il conto; ciò per una di queste cause: tentativi di accesso che hanno provocato il blocco della password, accesso da un indirizzo del Cliente diverso da quello solitamente utilizzato ( in questo caso si nota una incongruenza:

l'accesso è bloccato, ma si chiede al Cliente di digitare le credenziali per accedere!) un accredito è stato bloccato, in quanto vi sono delle irregolarità; il Cliente acceda al conto per correggere tali difformità. Ciò che fa piacere osservare, è sia come le Aziende - tramite l'Autorità Giudiziaria - intervengano immediatamente per bloccare gli indirizzi Internet forniti dalle email di phishing, sia sulla efficacia dei più recenti software prodotti per difendere i computer (antiphishing, antispamming, personal firewall, ecc.).

In conclusione, ci sembra che, per le ragioni sopradette, la situazione phishing, a tre anni dal suo manifestarsi, appaia oramai avere un lento declino nell'area dell'efficacia.

Una preoccupazione, invece, ci assilla. Come scritto diversi mesi fa, e riportato anche dalla stampa specializzata, non si assiste da tempo ad un attacco virus massiccio. Aumentano invece gli spyware ed i malware, ossia, programmi atti a catturare le informazioni digitate sul computer ovvero a dirottare su siti criminali gli utenti.

Appare pertanto esserci una stretta correlazione fra i due fenomeni. Infatti, qualora vi fosse un massiccio attacco di virus tesi a bloccare le comunicazioni o a distruggere il contenuto dei computer, gli utenti interverrebbero con tempestività e senza tentennamenti nel migliorare le difese dei computer.



Il consiglio, quindi, che ci sentiamo di dare, è chiaramente quello di adottare misure periodiche quali le seguenti:

- sensibilizzare gli utenti ed i Clienti sui possibili rischi nei quali possono incorrere se: non aggiornano il software a protezione del computer utilizzato, evitano di accedere a siti non conosciuti, non scaricano musiche o filmati o foto da siti sconosciuti
- intensificare i controlli sui computer, specialmente alla ricerca di spyware; possibilmente, tal fine, eseguire la scansione del pc tramite un antivirus o software diverso da quello dell'antivirus attivo sul computer;
- mettersi in allarme in caso di attività insolita del computer (da non confondere con l'aggiornamento in background del software di sistema).

(Fonte: ANSSAIF - [www.anssaif.it](http://www.anssaif.it))

-----  
Worm Wi-Fi

Non sono solo i PC ad essere suscettibili da tipologie di attacco "tradizionali", se così si può dire. Hao Hu e Steven Myers ricercatori dell'Indiana University, in collaborazione con Vittoria Colizza e Alessandro Vespignani del Complex Networks Lagrange Laboratory (CNLL), Institute for Scientific Interchange (ISI) di Torino, in una pubblicazione

([http://arxiv.org/PS\\_cache/arxiv/pdf/0706/0706.3146v1.pdf](http://arxiv.org/PS_cache/arxiv/pdf/0706/0706.3146v1.pdf))

illustrano come sia possibile realizzare un worm in grado di sfruttare le debolezze intrinseche in (ahimè) diffuse configurazioni di reti Wi-Fi per attaccare gli stessi router wireless, installando su di essi firmware opportunamente modificati.

Le principali novità introdotte in questo lavoro sono:

- l'ipotesi secondo cui il worm si diffonderebbe esclusivamente attraverso le reti wireless sfruttando la concentrazione di router di questo tipo in grandi contesti urbani: da qui, non è da escludere che evoluzioni di un tale attacco porti a azioni diversificate a seconda del tipo di rete fisica, una caratteristica fino ad oggi non considerata in questo tipo di malware;
- la possibilità che il worm violi la chiave WEP, qualora sia presente almeno questo minimo livello di protezione, con un attacco a forza bruta;
- la possibilità di accedere, sempre basandosi su un dizionario pre-costituito di password, alle interfacce amministrative dei router per installare un firmware modificato, in grado quindi di porre sotto il controllo dell'attaccante il dispositivo.

Per descrivere la potenziale diffusione del worm i ricercatori hanno utilizzato modelli basati sullo studio della diffusione delle malattie infettive negli organismi animali e nell'uomo, poichè la modalità di infezione del worm è atipica rispetto ai "cugini" che sfruttano Internet (il worm incriminato, infatti, utilizzerebbe il raggio di copertura del segnale, analogamente al "contagio" umano, per individuare altri router da infettare). I risultati: 20.000 potenziali infezioni nella città New York in 2 settimane, la maggior parte delle quali in 24 ore.

Possibili soluzioni? Attenersi alle buone pratiche di sicurezza da tempo consigliate per gli apparati Wi-Fi: abilitare l'autenticazione e la cifratura del canale con WPA o WPE, data l'obsolescenza e la ormai dimostrata debolezza del protocollo WEP, dando per scontato (e ancora oggi non è purtroppo possibile farlo) che almeno questo sia comunque utilizzato... I ricercatori affermano che la complessità dell'attacco è tale da ritenere che non possa essere realizzato un worm del genere di qui a breve, fortunatamente: c'è tutto il tempo per prepararsi a dovere!

(Autore: Luca Bechelli - Fonte: ComputerWorld)

In aumento i reati online: è allarme Italia sesta al mondo per numero di vittime Segnaliamo un articolo apparso sul Corriere della Sera dello scorso 19 gennaio, ripreso anche nella versione online.



[www.corriere.it/cronache/08\\_gennaio\\_19/I\\_truffatori\\_della\\_rete\\_07666\\_ac8-c665-11dc-9f4d-0003ba99c667.shtml](http://www.corriere.it/cronache/08_gennaio_19/I_truffatori_della_rete_07666_ac8-c665-11dc-9f4d-0003ba99c667.shtml)

=====

## RAPPORTO CLUSIF SUL CYBERCRIME: BILANCIO DEL 2007

=====

Come ogni anno, il CLUSIF ha presentato un rapporto sugli eventi più significativi che hanno caratterizzato l'anno precedente, in materia di cybercrime.

La presentazione è disponibile in francese (prossimamente lo sarà anche in inglese) sul sito del CLUSIF

<https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k7-fr.pdf>

=====

## BLOG DEL CLUSIT

=====

Dopo qualche mese di "sperimentazione" prende il via il blog del CLUSIT, uno spazio in cui i soci possono partecipare con segnalazioni, commenti e riflessioni sul mondo della sicurezza. E' un modo nuovo di favorire la partecipazione dei soci al dibattito e nel contempo di offrire al mercato spunti e suggerimenti perchè ci sia sempre più informazione e consapevolezza che la protezione dei sistemi informativi è una necessità inderogabile e vitale per le istituzioni, le imprese e per i singoli individui. La formula del blog offre immediatezza e tempestività nell'informazione e allarga, attraverso i commenti, il dialogo con l'utenza più generale, preparandoci a giocare il ruolo di orientamento che il CLUSIT intende svolgere attivamente con la prossima iniziativa di "Online Sicuro". La pubblicazione dei messaggi è riservata ai soci a cui è affidata la responsabilità dei contenuti e del rispetto di una "netiquette" che mantenga alto il livello e la qualità dell'iniziativa.

Il sito è già visibile all'indirizzo <http://blog.clusit.it> (se avete un aggregatore RSS attivate subito il feed!) e ci auguriamo che, dopo qualche mese ancora di "rodaggio", possa diventare un punto di riferimento autorevole e utile per tutti e possa offrire contenuti e spunti che periodicamente saranno riportati sulla newsletter e sul sito ufficiale dell'associazione che continueranno a svolgere la loro funzione.

=====

## NUOVI OBBLIGHI DI INFORMATION SECURITY PER LE CENTRALI USA

=====

L'autorità per l'energia USA (FERC: Federal Energy regulatory Commission) ha stabilito nuovi obblighi di protezione contro attacchi informatici per proteggere le infrastrutture critiche.

Link: FERC: News Release - FERC approves new reliability standards for cyber security [[www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp](http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp)].

=====

## EVENTI SICUREZZA

26-27 febbraio 2008, Milano Cisco Expo 2008 [www.ciscoexpo.it](http://www.ciscoexpo.it)

28 febbraio 2008, Roma Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi  
[https://edu.clusit.it/scheda\\_seminario.php?id=22](https://edu.clusit.it/scheda_seminario.php?id=22)



---

Associazione Italiana  
Information Systems Auditors

---



11 marzo 2008, Roma Seminario Clusit - Sicurezza degli ambienti virtualizzati  
[https://edu.clusit.it/scheda\\_seminario.php?id=21](https://edu.clusit.it/scheda_seminario.php?id=21)

17-21 marzo 2008, Milano Seminario CISSP [www.clusit.it/isc2/calendario\\_isc2.htm](http://www.clusit.it/isc2/calendario_isc2.htm)

25-28 marzo 2008, Amsterdam Black Hat Briefing & Training Europe [www.blackhat.com](http://www.blackhat.com)

2 aprile 2008, Milano Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi  
[https://edu.clusit.it/scheda\\_seminario.php?id=20](https://edu.clusit.it/scheda_seminario.php?id=20)

2-3 aprile 2008, Amsterdam Forrester's Security Forum EMEA 2008 (Sconto 20% per i soci Clusit)  
[www.forrester.com/events/eventdetail?eventID=2068](http://www.forrester.com/events/eventdetail?eventID=2068)

19 aprile 2008, Monza Esame CISSP [www.clusit.it/isc2/calendario\\_isc2.htm](http://www.clusit.it/isc2/calendario_isc2.htm)



- TROPPI DATI PER LE “FIDELITY CARD”: INTERVIENE IL GARANTE
- NO DEI GARANTI PRIVACY UE AL “PNR” EUROPEO

## Troppi dati per le “fidelity card”: interviene il Garante

L'Autorità vieta l'uso dei dati a quattro società che operano nella grande distribuzione

Troppi dati per le “carte di fedeltà”. Il Garante privacy (composto da Francesco Pizzetti, Giuseppe Chiaravallotti, Mauro Paissan, Giuseppe Fortunato) ha vietato a quattro società - di un gruppo di cinque sottoposto a controlli - l'uso di dati personali trattati in modo illecito: troppi i dati raccolti per i programmi di fidelizzazione, moduli poco chiari e con informazioni incomplete, impossibilità di esprimere liberamente il consenso per i trattamenti di dati a fini di marketing. Supermercati, catene di negozi, agenzie di viaggi raggiunti dal divieto non potranno più utilizzare i dati e dovranno conformarsi alle misure prescritte. Prosegue senza sosta, anche attraverso accertamenti della Guardia di finanza, l'azione del Garante a tutela dei consumatori che aderiscono ai programmi di fidelizzazione promossi da operatori economici della grande distribuzione, telefonia, trasporti, viaggi. Gli accertamenti, effettuati a livello nazionale, rientrano nel piano di verifiche programmate per accertare la corretta applicazione della normativa privacy e in particolare del provvedimento generale sulle “fidelity card” adottato nel febbraio del 2005. Il quadro che emerge dalle verifiche mostra numerose irregolarità. Innanzitutto le società raccolgono troppi dati: oltre a nome, cognome luogo e data di nascita necessari per attribuire sconti, premi o bonus connessi all'uso della carta, richiedono anche titolo di studio, e-mail, professione e numero dei componenti del nucleo familiare. Dati ritenuti non pertinenti ed eccedenti dal Garante che ne ha quindi vietato l'uso ed ha ordinato alle società di cancellarli o di renderli anonimi. Altre irregolarità sono state riscontrate nelle informative date ai consumatori e nella raccolta del consenso. Gli operatori dovranno riformulare l'informativa, sia cartacea sia on line, specificando, in particolare, quali dati sia obbligatorio indicare al momento dell'adesione al progetto e quali siano invece facoltativi. Dovranno inoltre precisare i diritti (di accesso, rettifica,

cancellazione) che la normativa riconosce e chiarire che il consenso per autorizzare l'uso dei dati per altre finalità (marketing, profilazione) è libero. E, soprattutto, dovranno mettere il consumatore in condizione di poter scegliere liberamente se e quali trattamenti di dati autorizzare. Scelta che non era invece possibile effettuare in alcuni dei moduli esaminati, dove con un'unica firma si aderiva al programma di fidelizzazione ma si autorizzava l'utilizzo dei dati a fini di marketing. Per quanto riguarda poi l'uso di dati facoltativi raccolti a fini statistici il Garante ha prescritto alle società di adottare opportuni accorgimenti che impediscano di ricondurre i dati all'interessato fin dal momento della raccolta.

## No dei Garanti privacy Ue al “Pnr” europeo

Critiche alla proposta della Commissione di introdurre in Europa l'obbligo di comunicare alle autorità di polizia e di frontiera i dati dei passeggeri aerei

La proposta presentata lo scorso novembre dalla Commissione europea, secondo cui verrebbe introdotto in Europa l'obbligo di comunicare alle “autorità competenti” i dati dei passeggeri aerei diretti verso i Paesi dell'Ue, come già avviene per gli Usa, è stata accolta con forti critiche da tutte le autorità europee per la protezione dei dati. Un parere adottato congiuntamente dal gruppo di lavoro Ue (Gruppo articolo 29) e dal “Working Party on Police and Justice”, presieduto da Francesco Pizzetti, ha richiamato l'attenzione del Consiglio Ue e della Commissione sugli aspetti giudicati contrari ai principi fondamentali in materia di tutela dei dati personali ([http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp145\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp145_en.pdf)).

Le Autorità per la privacy di tutti i Paesi europei hanno espresso critiche molto serrate contro la proposta di decisione quadro del Consiglio che istituirebbe il cosiddetto “Pnr europeo”. I Garanti ritengono che la proposta comporti una grave compressione dei diritti fondamentali dei cittadini europei, sanciti non soltanto

dalla direttiva sulla protezione dei dati, ma ancor prima dalla Convenzione di Roma del 1950 (sui diritti umani fondamentali, compreso il diritto al rispetto della vita privata) e, successivamente, dalla Convenzione 108 del Consiglio d'Europa (sulla protezione dei dati personali).

Secondo i Garanti Ue per il Pnr europeo non sono dimostrate né la necessità né la proporzionalità del trattamento previsto nel progetto di decisione quadro. Soprattutto perché esiste già una direttiva Ue, la 2004/82, che prevede l'obbligo per i vettori aerei europei di raccogliere e rendere disponibile, a richiesta, i dati Api (Advance Passenger Information), cioè i dati utilizzati per il check-in. Tale direttiva, peraltro, non ha trovato ancora piena attuazione in tutti gli Stati Membri. Appare quanto meno eccessivo introdurre, dunque, un obbligo ulteriore per finalità di sicurezza quando non si è ancora verificata l'efficacia di un sistema istituito per vigilare sulle frontiere europee. Numerosi altri aspetti della proposta appaiono problematici: sono troppe le categorie di informazione oggetto di trasferimento, addirittura ulteriori rispetto a quelle previste nell'Accordo sul Pnr Usa; il periodo di conservazione dei dati da parte delle autorità competenti è eccessivo (tredici anni); non vi è chiarezza sulla necessità di prevedere esclusivamente un sistema del tipo "push" (invio di dati su richiesta), e non "pull" (accesso dall'esterno ai database per recuperare le informazioni di interesse), come già indicato nei pareri sul Pnr Usa; l'eliminazione dei dati sensibili eventualmente raccolti (indispensabile per evitare il trattamento di questi dati, che è riservato solo ad alcuni specifici soggetti) va lasciato ai singoli vettori aerei, e non alle autorità riceventi; sono troppo larghi i margini della discrezionalità lasciata agli Stati Membri nell'attuare le disposizioni contenute nella decisione, soprattutto per quanto riguarda l'ambito di circolazione delle informazioni che dovrebbero essere fornite dai vettori aerei.

Le Autorità europee per la privacy chiedono di avviare quanto prima un serio dibattito sul tema che coinvolga tutte le parti in causa: dai Parlamenti nazionali alle compagnie aeree; dal Parlamento europeo alle autorità di protezione dati. Si tratta di evitare che i cittadini, non solo quelli europei, siano oggetto di una sorveglianza generalizzata nei loro spostamenti aerei in Europa.

## L'attività del Garante.

### Per chi vuole saperne di più

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

- Regolamento n. 1/2007 - Regolamento concernente le procedure interne all'Autorità aventi rilevanza

esterna, finalizzate allo svolgimento dei compiti demandati al Garante per la protezione dei dati personali - 14 dicembre 2007 (G.U. n. 7 del 9 gennaio 2008).

- Regolamento n. 2/2007 - Regolamento concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali - 14 dicembre 2007 (G.U. n. 7 del 9 gennaio 2008).

- Il Garante scrive a Parlamento e Governo: urgente ridurre i tempi di conservazione dei dati di traffico telefonico e Internet – Comunicato del 15.1.2008

- Ispezione all'ex ospedale Regina Elena di Roma – Comunicato del 21.1.2008

- Il Garante ai gestori Tlc: cancellate le informazioni sulla navigazione in Internet – Comunicato del 24.1.2008

- Tabulati sotto chiave: il Garante detta ai gestori le regole per la tenuta dei dati di traffico telefonico e Internet – Comunicato del 1.2.2008

## *Responsabilità amministrativa degli Enti ex D.Lgs. 231/01: le novità normative e giurisprudenziali*

Il tema della responsabilità amministrativa degli enti per reati commessi nel proprio interesse o a proprio vantaggio risulta di grande attualità, in ragione della forte eco del sistema punitivo introdotto dal Decreto Legislativo 8 giugno 2001, n. 231, nonché a motivo della continua evoluzione della medesima normativa e del recente proliferare delle pronunce giurisprudenziali in materia.

Gli addetti ai lavori pongono, naturalmente, particolare attenzione sui **Modelli organizzativi, di gestione e di controllo**, idonei, se valutati positivamente, ad esimere l'ente dalla citata responsabilità amministrativa.

Ciò tenendo conto di due fattori tra loro "opposti" da un lato la giurisprudenza, che fornisce indicazioni sempre più puntuali circa le caratteristiche di un Modello "idoneo", ossia su come la Magistratura interpreta la normativa e giudica i Modelli organizzativi elaborati dalle società; dall'altro il legislatore, che amplia sistematicamente le fattispecie di reato contemplate dal Decreto in questione, rimettendo così in continua discussione quanto già eventualmente implementato dagli enti.

Gli emendamenti che ampliano la responsabilità amministrativa degli enti, infatti, rendono necessaria la sistematica valutazione dell'idoneità dei Modelli organizzativi rispetto alle singole realtà societarie.

In tale contesto di grande dinamismo, Protiviti ha ritenuto utile raccogliere e sintetizzare le novità normative - in essere ed in divenire - nonché i più recenti casi di applicazione della norma al fine di evidenziare le ultime tendenze in atto nelle aule dei tribunali.

Questo numero della newsletter è nato con l'obiettivo di aggiornare i lettori sulle novità normative e giurisprudenziali in materia di D.Lgs. 231/01.

### **Novità normative in essere:**

- *i reati di omicidio colposo e lesioni colpose gravi o gravissime in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;*
- *i reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita.*

### **Novità normative in divenire:**

- *il reato di corruzione nel settore privato;*
- *i reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;*
- *i reati ambientali;*
- *il reato di grave sfruttamento dell'attività lavorativa;*
- *il reato di criminalità informatica;*
- *i reati in materia di inquinamento provocato dalle navi e scarico di sostanze inquinanti;*
- *i reati tributari.*

### **Novità giurisprudenziali**

- *sentenza Tribunale di Milano, sez. X penale, 20 marzo '07/31 luglio '07;*
- *ordinanza G.I.P. presso il Tribunale di Milano, 13 giugno '07*
- *ordinanza G.I.P. presso il Tribunale di Napoli, 26 giugno '07*

## Novità normative in essere

***Ampliamento del catalogo di reati rilevanti ai sensi del D.Lgs. 231/2001: introduzione dei reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene del lavoro***

La Legge 3 agosto 2007, n. 123 ha introdotto nel D.Lgs. 231/2001 l' art. 25-septies, in forza del quale il catalogo dei reati rilevanti ai fini dell' applicazione di quest' ultima normativa si amplia con i reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e della tutela dell' igiene del lavoro.

La novità appare di particolare rilievo, sia per il fatto che il legislatore ha per la prima volta previsto l' applicazione del Decreto 231/2001 a seguito di realizzazione di delitti colposi (anziché, precedentemente, la responsabilità amministrativa degli enti conseguiva alla sola commissione di delitti dolosi, ossia commessi intenzionalmente), sia poiché si sono stabilite pene più elevate che per ogni altro reato rilevante ai fini della medesima normativa.

## Novità normative in divenire

***Corruzione nel settore privato (in attuazione della decisione quadro 2003/568/GAI)***

E' stato approvato in data 25 settembre 2007 dal Senato e trasmesso alla Camera per approvazione il Disegno di legge governativo (Legge Comunitaria 2007) che stabilisce l' estensione della responsabilità amministrativa degli Enti al reato di corruzione nel settore privato.

In particolare, è prevista l' introduzione nel codice penale di una fattispecie criminosa che punisca chi, nell'ambito di attività professionali, intenzionalmente sollecita o riceve, per sé o per un terzo, direttamente o tramite un intermediario, un indebito vantaggio di qualsiasi natura, oppure accetta la promessa di tale vantaggio, nello svolgimento di funzioni direttive o lavorative non meramente esecutive per conto di una entità del settore privato, per compiere o omettere un atto, in violazione di un dovere, sempreché tale condotta comporti o possa comportare distorsioni

***Ampliamento del catalogo di reati rilevanti ai sensi del D.Lgs. 231/2001: introduzione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (su base nazionale)***

Il Decreto legislativo 21 novembre 2007, n. 231 ha introdotto nel D.Lgs. 231/2001 l' art. 25-octies, in tal modo prevedendo i reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita tra quelli che importano la responsabilità dell' ente. I reati di riciclaggio e di impiego di denaro, beni o utilità di provenienza illecita erano già rilevanti ai sensi del D.Lgs. 231/2001 purché connotati dal requisito della " transnazionalità " , ossia se realizzati in più stati contemporaneamente: in forza della nuova previsione normativa, cade quest' ultimo carattere e i predetti reati sono rilevanti per la responsabilità dell' Ente anche se commessi sul solo territorio italiano.

di concorrenza riguardo all'acquisizione di beni o servizi commerciali.

E' prevista altresì la punibilità di colui che, intenzionalmente, nell'ambito di attività professionali, direttamente o tramite intermediario, dà, offre o promette il vantaggio di cui sopra.

Tali fattispecie criminose, se commesse nell' interesse o a vantaggio dell' Ente, comportano l' applicabilità delle previsioni di cui al D.Lgs. 231/2001, con la conseguente comminazione di sanzioni pecuniarie ed interdittive (non ancora stabilite nel disegno di legge).

### ***Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all' autorità giudiziaria***

Il disegno di legge governativo C. 2783 in esame alle Commissioni Giustizia e Affari Esteri della Camera prevede l' introduzione nel catalogo dei reati rilevanti ai sensi del D.Lgs. 231/01 del reato di " induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all' autorità giudiziaria" di cui all' art. 377-bis c.p..

Nell' ipotesi di realizzazione del medesimo reato, l' Ente potrebbe subire l' applicazione di sanzioni pecuniarie fino a 500 quote.

### ***Reati ambientali***

E' all' esame della II Commissione di Giustizia della Camera il Disegno di Legge governativo C. 2692 sul riassetto dei reati ambientali e sulla conseguente introduzione degli stessi tra quelli espressamente richiamati dal D.Lgs. 231/01.

In particolare, i reati contemplati sarebbero i seguenti:

- inquinamento ambientale;
- danno ambientale e pericolo per la vita o l' incolumità personale;
- disastro ambientale;
- alterazione del patrimonio naturale, della flora e della fauna;
- traffico illecito di rifiuti;
- traffico di materiale radioattivo o nucleare e abbandono.

Sull' Ente dovrebbero gravare sanzioni pecuniarie ed interdittive.

### ***Grave sfruttamento dell' attività lavorativa***

E' all' esame della II Commissione Giustizia della Camera il Disegno di legge recante " disposizioni penali contro il grave sfruttamento dell' attività lavorativa e interventi per contrastare lo sfruttamento di lavoratori irregolarmente presenti sul territorio nazionale" .

A carico dell' Ente dovrebbero prevedersi sanzioni pecuniarie ed interdittive.

### ***Criminalità informatica***

In data 11 maggio 2007 il Consiglio dei Ministri ha approvato lo schema di disegno di legge in cui si prevede l' introduzione dei reati di attentato ad impianto di pubblica utilità , delitti informatici e trattamento illecito dei dati tra le fattispecie criminose rilevanti ai sensi del D.Lgs. 231/2001.

Sarebbero previste sanzioni pecuniarie ed interdittive nell' ipotesi di realizzazione dei predetti reati a favore dell' Ente.

### ***Inquinamento provocato dalle navi e scarico di sostanze inquinanti***

Approvato dal Consiglio dei Ministri, in data 30 agosto 2007, lo schema di decreto legislativo che prevede, tra l' altro, l' estensione dell' applicazione del D.Lgs. 231/01 a condotte illecite di inquinamento provocato dalle navi e scarico di sostanze inquinanti.

Sull' Ente dovrebbero gravare sanzioni pecuniarie ed interdittive.

### ***Reati tributari***

Tra le altre modifiche al D.lgs. 231/2001 proposte al legislatore, la Commissione del Ministero della Giustizia sul medesimo decreto ha proposto l' introduzione dei reati tributari tra quelli rilevanti per l' applicazione della responsabilità amministrativa degli enti.

Con riferimento alle sanzioni, potrebbero prevedersi sanzioni pecuniarie ed interdittive.

## Novità giurisprudenziali

Di seguito riportiamo i principali provvedimenti giurisprudenziali recentemente emanati in materia di responsabilità amministrativa degli Enti.

### ***Sentenza Tribunale di Milano, sez. X penale - 20 marzo 2007/31 luglio 2007***

La sentenza riguarda la condanna di una società operante nel settore della ristorazione commerciale per il reato di **corruzione**.

In particolare, l' Amministratore Delegato ed il Legale Rappresentante dell' ente avrebbero in più occasioni effettuato, verso dipendenti INAIL, la promessa ed il successivo versamento di somme di danaro, al fine di ottenere l' aggiudicazione di una gara di appalto per la fornitura di buoni-pasto nonché condizioni contrattuali di particolare favore. La società è stata riconosciuta colpevole del reato ascrittore per non aver predisposto un modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/01 prima della commissione del fatto illecito; la successiva adozione veniva invece considerata dal G.I.P. meramente formale, posto che non ne sarebbe seguita una concreta attuazione.

In seguito alla violazione del D.Lgs. 231/01, le sanzioni comminate sono state le seguenti:

- sanzione pecuniaria pari a € 75.000,00;
- sanzione interdittiva del divieto di contrattare con la Pubblica Amministrazione per un anno;
- confisca di € 1.000.000,00 considerato profitto del reato;
- pubblicazione della sentenza su un quotidiano nazionale.

### ***Ordinanza G.I.P. presso il Tribunale di Milano – 13 giugno 2007***

Nell' ordinanza il G.I.P. affronta la questione della **giurisdizione del giudice italiano** rispetto ad enti esteri che non hanno sede in Italia.

In particolare, viene affermato che il D.Lgs. 231/01 non esclude la sussistenza della giurisdizione italiana nei confronti di una banca estera che, pur non avendo succursale in Italia,

operi comunque sul territorio nazionale. Il complesso del quadro normativo lascerebbe intendere con chiarezza che solo lo Stato, gli enti pubblici territoriali, gli enti pubblici non economici e gli enti che svolgono funzioni di rilievo costituzionale sono esenti dall' applicabilità del D.Lgs. 231/01: diversamente, gli Enti esteri che – pur non avendo sede in Italia – decidono di operare sul territorio nazionale italiano hanno l' onere di attivarsi e di uniformarsi alle previsioni normative italiane.

### ***Ordinanza G.I.P. presso il Tribunale di Napoli – 26 giugno 2007***

Di particolare rilievo l' ordinanza emessa dal G.I.P. presso il Tribunale di Napoli rispetto ad un caso di presunta **truffa ai danni dello Stato**, a seguito di aggiudicazione di gare di appalto.

In particolare l' Ente, attraverso i suoi soggetti apicali, avrebbe violato gli obblighi contrattuali di cui a contratti di appalto per la gestione del ciclo di smaltimento dei rifiuti solidi urbani.

Il G.I.P. ordinava, pertanto, l' applicazione della misura cautelare del divieto di contrattare con la Pubblica Amministrazione nonché il sequestro preventivo finalizzato alla confisca per equivalente del profitto del reato in ragione della ritenuta inidoneità del modello organizzativo adottato dalla Società per i seguenti motivi:

- il modello non sarebbe stato elaborato a seguito di una corretta e specifica analisi dei rischi di reato;
- i protocolli di prevenzione non avrebbero regolamentato in modo stringente le attività pericolose presidiandole con adeguate specifiche sanzioni;
- dalle relazioni dell' OdV parrebbe non evincersi il comportamento fittivo tenuto dalla società prima e durante la perpetrazione degli illeciti presupposti in contestazione;
- con espresso riferimento alla composizione ed alle attività effettuate dall' Organismo di Vigilanza si è osservato che:
  - nel Modello non si prevedeva l' indicazione della professionalità richiesta ai membri, del OdV;
  - la mancanza di separazione tra compiti gestionali e compiti di sorveglianza propri

- dei componenti degli OdV sarebbe elemento da cui desumere la mancanza del requisito dell' indipendenza del medesimo Organismo;
- nel Modello non si prevedeva tra le cause di ineleggibilità e di revoca dei membri la condanna per uno dei reati contemplati nel Decreto. Del pari, è risultata censurabile la mancata verifica da parte del CdA societario della verifica dei requisiti di indipendenza, autonomia, onorabilità e professionalità ;
  - nel regolamento dell' OdV non si sarebbe prevista l' indicazione della tempistica e delle modalità di attuazione dell' attività ispettiva;
  - sarebbe risultato nel Modello che i componenti dell' OdV della capogruppo fossero al contempo consiglieri delle controllate;
- non si sarebbe espressamente sanzionata la violazione degli obblighi di informazione verso l' OdV sulle infrazioni al modello ed al codice etico;
  - non si sarebbe proceduto ad una tipizzazione del sistema sanzionatorio per le singole violazioni, posto che ad ogni precetto avrebbe dovuto corrispondere la relativa misura disciplinare;
  - nel Modello non si sarebbe espressamente prevista l' obbligatoria partecipazione del personale ai corsi di formazione, nonché la verifica dei contenuti e delle modalità di erogazione da parte dell' OdV.

## Conclusioni

Le novità normative innanzi indicate sono destinate ad ampliare a breve il perimetro del Decreto 231; la ricca elaborazione giurisprudenziale, d' altra parte definisce sempre più nitidamente i contenuti specifici dei Modelli organizzativi affinché questi ultimi possano essere ritenuti " idonei" per ottenere la condizionale esimente da parte degli enti.

Resta lo sforzo delle società di colmare costantemente le " lacune" dei propri Modelli di organizzazione, aggiornandoli le rispetto alle previsioni legislative nel tempo introdotte nel Decreto e ritagliandoli sulla propria realtà .

La particolare rilevanza dell' istituto della responsabilità amministrativa degli enti unitamente alla continua evoluzione della normativa di riferimento costituiscono fattori che impongono alle società di dedicarsi con impegno sistematico e crescente alla concreta attuazione dei propri Modelli organizzativi, nonché verifica della loro adeguatezza.

\*\*\*\*\*

Per maggiori informazioni, rivolgetevi all'ufficio Protiviti più vicino o telefonate al numero 02 6550 6301 (Francesca Delfini, Manager 231).