ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Il Decreto Legislativo n. 231 dell' 8 Giugno 2001

Aspetti legali e modalità applicative

(a cura di **Alberto Capeccioni, CIA, CISA**)

INDICE DELLA PRESENTAZIONE :

1. **Presentazione del relatore**
2. Obiettivi e struttura della presentazione
3. La normativa e la sua evoluzione
4. Il modello organizzativo “esimente”, modalità applicative
5. L’impatto sulla sicurezza informatica
6. Conclusioni
7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

Il relatore

1. Esperienza in varie aziende nelle aree IT, Organizzazione, Internal Audit, IT Audit;
2. Attualmente attività libero professionale nell'Internal Auditing e nella Formazione;
3. Implementazione e verifica di conformità del modello org.vo "esimente" ai sensi della legge 231/01;

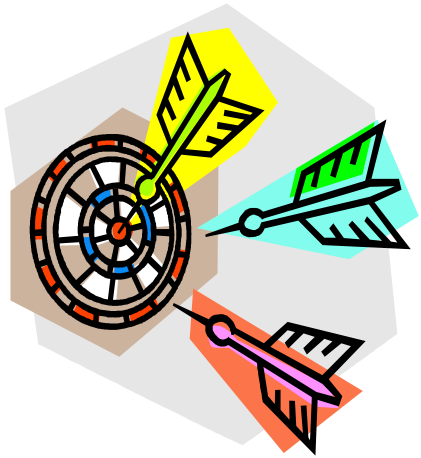
INDICE DELLA PRESENTAZIONE :

1. Presentazione del relatore
2. **Obiettivi e struttura della presentazione**
3. La normativa e la sua evoluzione
4. Il modello organizzativo “esimente”, modalità applicative
5. L’impatto sulla sicurezza informatica
6. Conclusioni
7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

2. Obiettivi della presentazione

Illustrare:

1. Principi ispiratori della normativa ed aspetti generali (in sintesi ed a titolo di esempio).
2. Sua evoluzione e modalità applicative
3. Implementazione del modello organizzativo
4. Aspetti legati all'IT Auditing ed alla Sicurezza Informatica



INDICE DELLA PRESENTAZIONE :

1. Presentazione del relatore
2. Obiettivi e struttura della presentazione
3. **Aspetti legali**
4. Il modello organizzativo “esimente”, modalità applicative
5. L’impatto sulla sicurezza informatica
6. Conclusioni
7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

3.1 Aspetti Legali – principi della normativa

1. "Societas delinquere non potest"
2. "Responsabilità Amministrativa" (rectius *penale*) degli enti
3. Solo per reati specifici
4. Vantaggio o interesse nel commettere il reato

3.2 Aspetti Legali – Reati

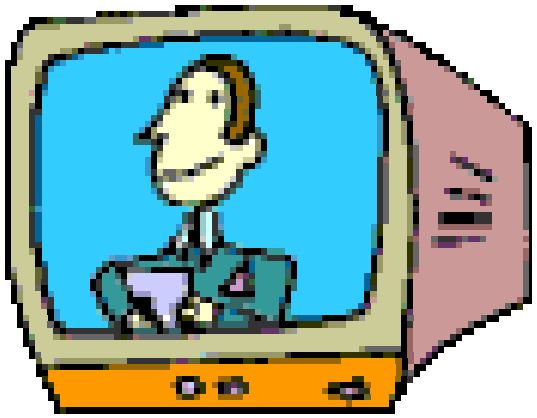
- Malversazione o indebita percezione di erogazioni a danno dello stato;
- Truffa;
- Frode informatica (alterazione del sistema informatico per ottenere ingiusto profitto);
- Concussione
- Corruzione e istigazione alla corruzione (per atto di ufficio o contrario ai doveri di ufficio, in atti giudiziari, di persona incaricata di servizio pubblico)

3.3 Aspetti Legali – Reati

- Peculato (appropriazione indebita di cose appartenenti alla P.A.)
- Falsificazione di monete
- False comunicazioni sociali (es. falso in bilancio, in particolare in danno della società, dei soci o dei creditori);
- Falsità nelle comunicazioni delle società di revisione
- Impedito controllo (es. occultando documenti):
- Illegale ripartizione degli utili o delle riserve;

3.4 Aspetti Legali – Reati

- Omessa comunicazione del conflitto di interesse
- Formazione fittizia del capitale;
- Aggiottaggio (diffusione di notizie false al fine di alterare il valore di strumenti non quotati);
- Manipolazione del mercato (notizie false per alterare il valore di strumenti finanziari quotati)
- Ostacolo all'attività delle autorità di vigilanza;
- Reati di terrorismo e contro la persona;
- Abuso di informazioni privilegiate (detto anche Market abuse)



3.5 Aspetti Legali – Reati

- Reati transnazionali (associazione per delinquere, associazione mafiosa, favoreggiamento, riciclaggio, contrabbando, traffico di stupefacenti, favoreggiamento dell'immigrazione clandestina.
- Reati che saranno inclusi per recepimento normative CEE (reati ambientali, reati informatici – convenzione cybercrime 1998, tutela della proprietà intellettuale)

3.6 Aspetti Legali – Sanzioni

1. Pecuniarie
2. Interdittive (es. ad operare con la P.A. per un certo tempo);
3. Pubblicazione della sentenza di condanna
4. Confisca del profitto che l'ente ha tratto dal reato
5. Reclusione
6. Commissariamento (per gli enti he fanno un servizio pubblico)

3.7 Aspetti Legali – Presupposti della responsabilità dell'ente

Reati commessi a vantaggio dell'ente da persone "apicali" (dirigenti) a meno che:

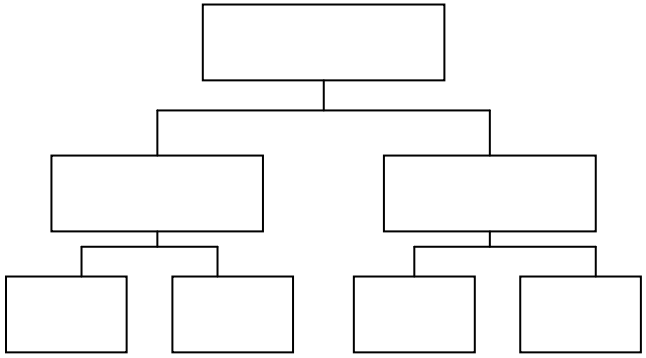
- sia stato adottato un modello di gestione idoneo a prevenire i reati;
- il soggetto apicale lo abbia eluso fraudolentemente;
- non vi sia stata omessa vigilanza da parte dell' Organo di Vigilanza (ODV).

INDICE DELLA PRESENTAZIONE :

1. Presentazione del relatore
2. Obiettivi e struttura della presentazione
3. Aspetti legali generali
4. **Il modello organizzativo "esimente"**
5. L'impatto sulla sicurezza informatica
6. Conclusioni
7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

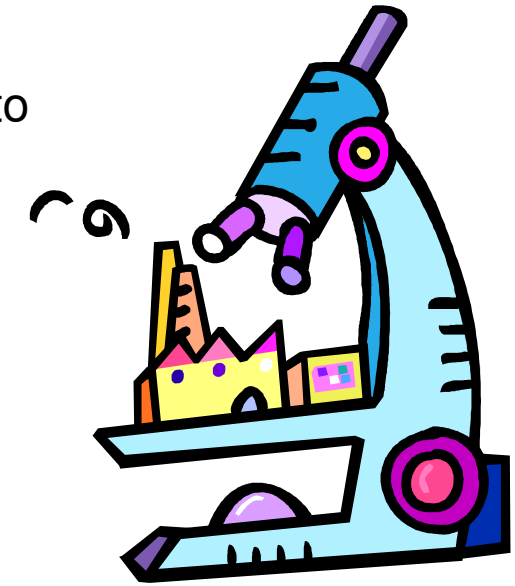
4.1 Il Modello organizzativo esimente - componenti

- Codice etico
- Organigramma e procedure
- Poteri di firma interni
- Procure
- Sistema di controllo di gestione
- Comunicazione e formazione del personale (in particolare sui processi sensibili)
- Poteri, compiti e composizione dell'OdV



4.2 Il modello organizzativo esimente - componenti

- Flussi informativi verso l'OdV;
- Sistema disciplinare per sanzionare il mancato rispetto di quanto previsto dal modello;
- Misure adottate per scoprire ed eliminare tempestivamente le situazioni a rischio;
- Verifiche di conformità.



4.3 Il modello organizzativo esimente – l'OdV

1. In genere collegiale (Internal Audit e Uff. Legale)
2. Compiti
3. Requisiti (autonomia, indipendenza, competenza in tema ispettivo e consulenziale, obiettività. Organo interno all'ente, a tempo pieno sul modello, libero accesso alle informazioni, no compiti operativi)
4. Fonti di informazione

4.4 Il modello organizzativo esimente – revisione indipendente esterna

1. L'OdV è interno ma la revisione (definita, ad esempio, Intervento di Conformità) può essere svolta da enti esterni.
2. Viene individuata una procedura analoga ad un intervento di audit pianificato (piano, kick off meeting, etc.)
3. La verifica si incentra sulle "attività sensibili", ovvero quelle che possono produrre, con maggiore probabilità, reati (ad esempio nei confronti della PA)

4.5 Il modello organizzativo esimente – indagine sulle modalità di adozione in soc. non quotate (fonte AIIA – Gennaio 2007)

1. Il modello 231 è stato adottato dal 62,5% del campione e per un altro 25% è in corso di adozione ;
2. Nel 95% dei casi l'Internal Auditing ha il ruolo di componente e/o di braccio operativo dell'OdV;
3. Nell'80 % dei casi Ufficio Legale ed Internal Auditing son coinvolti nella predisposizione del modello;
4. L'adozione del modello va dal 42% dei trasporti al 100% dell'edilizia (servizi finanziari 71%)

INDICE DELLA PRESENTAZIONE :

1. Presentazione del relatore
2. Obiettivi e struttura della presentazione
3. Aspetti legali generali
4. Il modello organizzativo “esimente”
5. **Il sistema di controllo interno e la sicurezza informatica**
6. Conclusioni
7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

5. 1 Il sistema di controllo interno –CO.SO. report

I principi di un sistema di controllo interno secondo il COSO (Committing Of Sponsoring Organization) report nel 1992:

1. Ambiente di controllo ("Tone at the top");
2. Risk Assessment;
3. Attività di controllo;
4. Informazione e comunicazione;
5. Monitoraggio.

5. 2 Il sistema di controllo interno – la sicurezza IT

Alla luce di quanto detto a cosa deve stare particolarmente attento un IT Manager o un IT Auditor ?

1. Affidabilità dei dati;
2. Disponibilità dei dati (Incident Response e Disaster Recovery);
3. Riconoscimento ed autenticazione;
4. Sicurezza fisica e controllo accessi.

INDICE DELLA PRESENTAZIONE :

1. Presentazione del relatore
2. Obiettivi e struttura della presentazione
3. Aspetti legali generali
4. Il modello organizzativo “esimente”
5. L’impatto sulla sicurezza informatica
6. **Conclusioni**
7. Riferimenti bibliografici e sitografici
8. Varie – Q&A

6. Conclusioni

Il modello organizzativo esimente ex dlgs 231 è un'altra buona occasione per riscoprire i principi del controllo interno, già noti da tempo. Un sistema di controllo ben fatto che parta dai presupposti del COSO Report e che si traduca in procedure operative ed informatiche adeguate, con un ruolo adeguato ai controlli di 1°, 2° e 3° livello è comunque in grado di garantire qualunque amm.re dai reati commessi da dirigenti e dipendenti. Un sistema adeguato di sicurezza IT ne è solo la logica conseguenza.

Bibliografia e sitografia :

1. www.rivista231.it
2. www.aiiaweb.it
3. www.coso.org
4. 231-01.blogspot