Seminario di aggiornamento

Lunedì 20 febbraio 2017

Orario 10.00 – 13.30 / 14.30 – 17.00

I reati informatici e modello 231: ottimizzare i processi aziendali anche attraverso la GDPR

Relatori:
Dr. Lorenzo Colzi, Dr. Marco Parretti
Consulenti legali in diritto delle nuove tecnologie

Firenze, sede Ti Forma - Via Giovanni Paisiello, 8

DESTINATARI

Presidenti, AD, Direttori, Componenti Organismo di Vigilanza, Responsabili ex D.Lgs. 231/2001, Responsabili dei Sistemi di Gestione Qualità e Responsabili e operatori degli Uffici: Legale, ICT, Privacy.

PRESENTAZIONE

Nell'ambito del Decreto Legislativo 231/2001, il corso si propone di fornire un excursus sui reati informatici, evidenziando come potrebbero essere commessi fuori dalla volontà dell'organo dirigente. Nella prospettiva della prossima e rigida applicazione del Nuovo Regolamento Europeo sulla Protezione dei Dati (GDPR), si rileverà poi come l'adozione di misure tecniche ed organizzative adeguate alla gestione e alla tutela dei dati personali all'interno delle aziende favorirà la razionalizzazione e la revisione dei modelli 231 esistenti, presidio contro i rischi derivanti dalla gestione delle informazioni.

OBIETTIVI

Fornire un overview sul D.Lgs. 231/2001, tratteggiando gli aspetti della normativa che sono necessari per comprendere le modalità con le quali l'azienda deve affrontare l'implementazione di un sistema 231 idoneo alla prevenzione dei reati presupposto previsti dal Decreto.

Contestualizzare i reati informatici all'interno dell'azienda, indicando le attività da porre in essere per la mappatura del rischio, la predisposizione del MOG e del relativo sistema di prevenzione.

SEGRETERIA ORGANIZZATIVA
Violetta Fusco – email vfusco@tiforma.it
☏ 055-210755 🖷 055-291715
Via Giovanni Paisiello, 8 - Firenze
P.IVA/C.F. 04633850484
Sito web www.tiforma.it

PROGRAMMA

1. L' ambito di applicazione soggettiva del D. Lgs. 231

2. I criteri di attribuzione della responsabilità:

- Soggettivi: ruoli in posizione apicale e sottoposti all'altrui direzione e vigilanza, e la delega di funzioni
- Oggettivi: Le nozioni di interesse e vantaggio

3. La "colpa di organizzazione":

- La mappatura del rischio
- I Modelli di Organizzazione e Controllo
- Il Codice Etico
- L' Organismo di Vigilanza: composizione, requisiti e compiti
- Il Sistema Disciplinare

4. Il sistema Sanzionatorio:

- La sanzione pecuniaria e le ipotesi di riduzione
- Le sanzioni interdittive: Presupposti e Caratteristiche e L'importanza delle condotte riparatorie

5. L' inosservanza delle sanzioni

6. Procedimento di accertamento e applicazione delle sanzioni: brevi cenni

7. Business case

SECONDA PARTE:

1. I Reati Informatici

2. La mappatura del rischio informatico

3. La rilevanza delle certificazioni in materia di sicurezza informatica presenti in azienda: (27001-22300 etc.)

4. Il MOG sui reati informatici:

- Amministratori di Sistema: gli AdS interni ed esterni, gli outsourcer e la relazione annuale
- Il Regolamento Informatico Interno e l'incidenza dell'art. 4 L. 300/1970 sul controllo a distanza dei dipendenti sulla prevenzione dei reati presupposto
- RAAE: procedure per lo smaltimento della spazzatura elettronica
- Il DPS
- Le licenze
- Le Procedure del comparto ICT

5. Business Case

6. General Data Potection Regulation: gli aspetti del Regolamento Europeo sulla protezione dei dati che impattano sui reati informatici ex 231:

- Data Breach notification
- Data Protection Officer: incarico e posizione rispetto ai reati informatici e all'ODV

7. Whistleblowing:

- scelte preliminari (identità del segnalante, e sistema informatico per la segnalazione)
- flussi verso l'Organismo di Vigilanza

8. Le attività di controllo dell'Organismo di Vigilanza sui reati informatici

9. I reati previsti dal D.Lgs. 196/2003