CORSO DI ALTA FORMAZIONE IN
INFORMATION SECURITY MANAGEMENT

8ª EDIZIONE, ROMA
FEBBRAIO 2011- SETTEMBRE 2011

ICT Risk Management
Aspetti legali

L'impatto del Decreto Legislativo 231/01 sui sistemi informativi

Profili giuridici e applicativi

II parte

Michele Crudele
www.crudele.it
2011-04-14

CONSEL
CONSORZIO ELIS
per la formazione professionale superiore

CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

MIP
POLITECNICO DI MILANO
SCHOOL OF MANAGEMENT

PRINCIPI DI CONTROLLO

- Ogni operazione, transazione, azione deve essere
  - Verificabile
  - Documentata
  - Coerente
  - Congrua
- Nessuno può gestire in autonomia un intero processo
  - Separazione delle funzioni
    - Autorizzazione
      - Singola o multipla
    - Esecuzione
      - Normalmente distribuita tra più soggetti
    - Controllo
      - Preferibile un solo controllore
      - Possibile un controllo di secondo livello
- Documentazione dei controlli

UN SISTEMA DI CONTROLLI DEI REATI DOLOSI

- Codice etico (o di comportamento) con riferimento ai reati considerati
- Sistema organizzativo
- Procedure manuali ed informatiche
- Poteri autorizzativi e di firma
- Sistema di controllo di gestione
- Comunicazione al personale e sua formazione

UN SISTEMA DI CONTROLLI DEI REATI COLPOSI

- Codice etico (o di comportamento) con riferimento ai reati considerati.
- Struttura organizzativa
- Formazione e addestramento
- Comunicazione e coinvolgimento
- Gestione operativa
- Sistema di monitoraggio della sicurezza

CODICE ETICO O DI COMPORTAMENTO

- Reati dolosi
  - Rispetto di leggi e regolamenti vigenti in tutti i Paesi in cui si opera
  - Ogni operazione e transazione deve essere correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua
  - Principi base relativamente ai rapporti con gli interlocutori
    - Pubblica Amministrazione, pubblici dipendenti e, nel caso di enti concessionari di pubblico servizio, interlocutori commerciali privati.
- Reati colposi
  - Formalizzare principi e criteri fondamentali in base ai quali vengono prese le decisioni, di ogni tipo e ad ogni livello, in materia di salute e sicurezza sul lavoro
    a) evitare i rischi
    b) valutare i rischi che non possono essere evitati
    c) combattere i rischi alla fonte
    d) adeguare il lavoro all'uomo: posto di lavoro, attrezzature, metodi
    e) tener conto del grado di evoluzione della tecnica
    f) sostituire ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso
    g) programmare la prevenzione
    h) dare priorità alle misure di protezione collettiva sulle individuali
    i) impartire adeguate istruzioni ai lavoratori

SISTEMA ORGANIZZATIVO

- Sufficientemente formalizzato e chiaro
- Attribuzione di responsabilità
- Linee di dipendenza gerarchica
- Descrizione dei compiti
  - Ruoli distinti per fasi distinte
- Sistemi premianti non basati solo su target di performance palesemente immotivati ed inarrivabili
  - Potrebbero costituire un velato incentivo a reati

PROCEDURE MANUALI E INFORMATICHE

- Sistema informativo
- Punti di controllo
  - Quadrature
  - Approfondimenti informativi su agenti, consulenti, intermediari
- Separazione di compiti fra coloro che svolgono fasi (attività) cruciali di un processo a rischio
- Gestione finanziaria
  - Doppia firma
  - Supervisione
  - Separazione acquisti e pagamenti
- Attenzione ai flussi finanziari non tipici, estemporanei e discrezionali
  - Trasparenza
  - Verificabilità
  - Inerenza all'attività aziendale

POTERI AUTORIZZATIVI E DI FIRMA

- Predefiniti con soglie di responsabilità
  - Relative alla funzione svolta
  - Spesso definiti dal consiglio di amministrazione
- Conosciuti nell'azienda
  - L'ignoranza non scusa ...
- Le banche *on line*
  - Non tutte hanno sistemi adeguati
    - Non prevedono la doppia firma sui pagamenti
    - Non danno un token fisico personale

SISTEMA DI CONTROLLO E GESTIONE

- Tempestiva segnalazione
  - Esistenza di criticità
  - Insorgere di criticità
  - Il problema della denuncia anonima
- Definire indicatori per tipologie di rischio rilevato
- Definire processi di *risk assessment* interni alle singole funzioni aziendali
- Tracciabilità
  - Documentare attività sensibili
  - Tutto il processo deve essere verificabile a posteriori
    - Decisione
    - Autorizzazione
    - Svolgimento
    - Controllo
  - Non è consentito il controllo qualitativo-quantitativo della prestazione del lavoratore

COMUNICAZIONE AL PERSONALE E SUA FORMAZIONE

- Codice etico
- Poteri autorizzativi
- Linee di dipendenza gerarchica
- Procedure
- Flussi di informazione
  - per la trasparenza nell'operare quotidiano
- Comunicazione
  - Capillare
  - Efficace
  - Autorevole
  - Chiara
  - Dettagliata
  - Periodicamente ripetuta
- Consultazione preventiva
  - individuazione e valutazione dei rischi
  - definizione delle misure preventive
  - riunioni periodiche
- Programma di formazione per personale delle aree a rischio
  - in funzione dei livelli dei destinatari
  - Assunzione, trasferimento, cambiamento di mansioni, introduzione di nuove attrezzature, tecnologie, sostanze e preparati pericolosi
  - Spiegare ragioni di opportunità, giuridiche e portata delle regole

STRUTTURA ORGANIZZATIVA

- Compiti e responsabilità
  - in materia di salute e sicurezza sul lavoro
  - a partire dal datore di lavoro fino al singolo lavoratore
- Attenzione a
  - RSPP - Responsabile del Servizio di Prevenzione e Protezione
  - ASPP – Addetti al Servizio di Prevenzione e Protezione
  - RLS – Rappresentante dei Lavoratori per la Sicurezza
  - MC – Medico Competente
  - Addetti primo soccorso
  - Addetti emergenze in caso d'incendio
  - Sicurezza cantieri D. Lgs. n. 494/1996
- Nella definizione dei compiti organizzativi e operativi della direzione aziendale, dei dirigenti, dei preposti e dei lavoratori esplicitare
  - attività di sicurezza di rispettiva competenza
  - responsabilità connesse all'esercizio delle stesse attività

GESTIONE OPERATIVA

- Sistema di controllo integrato e congruente con la gestione complessiva dei processi aziendali
- Definire modalità per lo svolgimento in sicurezza delle attività che impattano in modo sulla salute e sicurezza sul lavoro
  - assunzione e qualificazione del personale
  - organizzazione del lavoro e delle postazioni di lavoro
  - acquisizione di beni e servizi impiegati dall'azienda e comunicazione delle opportune informazioni a fornitori ed appaltatori
  - manutenzione normale e straordinaria
  - qualificazione e scelta dei fornitori e degli appaltatori
  - gestione delle emergenze
  - procedure per affrontare le difformità rispetto agli obiettivi fissati ed alle regole del sistema di controllo

SISTEMA DI MONITORAGGIO DELLA SICUREZZA

- Verifica del mantenimento delle misure di prevenzione e protezione dei rischi adottate e valutate idonee ed efficaci
- Monitoraggio sistematico di 1° livello
  - Modalità e responsabilità stabilite contestualmente alla definizione della gestione operativa
  - Programmazione temporale delle verifiche
  - Attribuzione di compiti e di responsabilità esecutive
  - Descrizione delle metodologie da seguire
  - Modalità di segnalazione delle eventuali situazioni difformi
  - Svolto generalmente da risorse interne
    - autocontrollo da parte dell'operatore
    - da parte del preposto/dirigente
    - in alternativa, con risorse di altri reparti o esterne
      - Servizio di Prevenzione e Protezione
- Monitoraggio di 2° livello
  - Condotto da personale
    - competente
    - obiettivo e imparziale
    - indipendente dal settore di lavoro sottoposto a verifica ispettiva
  - Analisi della funzionalità del sistema preventivo adottato

DOCUMENTI DI SUPPORTO AL MODELLO

- Codici e manuali
  - Codice etico
  - Disciplinare d'uso delle risorse informatiche
  - Manuale della Qualità
  - Manuale della Sicurezza
  - Manuale per la tutela dei lavoratori
  - Altri manuali specifici aziendali
- Organigramma aziendale
- Procedure
  - Fino a che dettaglio?
  - Dove pubblicarle?
  - Come pubblicizzare gli aggiornamenti?

LA RESPONSABILITÀ DELLE FUNZIONI APICALI

- Rapporto con i pari grado
  - Conoscenza di comportamenti a rischio
  - Dialogo e formazione reciproca
- Controllo dei sottoposti
  - Attenzione a non indirizzare su una strada pericolosa per raggiungere un obiettivo aziendale
    - L'eccesso di zelo del dipendente può essere fonte di guai
  - L'analisi delle necessità di formazione specifica
- L'interesse personale e l'influenza sull'attività aziendale
  - Se l'interesse è personale, la violazione non è responsabilità dell'azienda, ma il rischio resta
  - L'immagine derivante da un reato infame
- Segnalare anomalie
  - Possibile denuncia anonima all'organismo di vigilanza
  - Il ruolo della Polizia delle Comunicazioni

SISTEMA SANZIONATORIO

- Per i dipendenti vale lo Statuto dei lavoratori
  - Richiamo verbale
  - Ammonizione scritta
  - Multa
  - Sospensione dal lavoro e dalla retribuzione per alcuni giorni
  - Licenziamento per mancanze gravi
- A un collaboratore o fornitore si può rescindere il contratto