Delitti informatici e responsabilità legale degli enti

Dott.ssa Gloria Marcoccio, Dott.ssa Claudia Ciampi, Avv. Giuseppe Serafini

D.Lgs 231/01 ???

- “Responsabilità degli enti per delitti informatici e trattamento illecito di dati”

Considerazioni riguardo

- Le applicabili misure di sicurezza previste dalla legge come recepimento di normativa comunitaria
- Il prossimo recepimento della direttiva 2013/40/EU

Studio realizzato per CSA Italy per il comparto dei servizi cloud

CSA Italy - today

Not-for-profit Association

- **+570** **Linkedin community members (120 CSA Italy members)**
- **8** **Affiliations/Agreements:**

- **10** **Sponsors**:

- **Collaborations**: Oracle Community For Security cloudpeople

- **3** **Research Areas: (1)** ***Translations, (2) Portability-Interoperability-Application Security, (3) Privacy & Legal in the Cloud –*** ***5 WGs***

D.Lgs 231/01 e contesto Forensic

- Laddove il reato presupposto si concretizza tramite l'utilizzo di strumenti informatici (aziendali e non):
  - diventa fondamentale chiarire operativamente gli aspetti forensic di cui deve farsi carico l'azienda nel contesto delle misure predisposte con il "Modello 231",
    - con particolare attenzione agli strumenti "mobile/BYOD":

NIST Special Publication 800-101, Revision 1, May 2014: **Guidelines on Mobile Device Forensics**

"Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics. This guide attempts to bridge the gap by providing an in- depth look into mobile devices and explaining technologies involved and their relationship to forensic procedures. This document covers mobile devices with features beyond simple voice communication and text messaging capabilities. This guide also discusses procedures for the validation, preservation, acquisition, examination, analysis, and reporting of digital information"

DECRETO LEGISLATIVO 8 giugno 2001, n. 231:

Disciplina della responsabilita' amministrativa delle persone giuridiche, delle societa' e delle associazioni anche prive di personalita' giuridica

- La colpa organizzativa: omessa predisposizione degli accorgimenti preventivi idonei ad evitare la commissione del reato presupposto
- Da questa nasce l'imputabilità all'Ente della responsabilità per il reato commesso dal Dirigente o dal sottoposto
- Elemento essenziale per l'esclusione della responsabilità dell'ente: ***adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi***

Modello 231

Classi di reato presupposto individuate dal Dlgs 231/01

Art. 24 Responsabilità amministrativa da reato

Art. 24-bis Delitti informatici e trattamento illecito di dati

Art. 24-ter Delitti di criminalità organizzata

Art. 25 Concussione, induzione indebita a dare o promettere utilità

Art.25 bis Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Art. 25-bis 1 Delitti contro l'industria e il commercio

Art. 25-ter Reati societari

Art. 25-quater Delitti con finalità di terrorismo o di eversione dell'ordine democratico

Art. 25-quater 1 Pratiche di mutilazione degli organi genitali

Art. 25-quinquies Delitti contro la personalità individuale

Art. 25-sexies Abusi di mercato

Art. 25-septies Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Art. 25-octies Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

Art. 25-novies Delitti in materia di violazione del diritto d'autore

Art. 25-decies Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Art. 25-undecies Reati ambientali

Art. 25-duodecies Impiego di cittadini di paesi terzi il cui soggiorno e' irregolare

Modello 231

Classi di reato presupposto individuate dal Dlgs 231/01

Recenti normative creano importanti correlazioni tra

Art. 24-bis Delitti informatici e trattamento illecito di dati

Art. 25-quinquies Delitti contro la personalità individuale

- Il recentissimo D.Lgs 39/2014 "*Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia*" entrato in vigore il 6 Aprile 2014 ha apportato modifiche negli articoli del codice penale riguardo i reati connessi alla pedo-pornografia e, in aggiunta, ha modificato l'art 25 quinquies (Delitti contro la personalita' individuale) del D.Lgs 231/01

- Pertanto nell'insieme risulta più grave per l'Azienda l' esposizione a rischi derivanti da "Delitti contro la personalità individuale", ora molto più sbilanciati verso possibili reati di pedo-pornografia commessi tramite strumenti informatici/telematici dell'Azienda

Modello 231

Classi Art. 24-bis Delitti informatici e trattamento illecito di dati

615-ter. Accesso abusivo ad un sistema informatico o telematico

615-quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

615-quinquies. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

617-quater. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

617 quinquies. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

635 bis. Danneggiamento di informazioni, dati e programmi informatici

635-ter. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

635-quater. Danneggiamento di sistemi informatici o telematici

635-quinquies. Danneggiamento di sistemi informatici o telematici di pubblica utilità.

640-quinquies. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

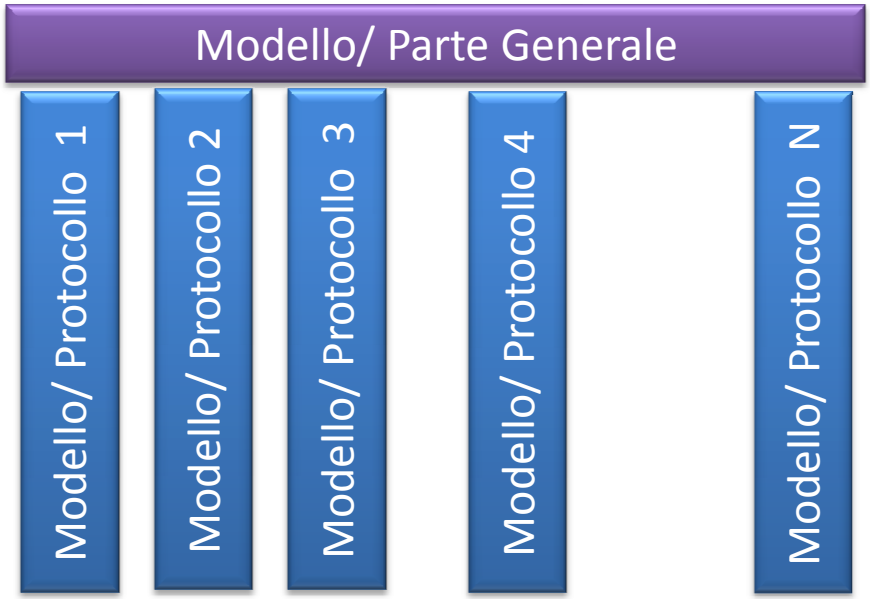
491-bis Documenti informatici

Caratteristiche essenziali per la costruzione del Modello 231

La tipica architettura per il Modello:

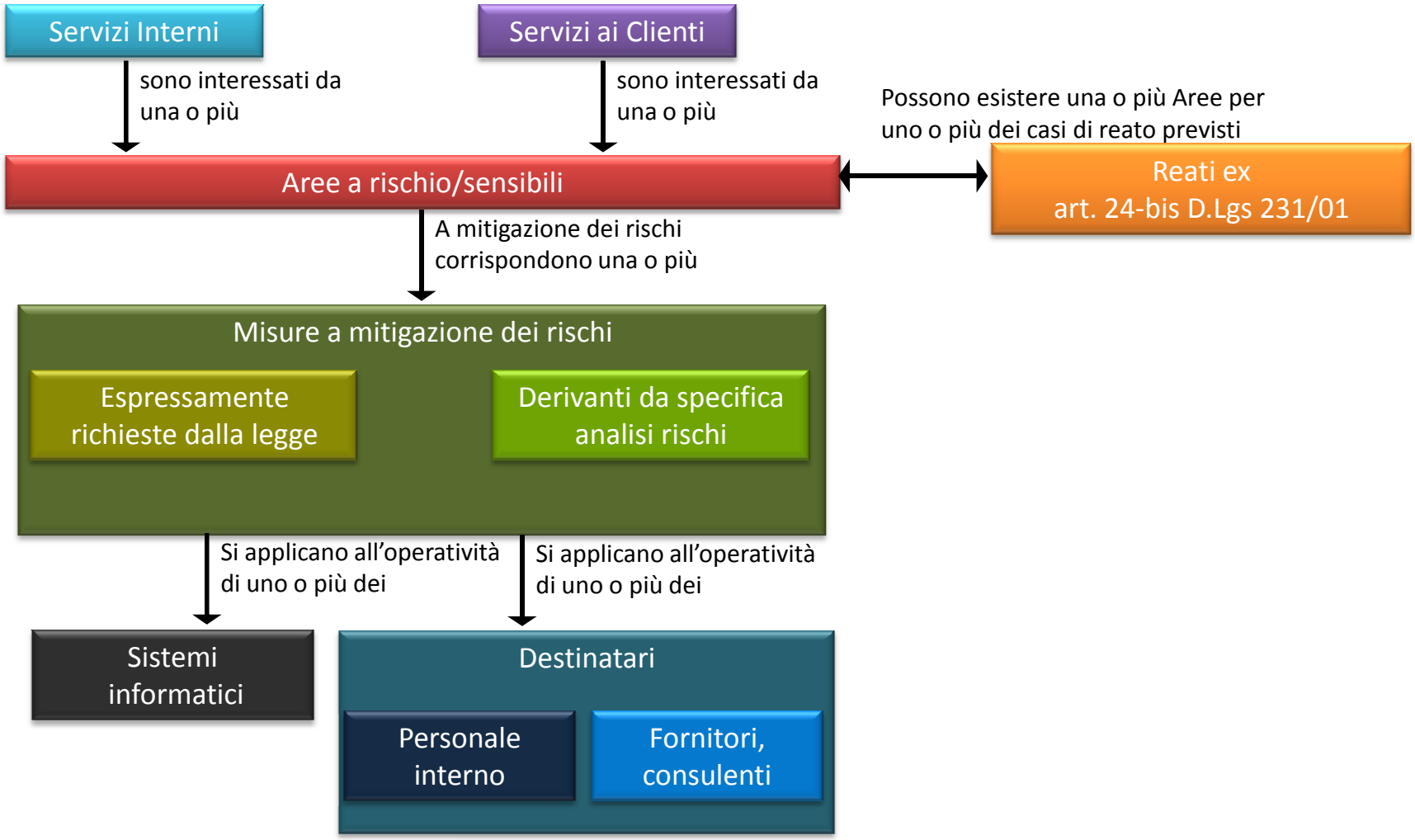
- Un documento 'padre' nel quale sono riportate le predisposizioni/misure/controlli validi nell'ente (misure trasversali)

- Tanti documenti 'figli' quanti sono i 'protocolli' a fronte delle 'aree di rischio' individuate (misure verticali).



Le aree di rischio sono individuate tenendo presenti le **'classi di reato presupposto'** stabilite nel D.Lgs 231/01 (gli articoli 24 - 25-duodecies) che risultano applicabili in funzione del tipo di ente, settore di mercato, struttura dell'ente, rapporti internazionali,…

Modello organizzativo Dlgs 231/01 e delitti informatici



Normativa di riferimento, in vigore

- **CONVENZIONE DEL CONSIGLIO D'EUROPA SULLA CRIMINALITÀ INFORMATICA Budapest, 23.XI.2001**

  recepita in Italia con la Legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"

- **Direttiva 12 agosto 2013, n. 40 del Parlamento europeo e del Consiglio, relativa agli attacchi contro i sistemi di informazione**

  sostituisce la Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione

  deve essere recepita nei Paesi Membri **entro il 4 settembre 2015**

Normativa per misure di sicurezza, in vigore

- **Direttiva 95/46/CE** per la tutela delle persone fisiche con riguardo al trattamento dei **dati personali**, nonché alla libera circolazione di tali
- **Direttiva 2002/58/CE**, direttiva relativa alla vita privata e alle **comunicazioni elettroniche** come modificata dalla Direttiva 2009/136/CE
- **Direttiva 2008/114/CE** relativa all'individuazione e alla designazione delle **infrastrutture critiche** europee e alla valutazione della necessità di migliorarne la protezione
- **Regolamento** Europeo **611 2013** sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche

Trasposizione in Italia

Decreto Legislativo 196/2003

Decreto Legislativo 61/2011

È in vigore, in quanto Regolamento UE non necessita di misure di trasposizione nei Paesi Membri UE

Normativa Comunitaria e misure di sicurezza, in vigore

Sistema di riferimento		Direttiva 95/46/CE	Direttiva 2002/58/CE, come modificata dalla Direttiva 2009/136/CE	Direttiva 2008/114/CE	Regolamento 611 2013
1.	Dati personali	X	X		X
2.	Altri dati, non personali			X	
A.	servizi della società dell'informazione	X			
B.	servizi di comunicazioni elettroniche accessibili al pubblico	X	X		X
C.	altri settori per business non necessariamente svolto on line	X		X	
I.	Misure di sicurezza preventive tali da minimizzare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della loro raccolta	X ART. 17	X ART. 4	X ART. 5 e Allegato II (ma non esplicitamente)	X ART. 4
II.	Misure in grado di individuare l'insorgenza di una violazione dei dati		X ART. 4	X ART. 5 e Allegato II (ma non esplicitamente)	X ART. 4
III.	Misure di sicurezza da attivare ex post in caso di insorgenza di una violazione dei dati allo scopo di limitarne i danni		X ART. 4	X ART. 5 e Allegato II (ma non esplicitamente)	X ART. 4
IV.	Misure per la notificazione agli utenti coinvolti dalla violazione e/o alle autorità competenti		X ART. 4		X ART. 3
V.	Misure per la gestione dell'incidente di violazione dei dati		X ART. 4	X ART. 5 e Allegato II (ma non esplicitamente)	X ART. 2,3, 4

Normativa Comunitaria e misure di sicurezza, prossime

- La proposta di nuova regolamentazione privacy "*Proposal for a Regulation of the European Parliament and of the Council on the protection* of individuals with regard to the processing of personal data and on the free movement of such data" (**General Data Protection Regulation**)

- La proposta di **direttiva Network Information Security (NIS)** "*Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union*"

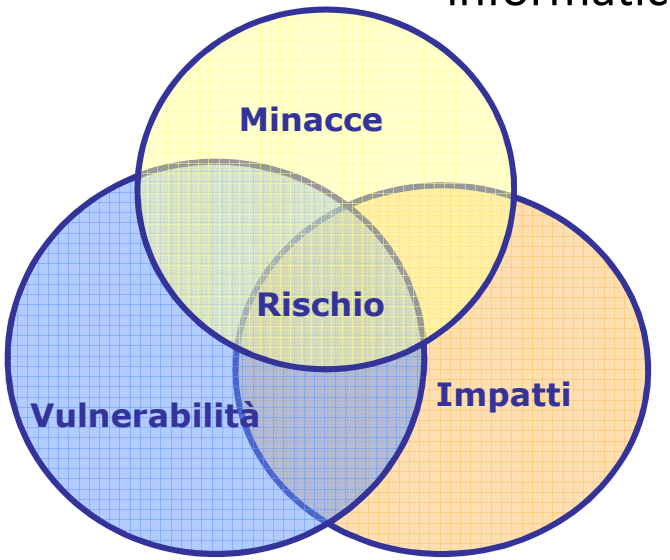
Individuazione misure di mitigazione: Approccio Risk Based

Sicurezza

L'insieme delle misure fisiche, logiche ed organizzative a protezione degli asset dell'organizzazione (beni) che assicurano il governo della compliance alla normativa.

Rischio

La probabilità che delle minacce, sfruttando le vulnerabilità degli asset, producano impatti negativi su una area operativa (rischio di commissione dei delitti informatici).



Dlgs 231 e Rischi di compliance: le principali minacce

Installazione/uso di software non autorizzato	78%
Uso di risorse aziendali per comunicazioni/attività illegali o illecite (porn sorfing, email harassement)	60%
Uso di risorse aziendali per profitti personali (spam, scommesse, gestione di personal e-commerce site, investimenti online)	60%
Abuso di computer control access	56%
Furto fisico, sabotaggio o distruzione intenzionale di computer equipment	49%
Installazione/utilizzo di hardware/periferiche non autorizzate	47%
Furto elettronico, sabotaggio o intenzionale distruzione/diffusione di dati/informazioni proprietarie	22%
Frodi	9%

Fonte: True Secure – Predictive System

% aziende con risposta affermativa

Dlgs 231 e Rischi di compliance: le vulnerabilità

- Una vulnerabilità è un punto debole-falla nella sicurezza dell'organizzazione
- In sé una vulnerabilità non provoca danni, si tratta solo di una condizione o di un insieme di condizioni che possono permettere ad una minaccia di minare un bene (asset)
- Una vulnerabilità, se non affrontata, permette la concretizzazione di una minaccia
- Esempi di vulnerabilità: mancanza di controlli sul personale, mancanza di consapevolezza, errata assegnazione degli incarichi, scarso addestramento nella sicurezza, carenze nella gestione dei profili di accesso alle risorse informatiche; mancanza di controlli sulle utenze ad elevati privilegi; carenze nella gestione dei sistemi antintrusione; carenze nel patching di sistemi operativi e programmi; ecc

Dlgs 231 e Rischi di compliance: Strumenti e Controlli

Gli Standard Internazionali come Strumenti per l'individuazione e la gestione dei controlli atti a mitigare i rischi di Compliance	
ISO/IEC 27001:2013	***Information tecnnology - Security techniques - Information security management systems - Requirements***. Standard internazionale che definisce i requisiti indispensabili di un sistema per la gestione della sicurezza delle informazioni ed identifica, per ciascun ambito di sicurezza, gli obiettivi di controllo ed i relativi controlli di sicurezza da porre in essere
ISO/IEC 27002:2013	***Information technology - Security techniques - Code of practice for information security management***. Code of Practice dell'ISO 27001, riporta le best practices di sicurezza per l'implementazione dei controlli di sicurezza previsti dall'ISO 27001
ISO 31000:2009	***Risk management - Principles and guidelines***. Standard internazionale che definisce i principi e le linee guida per il Risk Management
ISO/IEC 27005:2011	***Information technology - Security techniques - Information security risk management***. Standard internazionale che definisce le linee guida per la gestione dei rischi correlati alla sicurezza informatica

Ambito di operatività dei Controlli

- **Ruoli e responsabilità**
- **Formazione e addestramento**
- **Aspetti Contrattuali**
- **Classificazione delle risorse**
- **Sistemi autorizzativi**
- **Sistemi di tracciamento e controllo**
- **Gestione degli incidenti**
- **Sicurezza delle Operazioni**
- **Monitoraggio e verifiche periodiche**

CORRISPONDENZE TRA DELITTI INFORMATICI DELL'ATTUALE CODICE PENALE ITALIANO E DELLA DIRETTIVA 2013/40/EU

	Art.3 Accesso illecito a sistemi di informazione	Art 4 Interferenza illecita relativamente ai sistemi	Art 5 Interferenza illecita relativamente ai dati	Art. 6 Intercettazione illecita	Art 7 Strumenti utilizzati per commettere i reati
615-ter Accesso abusivo ad un sistema informatico o telematico	X				
615-quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici					X
615-quinquies Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico					X
617-quater Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche				X	
617-quinquies Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche					X
635-bis Danneggiamento di informazioni, dati e programmi informatici			X		
635-ter Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità			X		
635-quater Danneggiamento di sistemi informatici o telematici		X			
635-quinquies Danneggiamento di sistemi informatici o telematici di pubblica utilità		X			
491-bis Documenti informatici					
640-ter Frode informatica					
640-quinquies Frode informatica del soggetto che presta servizi di certificazione di firma elettronica					

Direttiva 2013/40/CE

RESPONSABILITÀ DELLE PERSONE GIURIDICHE (ART.10)

1. Gli Stati membri adottano le misure necessarie ad assicurare che le persone giuridiche possano essere ritenute responsabili dei reati di cui agli **articoli da 3 a 8**, commessi a loro vantaggio da qualsiasi persona, che agisca a titolo individuale o in quanto membro di un organismo della persona giuridica, e **che detenga una posizione dominante in seno alla persona giuridica** basata:

a) sul potere di rappresentanza della persona giuridica;

b) sul potere di prendere decisioni per conto della persona giuridica;

c) sul potere di esercitare il controllo in seno alla persona giuridica.

2. Gli Stati membri adottano le misure necessarie ad assicurare che le persone giuridiche possano essere ritenute responsabili qualora la **mancata sorveglianza o il mancato controllo da parte di una persona di cui al paragrafo 1 abbia permesso la commissione, da parte di una persona sotto la sua autorità**, di uno dei reati di cui agli **articoli da 3 a 8** a vantaggio di tale persona giuridica.

3. La responsabilità delle persone giuridiche a norma dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali contro le persone fisiche che siano autori o istigatori o abbiano concorso in uno dei reati di cui agli articoli da 3 a 8.

Modello organizzativo Dlgs 231/01 e controlli CSA-CCM

https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/

Classi di requisiti CSA-CCM	% di requisiti direttamente coinvolti per la conformità al D.Lgs 231/01
Application & Interface Security	50%
Audit Assurance & Compliance	67%
Business Continuity Management & Operational Resilience	25%
Change Control & Configuration Management	20%
Data Security & Information Lifecycle Management	50%
Datacenter Security	89%
Encryption & Key Management	75%
Governance and Risk Management	83%
Human Resources	42%
Identity & Access Management	85%
Infrastructure & Virtualization Security	75%
Interoperability & Portability	0%
Mobile Security	50%
Security Incident Management, E-Discovery & Cloud Forensic	60%
Supply Chain Management, Transparency and Accountability	22%
Threat and Vulnerbility Management	67%

Fine intervento di
Gloria Marcoccio e Claudia Ciampi
Grazie per l'attenzione!

Inizio intervento di Giuseppe Serafini

IT & Law

L'informatica e la telematica sono ormai **trasversali** nei processi aziendali e si assiste quindi ad un sempre maggiore ricorso, per ragioni di efficienza ed efficacia, a soluzioni (**contratti**) di delocalizzazione delle attività di elaborazione e/o di archiviazione dei dati, da parte delle imprese.

Digit 

Frequentemente, una condotta, si può esprimere attraverso strumenti elettronici di elaborazione e, può essere provata, nei suoi elementi costitutivi, solo facendo ricorso ad operazioni di ***digital forensics***; vale a dire, rinvenendo le evidenze, della condotta stessa in sistemi elettronici di elaborazione, sempre più spesso nella disponibilità, di soggetti).

IT Contract

I contratti relativi al settore IT rientrano nella categoria dei **c.d. contratti atipici**, vale a dire non disciplinati direttamente dal Codice Civile, di conseguenza, spetta alle parti prima, nel **contratto**, ed al Giudice poi, in caso di contenzioso, stabilire, sulla base degli accordi (se) intercorsi, i termini dell'adempimento, dell'inadempimento, della responsabilita', e dell'eventuale risarcimento del danno.

D. Lgs. 231/01

Il decreto, si caratterizza, per avere introdotto, un *tertium genus* di responsabilità, destinata a soggetti diversi dalle persone fisiche, conseguente da reato, che coniuga i tratti essenziali del sistema penale e di quello amministrativo.

Si imputa all'ente il ***deficit organizzativo*** di non avere predisposto un insieme di accorgimenti preventivi idonei ad evitare la commissione di reati del tipo di quello realizzato.

Art. 5 D. Lgs. 231/01

L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

(a). - Da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente (...) ;

(b). - Da persone sottoposte alla ***direzione o alla vigilanza di uno dei soggetti di cui alla lett. a)***".

D. Lgs. 196/2003
Art. 29 - Resp. Est.

Provv. 27.11.2008
A.G.P.D.P. - *Amm. di sistema*.

Art. 7 D. Lgs. 231/01

(1). - Nel caso previsto dall'articolo 5, comma 1, lettera b), l'ente è responsabile se la commissione del reato e' stata resa possibile dall'**inosservanza degli obblighi di direzione o vigilanza**.

(2). - In ogni caso, e' esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha **adottato ed efficacemente attuato** un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Art. 7 D. Lgs. 231/01

4. L'efficace attuazione del modello richiede:

(a). - una **verifica periodica** e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;

(b). - un sistema disciplinare idoneo a sanzionare il **mancato rispetto** delle misure indicate nel modello.

231 - “Computer Crimes”

Art. 24 - Bis

- **615 - ter**
- **617 - quater**
- **617 - quinquies**
- **635 - bis,**
- **635 - ter,**
- **635 - quater e**
- **635 - quinquies**
- **615 - quater**
- **615 - quinquies**
- **491 - bis**
- **640 - quinquies**

“Focus on”

(b). - persone sottoposte alla ***direzione o alla vigilanza di uno dei soggetti di cui alla lett. a)***”.

D. Lgs. 196/2003
Art. 29 - Resp. Est.

Provv. 27.11.2008
A.G.P.D.P. - *Amm. di sistema*.

Art. 29 D. Lgs. 196/2003

(2). - soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il ***profilo relativo alla sicurezza***.

(4). - I compiti affidati al responsabile sono **analiticamente specificati per iscritto dal titolare**.

(5). - Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, ***anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni***.

Sicurezza..?

se è vero che la sicurezza informatica e telematica (e quindi, in generale, la prevenzione da utilizzi indebiti dei dati), di uno specifico ambito, ad esempio, quello relativo ai pagamenti con carta di credito è “normata” da una serie di prescrizioni che sono applicabili al quel settore, in forza di vincoli contrattuali, ovvero in forza dei richiami al progresso tecnico ed alla natura dei dati oggetto di trattamento, contenuti nel citato articolo 31 del codice della privacy, sembra ragionevole ritenere, che con specifico riferimento ai reati c.d. informatici propri, previsti dal D. Lgs. 231/2001, occorrerà documentare, l'effettuazione, almeno di tutti quei controlli che lo standard stesso impone con riferimento alla prevenzione delle condotte degli utilizzatori che integrano fattispecie di reato.

Al contrario, la mancanza di misure logiche ed organizzative, apprezzabili e documentate, riferibili alla specifica attività svolta dall'ente, e prescritte dallo standard del settore di riferimento, renderà, ad avviso di chi scrive, assai ardua, se non impossibile, la dimostrazione dell'ottemperanza, da parte dell'Organismo di Vigilanza, al dovere di prevenzione controllo che su di esso incombe con riferimento alla commissione dei reati presupposti.

Sys Admin

Figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

ad. es.: ***amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.***

Esterno

Interno

(e). - Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di **verifica** da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Digital forensics & 231

Ma ... allora...

Come si dovrà procedere allorchè si renda necessario accertare e documentare la violazione del modello organizzativo da parte di uno dei soggetti indicati dall'art. 5, ***se la condotta del reato presupposto realizzata dall'autore del crimine si esprime attraverso strumenti elettronici di elaborazione o integra gli estremi di un reato informatico***?

… quindi ….

Un organismo di vigilanza ma prima ancora un modello organizzativo di gestione e controllo ***può non prevedere procedure ad hoc di investigazione digitale per la verifica delle operazioni svolte dai soggetti di cui all'art. 5 e/o per l'eventuale accertamento/documentazione delle stesse in funzione dell'esonero da responsabilità?***

Grazie per l'attenzione