PARTE SPECIALE

REATI IN TEMA DI CRIMINALITÀ INFORMATICA E DI TRATTAMENTO ILLECITO DI DATI

Parte speciale J
REATI IN TEMA DI CRIMINALITÀ INFORMATICA E DI TRATTAMENTO ILLECITO DI DATI

La “parte speciale J” è dedicata alla trattazione dei reati in materia di criminalità informatica e di trattamento illecito di dati così come individuati nell’art. 24 *bis* d.lgs. n. 231 del 2001.
Di seguito viene riportato l’elenco delle fattispecie criminose prese in considerazione dalle suddette disposizioni, le modalità attraverso le quali queste fattispecie criminose possono essere compiute nonché le “macro aree” sensibili, i ruoli aziendali coinvolti e i “protocolli di prevenzione” attuati all’interno della Società. Infine, vengono riportati anche i c.d. “processi strumentali”, i “principi generali di comportamento” e i “compiti dell’Organismo di Vigilanza.

Ai fini del presente documento si considera Protocollo di prevenzione “una specifica connotazione di una variabile organizzativa, secondo cui è progettata l’attività sensibile o che agisce sugli output della stessa, con l’effetto di azzerare o ridurre la probabilità o la frequenza con cui può essere compiuto un reato del catalogo di cui al d.lgs. n. 231 del 2001”.

Art. 491-bis c.p.: Falsità in un documento informatico pubblico o avente efficacia probatoria
Testo della norma del Codice Penale
Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Descrizione
La norma attribuisce la natura di documento informatico a qualsiasi specie di supporto (disco fisso, floppy disk, nastro, CD, disco ottico, …) che contenga dati, informazioni e relativi specifici programmi di elaborazione.

Anche il possibile abuso della firma elettronica è ascrivibile nell’ambito del falso.
L'articolo in questione è ad inserirsi nell'ambito del Capo III "Della falsità in atti" contenuto nel Titolo VII "Dei delitti contro la fede pubblica" del codice penale e richiama i seguenti articoli del Codice penale:

- Art. 476. Falsità materiale commessa dal pubblico ufficiale in atti pubblici;
- Art. 477. Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative;
- Art. 478. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privatie in attestati del contenuto di atti;
- Art. 479. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici;
- Art. 480. Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative;
- Art. 481. Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità;
- Art. 482. Falsità materiale commessa dal privato;
- Art. 483. Falsità ideologica commessa dal privato in atto pubblico;
- Art. 484. Falsità in registri e notificazioni;
- Art. 485. Falsità in scrittura privata;
- Art. 486. Falsità in foglio firmato in bianco. Atto privato;

- Art. 487. Falsità in foglio firmato in bianco. Atto pubblico;
- Art. 488. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali;
- Art. 489. Uso di atto falso;
- Art. 490. Soppressione, distruzione e occultamento di atti veri;
- Art. 492. Copie autentiche che tengono luogo degli originali mancanti;
- Art. 493. Falsità commesse da pubblici impiegati incaricati di un servizio pubblico.

Art. 476 c.p.: Falsità materiale commessa dal pubblico ufficiale in atti pubblici(richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni.

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale, con il quale può concorrere l'estraneo qualora, con la propria attività, abbia cooperato ad offendere il bene giuridico protetto. Non occorre che il pubblico ufficiale sia l'autore materiale del delitto, ma è sufficiente che la sua partecipazione sia determinata dalla sua qualità particolare.

Descrizione

Il reato si identifica nel falso materiale, il quale può manifestarsi nella forma della contraffazione, quando proviene da un autore diverso da quello reale, o della alterazione, quando subisce, dopo la sua formazione, modificazioni di qualsiasi specie, anche da parte dello stesso autore reale, senza autorizzazione degli aventi diritto.

Esemplificazioni

Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo in concorso con un pubblico ufficiale, falsifica il modulo con cui dà atto del pagamento della somma dovuta per imposte da parte del contribuente suo cliente, il quale, in cambio, investe il proprio denaro in prodotti della società medesima.

Art. 477 c.p.: Falsità materiale commessa dal pubblico ufficiale in certificati oautorizzazioni amministrative (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

Per ciò che concerne la falsa attestazione, mediante contraffazione od alterazione, ci si riferisce ad esempio alle legalizzazioni di firme, alle vidimazioni, al pagamento di tasse.

È un delitto istantaneo, poiché si consuma nel momento in cui è realizzata la contraffazione o l'alterazione, senza che occorra l'uso dell'atto falso.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame

può manifestarsi nella realtà societaria:

- La Società, agendo in concorso con un pubblico ufficiale, contraffà o altera certificati o autorizzazioni amministrative, ovvero mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità.

Art. 478 c.p.: Falsità materiale commessa dal pubblico ufficiale in copie autentichedi atti pubblici o privati e in attestati del contenuto di atti (richiamato dall'art. 491-bisc.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, nesimula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre ad otto anni.

Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

Per copia si intende la riproduzione fedele ed integrale, avvenuta con ogni mezzo, anche meccanico, di un documento ed è autenticata se rilasciata da un pubblico ufficiale che ne garantisca la conformità all'originale.Gli attestati sono, invece, le certificazioni sintetiche o parziali di altri documenti.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo in concorso con un pubblico ufficiale, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblicoo privato diversa dall'originale.

Art. 479 c.p.: Falsità ideologica commessa dal pubblico ufficiale in atti pubblici(richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

La condotta del pubblico ufficiale integra il reato se attesta falsamente che un atto è stato da lui compiuto o èavvenuto in sua presenza.

Le altre ipotesi sono rappresentate dalla falsa attestazione di dichiarazioni non ricevute, dall'omissione o alterazione di dichiarazioni ricevute e, infine, dalla falsa attestazione di fatti dei quali l'atto è destinato a provare la verità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo in concorso con un pubblico ufficiale e ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da essa compiuto o è

avvenuto in sua presenza, o attesta come da essa ricevute dichiarazioni non rese, ovvero omette o altera dichiarazioni da essa ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità.

Art. 480 c.p.: Falsità ideologica commessa dal pubblico ufficiale in certificati o inautorizzazioni amministrative (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.

Autore del reato

Soggetto attivo del reato è il pubblico ufficiale.

Descrizione

L'oggetto di tale reato ha la stessa natura di quello di cui all'art. 479 c.p.

La condotta tipica consiste nella falsa attestazione, ad opera del pubblico ufficiale nell'esercizio delle sue funzioni, in certificati o autorizzazioni amministrative, di fatti dei quali l'atto è destinato a comprovarne la verità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo in concorso con un pubblico ufficiale, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità.

Art. 481 c.p.: Falsità ideologica commessa da persone esercenti un servizio dipubblica necessità (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino ad un anno o con la multa da € 51,00 a € 516,00.
Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.

Autore del reato

L'illecito in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

La condotta tipica consiste nella falsa attestazione in un certificato, da parte di colui che esercita una professione sanitaria o forense od altro servizio di pubblica necessità dei fatti dei quali l'atto è destinato a provare la verità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, nell'esercizio di un servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità (ai sensi dell'art. 359 c.p., agli effetti della legge penale, sono persone che esercitano un servizio di pubblica necessità: a) i privati che esercitano […] professioni il cui esercizio sia per legge vietato senza una speciale abilitazione dello Stato, quando dell'opera di essi il pubblico sia per legge obbligato a valersi; b) i privati che, non esercitando una pubblica funzione, né prestando un pubblico servizio,

adempiono un servizio dichiarato di pubblica necessità mediante un atto della pubblica amministrazione).

Art. 482 c.p.: Falsità materiale commessa dal privato (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale
Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.

Autore del reato
Soggetto attivo del reato è il privato ovvero pubblico ufficiale fuori dell'esercizio delle sue funzioni.

Descrizione
La norma punisce il privato che commette alcuno dei fatti preveduti dagli artt. 476, 477 e 478 c.p.; lecondotte sono le stesse previste dai tre articoli richiamati, essendo diverso solo il soggetto attivo del reato.
Esemplificazioni
Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale soggetto privato, forma, in tutto o in parte, un atto falso o altera un atto vero.

Art. 483 c.p.: Falsità ideologica commessa dal privato in atto pubblico
Testo della norma del Codice Penale
Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.
Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.

Autore del reato
Il reato in esame è un illecito comune, ossia può essere commesso da "chiunque".

Descrizione
Il reato ricorre qualora il privato attesti falsamente al pubblico ufficiale, in atto pubblico, fatti che l'attestante ha il dovere giuridico di esporre veridicamente e dei quali l'atto, in cui tali attestazioni sono inserite, è destinato a provare la verità.

.

Esemplificazioni
Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo quale soggetto privato, attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità.

Art. 484 c.p.: Falsità in registri e notificazioni
Testo della norma del Codice Penale
Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00.

Autore del reato
Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione
Il reato può essere compiuto solo da colui che per legge è obbligato a fare registrazioni in relazione ad una sua qualsiasi attività e da colui che, pur per legge, sia obbligato a comunicare all'Autorità di PS fatti inerenti ad una attività industriale, commerciale o professionale. L'obbligo di fare le registrazioni o le notificazioni deve derivare da una norma giuridica.
Il reato consiste nello scrivere o nel lasciare scrivere (cioè nel caso in cui il soggetto obbligato, potendo impedire la perpetrazione del falso, non la impedisce) false indicazioni nelle registrazioni soggette all'ispezione dell'Autorità, ovvero false indicazioni nelle notificazioni all'Autorità circa le proprie operazioni industriali, commerciali o professionali.

Esemplificazioni
Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società – obbligata per legge a fare registrazioni soggette all'ispezione dell'autorità di pubblica sicurezza, o a fare notificazioni all'autorità stessa circa le proprie operazioni industriali, commerciali o professionali – scrive o lascia scrivere false indicazioni.

Art. 485 c.p.: Falsità in scrittura privata
Questo articolo è stato abrogato dall'art. 1 comma 1 lett. a) d.lgs. n. 7/2016.

Art. 486 c.p.: Falsità in foglio firmato in bianco. Atto privato
Questo articolo è stato abrogato dall'art. 1 comma 1 lett. a) d.lgs. n. 7/2016.

Art. 487 c.p.: Falsità in foglio firmato in bianco. Atto pubblico (richiamato dall'art.491-bis c.p.)

Testo della norma del Codice Penale
Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.

Autore del reato
Soggetto attivo del reato è il pubblico ufficiale.

Descrizione
Essendo l'autore del reato il pubblico ufficiale, il possesso del foglio firmato in bianco deve essere dovuto ad una ragione d'ufficio. È necessario che l'agente abbia scritto o fatto scrivere un atto pubblico; non occorre che venga fatto uso del documento.
Il delitto si consuma nel tempo e nel luogo dell'avvenuto riempimento non autorizzato.

Esemplificazioni
Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, agendo in concorso con un pubblico ufficiale e abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio o per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligata o autorizzata.

Art. 488 c.p.: Altre falsità in foglio firmato in bianco. Applicabilità delle disposizionisulle falsità materiali (richiamato dall'art. 491-bis c.p.) ([1])
Testo della norma del Codice Penale
Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dall'art. 487, si applicano le

disposizioni sulle falsità materiali in atti pubblici

Descrizione

Il reato si verifica quando viene riempito un documento firmato in bianco ad opera di chi non aveva il potere di realizzarlo. Si tratta di una falsità materiale.

Presupposto del reato è che il documento non sia stato acquisito legittimamente ovvero che il riempimento sia stato effettuato senza un valido mandato *ad scribendum*, perché mai esistito o perché non valido in quel momento o dopo che questo sia cessato.

Esemplificazioni

Non si forniscono esemplificazioni del reato in esame poiché l'art. 488 c.p. è una norma di rinvio e le esemplificazioni a riguardo sono già contenute nell'esemplificazioni di carattere generale concernenti le falsità materiali in atti pubblici

(1) Articolo modificato dall'art. 2, comma 1, lett. a) d.lgs. n. 7/2016.

Art. 489 c.p.: Uso di atto falso ([2])

Testo della norma del Codice Penale

Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoliprecedenti, ridotte di un terzo.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Risponde del reato in questione, per l'uso del documento contraffatto, l'autore della contraffazione che non risulti punibile a seguito di estinzione del reato, nonché l'autore della falsificazione tutte le volte in cui il reato di falso è venuto meno (per prescrizione o amnistia) o non è punibile (reato commesso all'estero) e l'autore o concorrente nella falsificazione persiste nel far uso dell'atto falso.

Esemplificazioni

Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, senza essere concorsa nella falsità, fa uso di un atto falso.
-

Art. 490 c.p.: Soppressione, distruzione e occultamento di atti veri ([3])

Testo della norma del Codice Penale

Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero, o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Le condotte previste come punibili sono tre: distruzione, soppressione e occultamento.

Esemplificazioni

Si riporta di seguito un'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero.

---

(2) Articolo modificato dall'art. 2, comma 1, lett. a) d.lgs. n. 7/2016.
(3) Articolo modificato dall'art. 2, comma 1, lett. d) d.lgs. n. 7/2016.

Art. 492 c.p.: Copie autentiche che tengono luogo degli originali mancanti(richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.

Descrizione

Per copia autentica si intende la riproduzione esatta, completa e letterale, tratta dall'originale di un atto pubblico o di una scrittura privata, formata sotto la responsabilità di un pubblico ufficiale o di un incaricato di pubblico servizio competente ad attribuire ad essa la pubblica fede attestandone l'autenticità e da luieffettivamente autenticata.

Esemplificazioni

Non si forniscono esemplificazioni del reato in esame poiché norma di carattere esplicativo. Pertanto è sufficiente riportarne il testo.

Art. 493 c.p.: Falsità commesse da pubblici impiegati incaricati di un serviziopubblico (richiamato dall'art. 491-bis c.p.)

Testo della norma del Codice Penale

Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

Autore del reato

Soggetto attivo del reato è il pubblico impiegato incaricato di esercitare un pubblico servizio.

Descrizione

Questa disposizione equipara gli atti redatti da pubblici impiegati incaricati di pubblico servizio agli atti pubblici, estendendo ai primi la tutela penale predisposta per i secondi.

Esemplificazioni

Non si forniscono esemplificazioni del reato in esame poiché lo stesso non è rilevante per la Società.

Art. 615-ter c.p.: Accesso abusivo ad un sistema informatico o telematico

Testo della norma del Codice Penale

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o

comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Autore del reato
Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione
La qualità soggettiva di cui al comma 2 n. 1) integra una circostanza aggravante.
Il reato si consuma con il semplice accesso ad un sistema telematico o informatico, a prescindere dal fine, purché il sistema sia protetto da misure di sicurezza (è sufficiente anche una protezione semplice, cioè una password).

Esemplificazioni
Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- Il dipendente della Società si introduce nel sistema informatico di una Società concorrente onde apprendere notizie su piani di investimento al fine di rendere più competitiva la propria azienda
- La Società abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza.
-

Art. 615-quater c.p.: Detenzione e diffusione abusiva di codici di accesso a sistemiinformatici o telematici

Testo della norma del Codice Penale
Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a € 5.164,00.
La pena è della reclusione da uno a due anni e della multa da € 5.164,00 a € 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Autore del reato
Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione
Questa norma completa la tutela prevista dalla precedente e punisce l'abusiva acquisizione in qualunque modo (comprensivo dell'autonoma elaborazione) dei mezzi o codici di accesso, che consegue a soggetti non legittimati di inserirsi nel sistema informatico o telematico altrui, vanificando l'ostacolo costituito dalle misure di protezione.

Esemplificazioni
Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Art. 615-quinquies c.p.: Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*Testo della norma del Codice Penale*

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a € 10.329,00.

Autore del reato
Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione
Rispetto alla norma precedente vi è stata un'estensione delle condotte punibili, con l'aggiunta delle locuzioni "si procura, produce, riproduce, importa" oltre a quelle già originariamente presenti di chi "diffonde, comunica, consegna", completando con quella di "mettere a disposizione di altri".
Le predette condotte, per essere punibili, devono essere dirette a danneggiare o interrompere illecitamente un sistema informatico o telematico.

Esemplificazioni
Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società finanzia direttamente o indirettamente – ovvero concorre nel reato agevolandone l'operato – soggetti o strutture che diffondono, comunicano o consegnano programmi informatici da loro stessi o da altri redatti, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.

Art. 617-quater c.p.: Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Testo della norma del Codice Penale
Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
da chi esercita anche abusivamente la professione di investigatore privato.

Autore del reato
Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione
La norma intende tutelare sia la libertà di comunicare che il diritto alla riservatezza delle comunicazioni.
Per essere punibile, tale condotta deve essere realizzata attraverso strumenti di comunicazione di

massa o comunque in grado di raggiungere un numero indeterminato di destinatari, non assumendo rilevanza la merarivelazione eseguita ad uno o più soggetti determinati.

Esemplificazioni
Si riportano di seguito le esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematicoo intercorrenti tra più sistemi, ovvero le impedisce o le interrompe.
- La Società rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi fraudolentemente intercettate.

Art. 617-quinquies c.p.: Installazione di apparecchiature atte ad intercettare,impedire o interrompere comunicazioni informatiche o telematiche

Testo della norma del Codice Penale
Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Autore del reato
Il reato in esame è un reato comune, ossia può essere commesso da “chiunque”.

Descrizione
La condotta consiste nell’installazione di strumenti idonei ad intercettare, impedire o interrompere le comunicazioni; non è necessario il loro effettivo funzionamento, a meno che non si tratti di mezzi tecnici assolutamente incapaci a realizzare una qualsiasi interferenza.

Esemplificazioni
Si riporta di seguito l’esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, fuori dei casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Art. 635-bis c.p.: Danneggiamento di informazioni, dati e programmi informatici
Testo della norma del Codice Penale
Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Autore del reato
Il reato in esame è un reato comune, ossia può essere commesso da “chiunque”.

Descrizione
Oltre alle ipotesi tradizionali di “distruzione” e di “deterioramento”, sono state aggiunte a questa norma anchequelle di “cancellazione, alterazione e soppressione” delle informazioni, dei dati o dei programmi informatici altrui.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui.

Art. 635-ter c.p.: Danneggiamento di informazioni, dati e programmi informaticiutilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Testo della norma del Codice Penale

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

La norma in questione si allinea con il contenuto di cui all'art. 635-bis, con la differenza che, in questo caso, si parla di danneggiamento di dati di pubblica utilità.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Art. 635-quater c.p.: Danneggiamento di sistemi informatici o telematici

Testo della norma del Codice Penale

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Rispetto a quanto previsto e punito nell'art. 635-bis c.p., la norma in questione contempla come condotte punibili anche l'introduzione o la trasmissione di dati, informazioni o programmi.

Si è, inoltre, aggiunta un'ulteriore e nuova ipotesi alternativa, realizzabile quando si ostacola gravemente il funzionamento del sistema.

Esemplificazioni

Si riporta di seguito l'esemplificazioni relative alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, mediante le condotte di cui all'art. 635-bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Art. 635-quinquies c.p.: Danneggiamento di sistemi informatici o telematici dipubblica utilità

Testo della norma del Codice Penale

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.(art. 635 c.p.)Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa, con la reclusione fino a un anno o con la multa fino a € 309,00. La pena è dellareclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso: 1) con violenza alla persona o con minaccia; (omissis)

Autore del reato

Il reato in esame è un reato comune, ossia può essere commesso da "chiunque".

Descrizione

Tale articolo si allinea alla formulazione dell'art. 635-quater c.p. per quanto attiene all'enunciazione dei verbi "distruggere, danneggiare, rendere, in tutto o in parte, inservibili od ostacolarne gravemente il funzionamento".

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società, mediante le condotte di cui all'art. 635-bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ne ostacola gravemente il funzionamento.

Art. 640-quinquies c.p.: Frode informatica del certificatore di firma elettronica

Testo della norma del Codice Penale

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00.

Autore del reato

Il reato in esame è un reato proprio, ossia può essere commesso dal soggetto che presta servizi di certificazione di firma elettronica.

Esemplificazioni

Si riporta di seguito l'esemplificazione relativa alle modalità con cui concretamente il reato in esame può manifestarsi nella realtà societaria:

- La Società – laddove dovesse agire quale soggetto deputato a prestare servizi di certificazione di firma elettronica – al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

2. Le "attività sensibili" in relazione ai reati in tema di criminalitàinformatica e di trattamento illecito di dati e i ruoli aziendali coinvolti

Con riferimento agli illeciti sopra elencati, nell'affrontare l'attività di *risk mapping*, occorre fare alcune considerazioni:

l'utilizzo della strumentazione informatica è ormai talmente generalizzato da estendersi a ogni area e ad ogni processo operativo esistente in qualunque tipo di società pertanto la mappatura dei rischi di commissibilità di reati informatici difficilmente potrà escludere qualche area o qualche processo operativo della società e conseguentemente che non è possibile escludere a priori nessun settore di attività della società dalla mappa di commissibilità di reati informatici presupposto;

la commissione di reati informatici presupposto non può avvenire esclusivamente mediante l'utilizzo dei mezzi informatici messi a disposizione dalla società ai suoi dipendenti o apicali. chi li commette può utilizzare strumenti informatici di sua proprietà e può agire operando al di fuori della società. In tal caso qualsiasi misura preventiva aziendale risulterà inutile;

per quanto riguarda i ruoli aziendali coinvolti nelle suddette fattispecie delittuose, è evidente che i reati richiamati dall'art. 491 *bis* c.p. che, a loro volta, fanno riferimento a comportamenti propri dei pubblici ufficiali, potranno essere compiuti da dipendenti o apicali della società soltanto a titolo di concorso ai sensi dell'art. 110 c.p.;

in generale, i ruoli aziendali coinvolti nei reati qui considerati saranno tutti coloro che, all'interno della società, hanno accesso al sistema informatico.

3. I protocolli preventivi adottati dalla Società

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole stabilite nel Modello di organizzazione, gestione e controllo (di seguito "Modello"), i soggetti aziendali coinvolti nella gestione delle "macro aree" di attività sensibili individuate in relazione ai reati di cui all'art. 24 *bis* del Decreto sono tenuti, al fine di prevenire e impedire il verificarsi dei reati, al rispetto di una serie di "Protocolli preventivi" ("di sistema" o, talvolta, "specifici").

Di seguito è riepilogato il quadro in precedenza esposto.

I Controlli di carattere generale e I Principi di Controllo

La prevenzione dei crimini informatici deve essere svolta attraverso adeguate misure organizzative, tecnologiche e normative. A tal fine la società si è dotata dei seguenti controlli di carattere generale, nonchè dei seguenti principi di controllo.

Controlli di carattere generale

- previsione di un sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino in maniera intenzionale i sistemi di controllo le indicazioni comportamentali forniti;
- predisposizione di adeguati strumenti tecnologici atti a prevenire e/o impedire la realizzazione di illeciti informatici da parte dei dipendenti;
- predisposizione di programmi di informazione, formazione e sensibilizzazione rivolti al personale, al fine di diffondere una chiara consapevolezza sui rischi derivanti d un utilizzo improprio delle risorse informatiche aziendali;

Credenziali di autenticazione

Gli accessi ai dati attraverso gli strumenti elettronici sono consentiti tramite apposite credenziali di autenticazione, che devono essere custoditi con diligenza a cura dei lavoratori / incaricati al fine di assicurarne segretezza.
La politica di generazione e cambio password prevede che queste siano composte da almeno 8 caratteri e abbiano validità non superiore a 90 giorni.

Profilazione utenti

I profili utenti dei lavoratori / Incaricati, sono opportunamente configurati in rapporto al mansionario assegnato.
Ogni utente ha accesso esclusivamente ai dati per i quali è stato abilitato, alla luce della mansione svolta ed ha la facoltà di gestire esclusivamente quei dati ed eseguire quelle transazioni che corrispondono al suo profilo.
In ogni caso gli Incaricati sono tenuti a prestare la massima attenzione nel dar corso ad operazioni - anche potenzialmente possibili- che possono mettere in pericolo la sicurezza, l'integrità e la disponibilità dei dati e delle risorse informatiche.

Internet

La società non presenta alcun regolamento che limiti l'utilizzo di internet.

Posta elettronica

La società non pone limiti all'utilizzo della posta elettronica, e non c'è un regolamento per il suo utilizzo.
Solo per l'utilizzo della Posta Elettronica Certificata l'accesso è solo per l'Amministratore e comunque è sempre tracciato: chiunque accede al servizio viene loggato e memorizzato nel sistema.

Divieto di attività non rientranti nel mansionario

È fatto divieto ai lavoratori non preposti ad attività di manutenzione/gestione del Sistema Informativo, di variare in proprio le configurazioni dei beni facenti parte del sistema informativo aziendale, e di dar corso adinstallazioni, manutenzioni, di software/hardware di qualsiasi tipo.

Protezione, manutenzione, installazione delle risorse informatiche aziendali

Le risorse informatiche aziendali sono protette da rischi di danneggiamento, indisponibilità, violazione, vulnerabilità e intrusione, tramite appositi strumenti / tecnologie software e hardware, di analisi e monitoraggio delle attività, che vengono aggiornati costantemente.

I locali stessi in cui le risorse sono collocati, sono protetti e dotati di sistema antiincendio.
I back up sono giornalieri, e avvengono sia in locale che all'esterno. In più fanno un estrazione dei documenti ogni tre ore.

Disabilitazione dell'accesso agli utenti

In caso di dimissioni/licenziamento dell'utente, si procede prima con un back up e poi alla disattivazione dell'utente, secondo i seguenti passaggi:

- provvede alla periodica cancellazione delle caselle di posta elettronica che risultano ormai inutilizzate;
- provvede al recupero dei dispositivi informatici, ove questi siano stati assegnati al dipendente, trasferendone il contenuto, dopo aver eliminato le precedenti credenziali di accesso, sulla casella di un altro utente.

Comportamenti

I lavoratori / Incaricati al trattamento dei dati, così come il Titolare ed i Responsabili, nel principio della riservatezza, si attengono a quanto segue :

- non comunicano, non diffondono in alcun modo dati personali e/o sensibili, informazioni e/o dati di qualsiasi tipo di cui dovessero venire a conoscenza e/o in possesso da qualsiasi fonte (verbale, cartacea, informatica…) nel corso del rapporto di lavoro;
- non comunicano, non diffondono in alcun modo dati personali e/o sensibili di cui sono a conoscenza per ragioni d'ufficio;
- non lasciano incustoditi o liberamente accessibili supporti cartacei, magnetici o di qualsiasi tipo o natura, terminali, PC o altri strumenti che consentano di accedere o visionare dati personali e/o sensibili.

PROTOCOLLI PREVENTIVI DI SISTEMA

Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi
destinatariSistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei processiSistema disciplinare
Clausola 231/01 nei contratti con i terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale antiriciclaggio

PROTOCOLLI PREVENTIVI SPECIFICI

a) Art. 491-bis c.p.: Falsità in un documento informatico pubblico o avente efficacia probatoria

Oltre ai controlli generali, si applicano i seguenti controlli specifici:

a. misure di protezione dei documenti elettronici (es. firma digitale);

b) Art. 615-ter c.p.: Accesso abusivo ad un sistema informatico o telematico

L'accesso abusivo, oltre ad essere di per sé un illecito, può essere strumentale alla realizzazione di altre fattispecie criminose. I controlli predisposti per prevenire tale fattispecie di reato devono pertanto risultare efficaci anche per la prevenzione di altri reati. Tra tali controlli si segnalano:

- Procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche;
- Rimozione dei diritti di accesso al termine del rapporto di lavoro;
- Aggiornamento regolare dei dispositivi di protezione in uso;
- Modalità di accesso ai sistemi informativi aziendali mediante adeguate procedure di autorizzazione che prevedono la concessione dei diritti di accesso a un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al ruolo ricoperto dal soggetto;
- Procedura per il controllo degli accessi;
- Tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali;

c) Art. 615-quater c.p.: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Oltre ai controlli generali, devono essere applicati i seguenti controlli specifici:

- Inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni;
- rimozione dei diritti di accesso al termine del rapporto di lavoro.

d) Art. 615-quinquies c.p.: Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Oltre ai controlli generali, si applicano i seguenti controlli specifici:

- Formalizzazione di regole al fine di garantire un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- Procedure di controllo della installazione di software sui sistemi operativi;
- Presenza di misure per un'adeguata protezione delle apparecchiature incustodite;
- Previsione di ambienti dedicati che sono considerati sensibili sia per il tipo di dati contenuti sia per il valore di business.

e) Art. 617-quater c.p.: Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Art. 617-quinquies c.p.: Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Oltre ai controlli generale, si applicano i seguenti controlli:

- Utilizzazione di misure di protezione dell'accesso alle aree dove hanno sede informazioni e

strumentidi gestione delle stesse;
- Misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'organizzazione; ;
- Definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte dipersonale all'uopo incaricato;
- Esistenza di procedure di controllo della installazione di software sui sistemi operativi;

f) Art. 635-bis c.p.: Danneggiamento di informazioni, dati e programmi informatici

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

Oltre ai controlli generali, dovrebbero essere applicati i seguenti controlli specifici:
- Formalizzazione di regole per un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- Procedure di controllo della installazione di software sui sistemi operativi;

g) Art. 635-quater c.p.: Danneggiamento di sistemi informatici o telematici

Art. 635-quinquies c.p.: Danneggiamento di sistemi informatici o telematici di pubblica utilità

Oltre ai controlli generali, si applicano i seguenti controlli specifici:
- Definizione di regole per un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- Misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'organizzazione;
- Misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestionedelle stesse;
- Definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte dipersonale all'uopo incaricato;
- Presenza di misure per un'adeguata protezione delle apparecchiature incustodite;
- Previsione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business.

h) Art. 640-quinquies c.p.: Frode informatica del certificatore di firma elettronica

Oltre ai controlli generali, devono essere applicati i seguenti controlli specifici:
- Misure volte alla protezione dei documenti elettronici (es. firma digitale).

GESTIONE SISTEMI INFORMATIVI AZIENDALI

attività sensibili

a) Gestione delle attività di accesso ai sistemi informatici e telematici e loro applicazioni (autenticazione, account e profili)

b) Gestione degli accessi fisici agli strumenti informatici

protocolli preventivi

Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure,oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie dicontrolli specifici e concreti, ovvero:

Nell'espletamento delle rispettive attività/funzioni, i soggetti aziendali che svolgono le loro mansioni all'interno della presente area strumentale sono tenuti al rispetto delle procedure aziendali. Tali procedure, oltre a definire chiaramente ruoli e responsabilità degli attori coinvolti nel processo, prevedono una serie di controlli specifici e concreti, ovvero:

1. la gestione dei sistemi informativi è stata affidata a un consulente esterno alla società;
2. i sistemi sono monitorati e gestiti da un consulente esterno;
3. esistono software per il controllo e le verifiche dello stato dei sistemi informatici.
4. il datacenter è protetto e allarmato e l'accesso è consentito alle sole persone autorizzate;
5. l'accesso alla rete ai sistemi aziendali è soggetto ad autenticazione mediante l'uso di UserID e Password, tramite Active Directory di Microsoft;
6. tutta la rete Palma Boria è gestita a livello globale e protetta da firewall;
7. I back up sono giornalieri, e avvengono sia in locale che all'esterno. In più fanno un estrazione dei documenti ogni tre ore. Ogni dipendente ha un computer e in base alle problematiche fanno richiesta agli amministratori di sistema.
8. Palma Boria ha chiaramente informato gli utenti che, in conformità altresì a quanto previsto da apposita policy aziendale, non è possibile installare nessun software o hardware che non sia stato approvato dai sistemi informativi (ufficio amministrazione e finanza);
9. il sistema di posta elettronica è protetto da un sistema ANTISPAM che filtra preventivamente tutta la posta elettronica indicando lo stato di spam;

protocolli preventivi di sistema

Previsione dei divieti nel Codice etico
Diffusione del Codice etico verso tutti i dipendenti e i terzi
destinatariSistema di deleghe
Informazione e formazione specifica del personale
Segregazione dei compiti tra i differenti soggetti coinvolti nei
processiSistema disciplinare
Clausola 231/01 nei contratti con i
terzi
Gestione delle risorse finanziarie
Tracciabilità/archiviazione
Direttiva aziendale antiriciclaggio

5. I compiti dell'Organismo di Vigilanza

Pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'OdV nel documento approvato dal Amministratore Unico e denominato "Parte speciale B – Struttura, composizione, regolamento e funzionamento dell'Organismo di Vigilanza", in relazione alla prevenzione dei reati di cui alla presente Parte speciale, l'OdV, tra l'altro, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati in tema di criminalità informatica e di trattamento dei dati;
- verificare, in particolare, il rispetto delle regole procedurali e del Modello in ordine ai flussi finanziari aziendali, con riferimento sia ai pagamenti da/verso i terzi sia a quello da/verso le società delGruppo;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi di flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai suoi *sub* responsabili, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema sanzionatorio, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività;
- verificare la correttezza della valutazione della congruità economica degli investimenti effettuati dai soggetti aziendali competenti o dai consulenti all'uopo nominati;
- verificare l'applicazione dei punti di controllo previsti nelle procedure riferibili alla prevenzione dei reati contro la P.A. (parte speciale "E") e ai reati societari (parte speciale "F"), qualora inerenti le medesime attività "sensibili" o "strumentali" rilevanti ai fini della prevenzione dei reati informatici e di trattamento illecito di dati.