PARTE SPECIALE
REATI INFORMATICI

Fattispecie richiamate dall'Art. 24 bis Dlgs 231/01
Il Dlgs 231/01 ha recepito con L. 48/08, art. 7, la Convenzione del Consiglio d'Europa sulla criminalità informatica, redatta a Budapest il 23 novembre 2001.
A seguito della ratifica ed esecuzione della Convenzione suddetta dopo l'art. 24 del Dlgs 231/01 è stato inserito l'art. 24 bis "*Delitti informatici e trattamento illecito dei dati"*.
Il recepimento della convenzione ha quindi esteso la responsabilità amministrativa degli enti ai reati di seguito riportati.

Art. 24 bis comma 1 Dlgs 231/01

Accesso abusivo a un sistema informatico o telematico (art. 615-*ter* cod. 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".
La norma non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "*ius excludendi alios"*, quale che sia il contenuto dei dati.
Il delitto in questione è reato di mera condotta e si perfeziona con la violazione del sistema informatico senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una lesione della stessa.

Definizioni

Sistema informatico

L'art. 1 della Convenzione di Budapest chiarisce che per sistema informatico si considera "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati". Si tratta di una definizione molto generica che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche dispositivi elettronici che siano dotati di software che permette il loro funzionamento elaborando delle informazioni o comandi.

Dato informatico

Sempre nell'art. 1 della Convenzione di Budapest è contenuta anche la definizione di dato informatico: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con sistema informatico, incluso un programma in grado di consentire ad un sistema di svolgere una funzione".

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. 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:

1) 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;

2) 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;

3) da chi esercita anche abusivamente la professione di investigatore privato".

Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* cod. 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'art.617-quater."

Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis*cod. 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 una o più delle circostanze 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 quattro anni e si procede d'ufficio."

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-*ter* cod.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'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore di sistema, la pena è aumentata."

Danneggiamento di sistemi informatici e telematici (art. 635-*quater* cod. 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, 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 una o più delle circostanza di cui al secondo comma dell'articolo 635 c.p., ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da due a sette anni".

Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-*quinquies* cod. penale)

"*Se il fatto di cui all'art.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) dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Gli articoli del Codice Penale summenzionati, previsti nel comma 1 dell'art. 24 bis Dlgs 231/01 hanno come fattore comune il danneggiamento informatico: si

parla di danneggiamento informatico quando, considerando la componente hardware o software, interviene una modifica tale da impedirne il funzionamento, anche solo parziale.

Art. 24 bis comma 2 Dlgs 231/01
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* cod. penale)
"*Chiunque, al fine di procurare a sè 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 euro 5.164..*
La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617quater".
Diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* cod. penale)
"*Chiunque, diffonda, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente 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, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329"*.
Gli articoli del Codice Penale summenzionati previsti nel comma 2 dell'art. 24 bis ex Dlgs 231/01 hanno come fattore comune la detenzione o diffusione di codice o programmi atti al danneggiamento informatico. Da un punto di vista tecnico, gli artt. 615 quater e quinqies possono essere considerati accessori ai precedenti artt. 615 ter, 635 bis, 635 ter e quater: la detenzione o dissezione di codici di accesso o la detenzione o diffusione di programmi o dispositivi diretti a danneggiare o interrompere un sistema telematico, di per sé non compiono alcun danneggiamento, se non utilizzati per un accesso abusivo ad un sistema o nella gestione di un'intercettazione di informazioni.

Documenti informatici (art. 491-*bis* cod. penale).
"*Se alcune 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*".
La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:
- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.):

"*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*";
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.): "*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*";
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.): "*Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula 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 a 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*";
- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.): "*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*";
- Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.): "*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*";
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.): "*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 a 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*";
- Falsità materiale commessa da privato (art. 482 c.p.): "*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*";
- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.): "*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";
- Falsità in registri e notificazioni (art. 484 c.p.): "*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*";
- Falsità in scrittura privata (art. 485 c.p.): "*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata*";
- Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.): "*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito*";
- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.): "*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*";
- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.): "*Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private*";
- Uso di atto falso (art. 489 c.p.): "*Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno*";
- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.): "*Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente*";
- Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.): "*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";
- Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.): "*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*".

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* cod. 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*".

***

Principi di riferimento generali
Ciò posto, con specifico riguardo alle problematiche connesse al rischio informatico, Cooperativa Noncello consapevole dei continui cambiamenti delle tecnologie e dei epericoli che possono derivare dall'(ab)uso di tali strumenti si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi).
Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti di Cooperativa Noncello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-*bis* del D.Lgs. 231/2001); violare i principi e le procedure aziendali previste nella presente parte speciale.
Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:
a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici privati;
c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;
d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei

all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
h) istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.
Pertanto, i soggetti sopra indicati devono:
1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
3. in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;
5. evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa , se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc…);
7. evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi;
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

Le disposizioni del presente regolamento costituiscono specificazioni esemplificative degli obblighi generali di diligenza e fedeltà, il cui adempimento è richiesto dalla legge ai prestatori di lavoro (artt.2104-2105 c.c.) e a quelli di correttezza e buona fede richiesti ai collaboratori a qualsiasi titolo (artt. 1175 e 1375 c.c.)

Coop Noncello non ammette violazioni delle previsioni contenute nel presente regolamento.

Ogni violazione da parte dei dipendenti costituisce infrazione disciplinare e comporta le conseguenze sanzionatorie di cui all'art. 7 legge 300/70 (rimprovero verbale o scritto, multa, sospensione dal servizio e dalla retribuzione, licenziamento), agli artt. 2119 e 2106 c.c., al Dlgs 231/01 ed alla normativa collettiva e regolamentare applicata.

Ogni violazione da parte dei collaboratori, dei borsiti …..è fonte di responsabilità contrattuale e come tale è sanzionata in base ai principi generali del diritto e alle norme che regolano i relativi rapporti contrattuali.

ATTIVITA' SENSIBILI

Di seguito vengono riportate le attività potenzialmente a rischio per la commissione dei reati informatici più sopra richiamati emerse da un'analisi della realtà aziendale, nonché i presidi attualmente adottati per prevenire la realizzazione di tali fattispecie .

Gestione del profilo utente e processo di autenticazione

Il profilo dell'utente è accessibile solamente tramite autenticazione con password su server LDAP.

Solo il proprietario, ovvero il Presidente, e l'amministratore di sistema può vedere i files presenti nella propria home directory.

Ad ulteriore presidio del sistema si rileva che, nel momento in cui viene creato l'utente di sistema, viene attribuita una password standard con scadenza

immediata in modo che al primo accesso il sistema richieda immediatamente di cambiare la password. In questo modo, pertanto, la password è nota soltanto all'utente.
E' fatto assoluto divieto agli utenti di rendere nota la loro password ad altri.
Ed invero, come già sopra precisato, ogni violazione da parte dei dipendenti costituisce infrazione disciplinare e comporta le conseguenze sanzionatorie di cui all'art. 7 legge 300/70 (rimprovero verbale o scritto, multa, sospensione dal servizio e dalla retribuzione, licenziamento), agli artt. 2119 e 2106 c.c., al Dlgs 231/01 ed alla normativa collettiva e regolamentare applicata.
Ogni violazione da parte dei collaboratori, dei borsisti e degli stagisti è fonte di responsabilità contrattuale e come tale è sanzionata in base ai principi generali del diritto e alle norme che regolano i relativi rapporti contrattuali.
Da ultimo, la sicurezza delle password è garantita dal protocollo di cifratura MD5.

Gestione e protezione della postazione di lavoro

Nel caso in cui l'operatore rimanga inattivo per più di tre minuti lo schermo viene bloccato dal salvaschermo ed è necessaria la password per poter accedere al file/programma/sito che si stava utilizzando.

Gestione accessi verso l'esterno

Tutti i computer della sede centrale di Roveredo accedono ad Internet tramite un server proxy che impedisce la navigazione verso siti non autorizzati.
E' in programma di dotare a breve anche la sede di Udine di un server proxy.
I siti ai quali non è consentito l'accesso sono quelli ricompresi in una "lista nera" e quelli il cui nome contiene parole chiave non permesse (ad es. scommesse, giochi, sesso).
Diversamente, i siti ai quali è possibile accedere sono annoverati in una "Lista Bianca."
Il proxy, inoltre, impedisce il Download di files eseguibili che possono compromettere il funzionamento dei computers.
Le uniche postazioni che non passano attraverso il proxy sono quelle dell'amministratore di sistema, del Presidente,una postazione in amministrazione ed una dell'ufficio paghe per consentirne l'accesso a servizi (es. sito INAIL) che non sono configurabili nelle regole del proxy.
In caso di interruzione di connettività della sede centrale alcuni servizi (web, posta..) possono essere deviati verso una linea di backup.

Gestione e protezione delle reti

Tutte le sedi operative accedono ad Internet tramite un router; nelle sedi minori (Conegliano, lavanderia) il router funziona anche da firewall; in quelle più grandi(Udine, Pordenone) è invece presente un distinto firewall per salvaguardare il sistema dagli accessi provenienti dall'esterno.
Nelle sedi di Pordenone e Udine è attivo un hotspot Wifi per il collegamento di dispositivi Wireless; la rete è protetta (ovvero è necessaria un'autenticazione per potersi connettere) e richiede una password di 16 caratteri.

Dispositivi di memorizzazione

Attualmente il backup viene eseguito con le seguenti modalità: backup completo delle cartello di lavoro (con ciò intendendosi cartelle condivise tra più utenti, generalmente all'interno dello stesso ufficio) dei database ogni giorno in ciclo settimanale e una volta alla settimana il backup delle cartelle personale (quelle del desktop).

Il Backup risiede nella sede centrale (Roveredo) ma viene replicato nelle sedi di Udine durante la notte. Il sistema di Udine esegue la stessa operazione e la replica nella sede di Pordenone.
Nei prossimi giorni il sistema verrà cambiato con il seguente sistema:
Backup incrementale di tutti i files ogni giorno; backup completo dei database ogni giorno in ciclo settimanale.

Protezione del sistema

Non è possibile installare software nelle postazioni e nei server se non all'amministratore di sistema.
I server sono collocati in una stanza chiusa climatizzata chiusa a chiave; le chiavi sono in possesso dell'amministratore di sistema e del responsabile della sicurezza.
I server e le postazioni sono alimentate tramite gruppi di continuità distinti che le pongono al riparo da picchi di tensione e impediscono spegnimenti repentini del sistema.
Tutti i server sono virtualizzati: esistono diversi backup dei server che permettono un ripristino integrale di tutte le configurazioni su un host standard di virtualizzazione.

INTERVENTI MIGLIORATIVI IN PROGRAMMA

I. Reingenerizzazione del sistema di backup da completo a incrementale.
II. Introduzione di server proxy presso la sede di Udine (il proxy è impostato nel server ma non ancora configurato nelle macchine).
III. Aumento delle postazioni Linux (sistema operativo solido e molto poco vulnerabile) al posto delle postazioni Windows più vulnerabili dai virus.
IV. Standardizzazione delle postazioni e dei dispositivi (omogeneità di nomi macchina,ovvero stilare un inventario aggiornabile di tutti i dispositivi, individuare una forma di installazione standard, nomi stampante…).
V. Creazione di documentazione tecnica specifica per il nostro sistema informatico.
VI. Creazione di documentazione tecnica base per gli utenti del sistema.
VII. Configurazione di un altro server che possa ospitare server virtualizzati per poter rapidamente far fronte ad improvvisi guasti al server principale.
VIII. Configurazione di una serie di regole del firewall per poter rapidamente passare la maggior parte dei servizi internet alla linea adsl di backup.