FONDAZIONE ITS MAKER

Sede Legale in Bologna, Via Bassanelli n. 9/11

MODELLO
DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

sulla "Responsabilità Amministrativa delle Imprese"

Parte Speciale

Delitti informatici
Art. 24-bis del D.Lgs. n. 231/2001

INDICE **PAGINA**

Premessa

Le disposizioni in materia di reati informatici - oggetto di un intervento di riforma ad opera della L. n. 48 del 19 marzo 2008 di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001 – presuppongono un comune riferimento alle definizioni di "sistema informatico" e "dato informatico".

Con la prima espressione, si intende qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati (art. 1 della Convenzione): si tratta di una definizione piuttosto ampia e idonea a comprendere ogni genere di strumento elettronico, informatico o telematico, che sia in grado di elaborare delle informazioni (ad es., anche un palmare o un telefono cellulare che supporta programmi in grado di elaborare dati).

Il "dato informatico", invece, è definito come qualunque rappresentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione (*software*).

1. TIPOLOGIA DEI REATI INFORMATICI

Si riporta di seguito una breve descrizione dei reati contemplati nell'art. 24 bis del Decreto 231/01 la cui commissione possa comunque comportare un interesse e/o un vantaggio per la Società.

a. Reati di intrusione illecita

Accesso abusivo ad un sistema informatico o telematico (Art. 615 ter c.p.)

"*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."

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615 quater c.p.)
"*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 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'articolo 617-quater."

Si tratta di disposizioni introdotte dall'art. 4 della L. 547/1993 al fine di adeguare il codice penale alla progressiva diffusione della tecnologia informatica.

Nello specifico, **l'art. 615 ter c.p**. prevede come reato la condotta di chi si introduce abusivamente in un sistema informatico o telematico altrui (purché sia protetto), ovvero di chi vi permane contro la volontà di chi ha il diritto ad escluderlo. In sostanza, la fattispecie intende sanzionare chi viola la riservatezza delle comunicazioni o delle informazioni altrui, che sempre più di frequente vengono trasmesse attraverso sistemi informatici protetti.
Peraltro, la norma prescinde dalla rivelazione a terzi delle informazioni abusivamente captate, essendo rilevante anche solo l'accesso effettuato in assenza di autorizzazioni (es. credenziali di autenticazione) ovvero in presenza di autorizzazioni per una funzione diversa da quella per cui si esegue l'accesso.
La configurabilità del reato, inoltre, prescinde dal danneggiamento o dalla distruzione dei sistema o dei dati, che costituiscono, invece, circostanze aggravanti che danno luogo ad un aumento di pena. La pena è aumentata anche se il fatto è commesso con abuso della qualità di operatore del sistema

(qualifica rivestita da chi professionalmente o per le funzioni di fatto esercitate di trova ad intervenire in via non occasionale su dati e programmi – es. programmatore, sistemista, analista etc.).

L'accesso abusivo può essere effettuato sia in modo "virtuale" (es. tramite un atto di hackeraggio) che in modo "fisico" o materiale, cioè ad esempio, mediante l'abusiva introduzione nei locali in cui si trova l'elaboratore.

L'art. 615 quater c.p., invece, mira a sanzionare le condotte preparatorie e strumentali all'acceso abusivo, consistenti nella detenzione o diffusione, sotto svariate forme (acquisizione, riproduzione, diffusione, comunicazione o consegna) di codici di accesso (quali password, PIN, etc.) mediante i quali è possibile superare i dispositivi di protezione di cui può essere dotato un sistema informativo. Anche in tal caso, la condotta è punita indipendentemente dal verificarsi dell'accesso, in quanto idonea a creare una situazione di pericolo per il bene protetto.

b. Reati di danneggiamento informatico

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

"*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 euro 10.329*."

Danneggiamento di informazioni, dati e programmi informatici (Art. 635 bis c.p.)

"*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 il fatto è commesso con violenza alle persone o minacce ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni."

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

"*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 il fatto è commesso con violenza alle persone o minacce ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata."

Danneggiamento di sistemi informatici o telematici (Art. 635 quater c.p.)
"*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 il fatto è commesso con violenza alle persone o minacce ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata."

Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635 quinquies c.p.)
"*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 il fatto è commesso con violenza alle persone o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata."

Tali disposizioni mirano a sanzionare le diverse figure di danneggiamento informatico, nonché le condotte che lo rendono possibile. Nello specifico:

- **l'art. 615 quinquies** reprime, in via preventiva, una serie di condotte che non costituiscono ancora danneggiamento ma sono considerate intrinsecamente pericolose per l'integrità di dati, programmi e sistemi informatici. In particolare, costituisce reato l'acquisizione, la produzione, la riproduzione, l'importazione, la consegna, la comunicazione o la messa a disposizione di programmi informatici (es. virus), dispositivi o apparecchiature qualora tali condotte siano effettuate allo scopo di danneggiare dati, programmi oppure sistemi informatici. Stante il carattere "preventivo" di tale disposizione, la condotta acquista rilievo anche nel caso in cui il danneggiamento non si sia mai verificato;

- **l'art. 635 bis** punisce chiunque distrugge, deteriora o rende inservibili informazioni, dati, o programmi informatici altrui (con l'esclusione dei sistemi informatici, il cui danneggiamento è sanzionato più gravemente da una successiva fattispecie);
- **l'art. 635 ter** sanziona chiunque commette un fatto diretto a danneggiare informazioni, dati, o programmi informatici utilizzati dallo Stato o da altro ente pubblico, anche nel caso in cui il danneggiamento in concreto non si verifichi. Rispetto alla norma precedente, dunque, la soglia della punibilità è arretrata a condotte meno offensive (non si richiede il danneggiamento ma il semplice compimento di atti diretti a danneggiare) in considerazione della natura pubblica o di pubblica utilità dei dati e programmi "attaccati". Qualora il danneggiamento si verifichi, tuttavia, la pena è aumentata;
- **l'art. 635 quater** punisce il danneggiamento di sistemi informatici realizzato mediante l'introduzione o la trasmissione di dati o programmi ovvero mediante le condotta di cui all'art. 635 bis (distruzione, danneggiamento, deterioramento, cancellazione, alterazione, soppressione di dati o programmi). Rispetto a tale articolo, l'art. 635 quater prevede pene più elevate, in quanto il danneggiamento non riguarda il mero dato o programma, ma l'intero sistema informatico;
- **l'art. 635 quinquies** sanziona le medesime condotte dell'articolo precedente se dirette a danneggiare un sistema informatico dello Stato o comunque di pubblica utilità. In tal caso, tuttavia, il fatto è punito anche se il danneggiamento non si realizza, per il solo fatto di avere esposto a pericolo il sistema. Ciò in ragione dell'importanza attribuita al regolare funzionamento dei servizi pubblici e di pubblica utilità che si svolgano attraverso sistemi informatici. Se il danneggiamento si verifica, la pena è aumentata.

c. Reati a tutela della libertà e segretezza delle comunicazioni

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

"*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 ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617 quinquies c.p.)
"*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."

Gli artt. **617 quater e 617 quinquies c.p.** tutelano l'inviolabilità e la segretezza delle comunicazioni che avvengono mediante sistemi informatici e telematici, oggetto di protezione – al pari di ogni forma di comunicazione – anche da parte dell'art. 15 della Costituzione.

Nello specifico:

- **l'art. 617 quater** punisce chiunque impedisce, interrompe o intercetta in modo fraudolento comunicazioni relative ad un sistema informatico o telematico. La norma punisce, inoltre, chiunque riveli al pubblico il contenuto di tali comunicazioni. Sono previste delle aggravanti che comportano un aumento di pena, tra cui l'abuso della qualità di operatore di sistema. L'intercettazione consiste nella presa di conoscenza, con o senza registrazione, delle comunicazioni indicate e deve essere fraudolenta, cioè avvenire in maniera occulta e artificiosa;
- **l'art. 617 quinquies** punisce l'installazione abusiva di apparecchiature atte ad intercettare, interrompere o impedire comunicazioni relative a sistemi informatici o telematici, sanzionando, in tal modo, le attività preparatorie all'intercettazione o all'interruzione delle comunicazione. Il reato, perciò, si consuma quando l'installazione dell'apparecchio è completata, a prescindere dal suo effettivo funzionamento.

d. Frode informatica nei servizi di certificazione

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640 quinquies c.p.)

"*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 a 1.032 euro*."

Tale disposizione punisce la condotta del soggetto incaricato di prestare servizi di certificazione di firma elettronica che violi gli obblighi previsti dalla legge per il rilascio del certificato. La violazione è punita solamente se effettuata con il fine di procurare a sé o altri un profitto o di arrecare ad altri un danno. Si tratta, dunque, di un reato che può essere compiuto solo da soggetti in possesso della qualifica di certificatore, ma ad esso possono concorrere anche soggetti privi della qualifica, ad esempio, istigando o sollecitando il certificatore a commettere il reato.

e. Delitti di falso

Documenti informatici (Art. 491 bis c.p.)

"*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici*."

L'art. 419 bis c.p. estende le norme in materia di delitti di falsità in atti ai documenti informatici, da intendersi come ogni rappresentazione di dati, informazioni o concetti suscettibili di essere utilizzata in un sistema o con un programma informatico.

Si tratta di una serie di reati posti a tutela della fede pubblica documentale, cioè della fiducia e sicurezza che le persone ripongono in determinati documenti, alla luce dell'efficacia probatoria riconosciuta dall'ordinamento (e, in particolare, ad atti pubblici, ma anche certificati ed autorizzazioni amministrative).

In termini generali, il falso può ricadere sia sul contenuto "ideologico" dell'atto (es. un atto perfettamente integro e genuino ma non veritiero nel suo contenuto), oppure nella materialità dell'atto (es. un documento originariamente vero nel suo contenuto, ma successivamente contraffatto o alterato mediante cancellature o abrasioni).

Anche con specifico riguardo ai documenti informatici, il falso può ricadere sulla veridicità del contenuto dell'atto (e in ciò non differisce dal falso "cartaceo"), oppure sulla genuinità esteriore dell'atto, e in ciò si rivela anche più insidioso del falso "ordinario". Infatti, un documento informatico contraffatto può apparire in tutto e per tutto simile a quello originale.

La nozione di documento informatico si ricava dall'art. 1, lett. p) del D.Lgs. 7 aprile 2005, n. 82 ("Codice dell'amministrazione digitale"), che lo definisce come una "*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"*.

L'art. 491bis c.p., inoltre, precisa che, per essere rilevante, il falso deve avere ad oggetto un documento informatico dotato di efficacia probatoria. In proposito, il documento informatico può ritenersi dotato di efficacia probatoria quando sia formato nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore e l'integrità del documento (art. 20 Codice dell'Amministrazione Digitale).

Di seguito riportiamo una elencazione dei delitti di falso richiamati dall'art 491bis precedentemente descritto:

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 in 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 dal 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 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 dall'articolo 487 si applicano le disposizioni sulle falsità materiali in atti pubblici."

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."

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."

2. PRINCIPALI ATTIVITA' A RISCHIO AI SENSI DEL DECRETO 231/2001.

Tutto lo Staff di ITSMAKER (Direzione, referenti di funzione e personale in convenzione, collaboratori con incarichi funzionali continuativi presso l'Ente), opera su dispositivi portatili personali o forniti dall'Organizzazione, configurati per l'accesso a banche dati remote che consentono la condivisione dei documenti di progettazione e strumenti di gestione delle attività formative.
In specifico, lo Staff della Fondazione ITSMAKER opera con le seguenti diverse categorie di Sistemi Informativi:

1. I Sistemi informativi della PA locale o nazionale (SIFER- INDIRE) cui accedono direttamente gli Operatori tramite credenziali assegnate ai Referenti locali delle attività di coordinamento didattico e alla Direzione,
2. Il sistema informativo amministrativo di gestione delle commesse /Incarichi fornitori (GECO-IAL) cui accedono gli Operatori tramite credenziali assegnate ai Referenti locali delle attività di coordinamento didattico,
3. Il Sistema informativo di Content Sharing Microsoft SharePoint /Onedrive cui accedono tutti gli Operatori con credenziali gestite dal Responsabile dei Sistemi Integrati.

L'accesso ai PC e la loro configurazione è invece regolamentata dal Consulente esterno informatico (IAL).
La Fondazione ITSMAKER ha individuato come Amministratori di Sistema:

- Il Consulente Esterno (IAL) per quanto riguarda la configurazione fisica degli strumenti di lavoro e l'accesso ai servizi amministrativi (GECO-IAL)
- Il Consulente esterno (Referente Sistemi Integrati) per quanto riguarda la gestione degli strumenti cloud di condivisione dei contenuti (SHAREPOINT/ONEDRIVE)

In considerazione della tipologia di attività svolta da ITS MAKER è astrattamente ipotizzabile la commissione dei seguenti reati oggetto di questa parte Speciale:

- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinqies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);

- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di sistemi informatici e telematici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- falso in documenti informatici (art. 491 bis c.p.),

attraverso:
- la gestione delle credenziali di autenticazione e autorizzazione per l'accesso a sistemi informatici;
- la gestione dei sistemi hardware e software aziendali e delle relative licenze;
- l'eventuale utilizzo di dispositivi di firma digitale;
- la protezione degli accessi fisici ai dati;

Tuttavia, va precisato che l'utilizzo della strumentazione informatica, e con esso il rischio reato, è ormai talmente generalizzato nello svolgimento delle varie attività aziendali da estendersi sostanzialmente ad ogni area e processo operativo della Fondazione, soprattutto in considerazione dell'utilizzo dell'informatica quale mezzo di insegnamento e/o strumento di comunicazione con i docenti e gli alunni.

Comportano, pertanto un particolare rischio di commissione dei reati informatici (ad esempio in relazione alla possibile creazione o utilizzo di documenti falsi ex art. 491-bis c.p.) quelle attività che prevedono l'utilizzo di dispositivi di firma digitale e l'accesso a sistemi informatici o telematici della P.A. (es. in ambito fiscale, contributivo, per la trasmissione dei dati alle Pubbliche Amministrazioni, ovvero per la partecipazione a bandi e/o per la rendicontazione etc.).

Aree sensibili

Per quanto sopra citato, il rischio si può presentare in misura maggiore, nelle seguenti aree:

- In generale sui tutti i Sistemi Informativi e per tutti i soggetti, Partner e Consulenti che hanno accesso alle risorse informatiche o utilizzano dispositivi di firma digitale messi a disposizione della Fondazione per l'espletamento dell'attività lavorativa;
- In specifico per i Sistemi Gestionali/Amministrativi (Amministrazione, Finanza, Controllo e rendicontazione),

e rispetto ai seguenti soggetti:

- Docenti, Tutor, Coordinatori
- Consulenti esterni dotati di delega in materia di firma digitale;

Stante l'utilizzo generalizzato della strumentazione informatica nello svolgimento delle varie attività aziendali, le funzioni e Aree a rischio di reato sono quindi da estendere sostanzialmente ad ogni funzione ed ufficio operativo della Società.

3. SISTEMI DI CONTROLLO.

La Fondazione ITSMAKER si è dotata di specifici Modelli Organizzativi atti alla tenuta sotto controllo delle aree di rischio definite in questa Parte Speciale:

- Il Modello di Organizzazione e Gestione per la Qualità In conformità alla Normativa ISO 9001
- Il Modello Organizzativo Privacy in conformità al Regolamento UE 2016/679
- Il Modello per la gestione della Sicurezza ai sensi del Dlgs 81/08
- Il Modello Di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

I Destinatari di questa Parte Speciale devono inoltre specificatamente attenersi al REGOLAMENTO AZIENDALE – CODICE ETICO INFORMATICO, che viene consegnato a tutti i collaboratori ed è parte integrante delle procedure operative del Sistema di Gestione Qualità

I docenti e gli allievi che accedono ai laboratori devono invece rispettare il REGOLAMENTO SULL'UTILIZZO DEI LABORATORI.

La Fondazione ITSMAKER ha inoltre adottato quanto previsto dal GDPR (Regolamento generale sulla protezione dei dati):
- nominando il DPO (Responsabile protezione dati), gli Amministratori di Sistema, i Responsabili e gli Incaricati del trattamento
- redigendo e diffondendo presso tutti i collaboratori un Modello Organizzativo Privacy in conformità al Regolamento UE 2016/679 e analizzando le attività tramite un apposito Registro Delle Attività Di Trattamento.

4. PRINCIPI GENERALI DI COMPORTAMENTO E PRESCRIZIONI SPECIFICHE.

Il Sistema di Controllo Interno e di Gestione dei Rischi e le procedure del Sistema Gestione Qualità approvate ed adottate dalla Fondazione ITS Maker sono quindi impostati con l'obiettivo di garantire la maggiore tutela dell'Ente nei confronti del possibile rischio di commissione di reati informatici.

La Fondazione, nello svolgimento della propria attività, si avvale necessariamente di strumenti informatici, tra cui *personal computer*, periferiche, dispositivi di memorizzazione, *software*, posta elettronica, banche dati, rete *internet* e rete informatica aziendale, *fax* e posta vocale nonché ogni altro dispositivo o tecnologia per il trattamento di dati in formato elettronico (di seguito gli "**Strumenti informatici**"), che possono essere accordati in uso ai destinatari della presente Parte Speciale ("**Destinatari**") - per lo svolgimento della rispettiva attività lavorativa, ed è consapevole della necessità che tali Strumenti siano utilizzati in modo lecito e corretto e in modo da prevenire il rischio di un loro utilizzo indebito.
Nell'espletamento della propria attività, gli Amministratori, la Società Responsabile dell'Area Amministrazione e rendicontazione (IAL Emilia Romagna Impresa Sociale), i Sindaci qualora nominati, il revisore unico o la società di revisione e tutti i Dipendenti qualificati che operino nelle aree di attività a rischio sono qualificati come Destinatari di questa Parte Speciale e devono rispettare le norme di comportamento citate.

I Destinatari, pertanto, devono utilizzare gli Strumenti informatici nel rispetto della normativa in vigore (con particolare riferimento alle leggi vigenti in materia di protezione dei dati personali, di illeciti informatici e di diritto d'autore) e hanno il divieto assoluto di cooperare o comunque dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra descritte, ovvero da favorirne o agevolarne la commissione.

I Destinatari devono osservare i principi generali e norme di comportamento di seguito dettate, nel rispetto degli obblighi normativi e delle procedure aziendali:

- osservare scrupolosamente le policy ed i regolamenti dell'Ente per l'utilizzo degli strumenti informatici;
- rispettare le procedure relative ai profili di autenticazione ed autorizzazione nell'accesso agli strumenti informatici;
- custodire la riservatezza delle parole chiave e dei codici di accesso agli strumenti informatici al fine di prevenire accessi non autorizzati;
- segnalare tempestivamente l'eventuale furto o smarrimento degli strumenti informatici in modo da consentire alla Società di adottare le misure idonee a prevenire accessi non autorizzati;
- sottoporre all'ufficio Sistemi Informativi (responsabile informatico) tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa.
- Dare tempestiva comunicazione all'OdV di eventuali anomalie o irregolarità riscontrate rispetto ai suddetti obblighi.

- la password per l'accesso ai personal computer e all'indirizzo di posta elettronica sono strettamente personali e riservate. Vengono create dal Consulente esterno del Sistema Informatico (IAL) e può essere successivamente modificata alla prima connessione.
- la password per l'accesso alla rete SharePoint è strettamente personale e riservata. Viene creata dal Referente dei Sistemi di Gestione Integrati e può essere successivamente modificata alla prima connessione.
- Il Referente dei Sistemi di Gestione Integrati e il Consulente esterno del Sistema Informatico (IAL) hanno la facoltà di cambiare le password di accesso alla rete qualora lo ritengano necessario.

I Destinatari, inoltre, hanno il divieto di:

- accedere agli strumenti informatici mediante profili di autorizzazione o autenticazione diversi da quelli assegnati;
- lasciare incustoditi senza adeguata protezione gli strumenti informatici o, comunque, consentirne l'accesso a soggetti non autorizzati;
- modificare le configurazioni hardware e software pre-impostate dall'ufficio Sistemi Informativi e/o dal Responsabile Informatico (ad esempio tramite l'installazione di programmi non autorizzati, masterizzatori, schede wireless, modem, webcam, software di interfaccia con cellulari, supporti rimovibili), salvo previa autorizzazione esplicita del responsabile dei sistemi informatici aziendali;
- effettuare operazioni di download, duplicazione, memorizzazione di files e/o dati non strettamente attinenti all'attività lavorativa;
- distruggere, deteriorare, cancellare, sopprimere informazioni, dati, informazione o programmi telematici altrui senza averne l'espressa e documentata autorizzazione;
- utilizzare software o hardware o qualsivoglia altro strumento o apparecchiatura atta a intercettare, falsificare, alterare o sopprimere il contenuto di documenti informatici o ad interrompere le comunicazioni relative ad un qualsiasi sistema informatico o telematico (quali, ad esempio, virus, worm, trojan, spyware, dialer, keylogger, rootkit etc);
- alterare e/o modificare indebitamente, mediante l'utilizzo di firma elettronica altrui o in qualsiasi altro modo, documenti informatici;
- elaborare o trasmettere per via informatica o telematica dati falsi e/o alterati;
- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza o, comunque, procurarsi o detenere abusivamente codici di accesso a sistemi informatici o telematici.

I Destinatari che venissero a conoscenza di eventuali anomalie rispetto agli obblighi e ai divieti di cui sopra devono darne tempestiva comunicazione all'Organismo di Vigilanza.

5. ATTIVITA' E VERIFICHE DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza verifica che le procedure adottate siano rispettate e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza segnala la necessità di adeguamento ed eventuali necessità di integrazione delle prescrizioni specifiche di cui sopra e delle relative procedure di attuazione.

L'OdV incontra periodicamente i responsabili di funzione per uno scambio informativo al fine di verificare eventuali carenze o necessità di ulteriori interventi a presidio dell'area interessata.

6. PROCEDURE A PRESIDIO DELLA PRESENTE PARTE SPECIALE

Le procedure a presidio della seguente Parte Speciale sono:

MODELLO ORGANIZZATIVO PRIVACY E REGISTRO DEL TRATTAMENTO DATI.
REGOLAMENTO AZIENDALE – CODICE ETICO INFORMATICO
REGOLAMENTO SULL'UTILIZZO DEI LABORATORI.
MANUALE ITS GESTIONE QUALITA'
MANUALE GESTIONE ATTIVITÀ FORMATIVE