

PARTE SPECIALE "B"

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

ART. 24 *BIS* D.LGS. 231/2001

LE FATTISPECIE DEI DELITTI INFORMATICI

L'art. 24-bis - (Delitti informatici e trattamento illecito di dati) del Decreto prevede:

- "1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote;
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote;
3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote;
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

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 lire dieci milioni.

La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater.

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 sino a due anni e con la multa sino a 10.329 euro.

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 a 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'art. 617-quater.

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 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 a 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 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 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 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 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.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies C.P.)

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.

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.

Documenti informatici (art. 491 bis C.P.)

Se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applica 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.

Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. n. 105/2019)

Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni.

LE ATTIVITA' SENSIBILI AI FINI DEL S.LGS 231/2001

L'art. 6, comma 2, lett. a) del d.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dall'art. 24 bis d.lgs. n. 231/2001. L'analisi dei processi aziendali di CEP EUROPE S.R.L. ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate nel paragrafo 1. Qui di seguito sono elencate le attività sensibili esaminate:

ATTIVITA'	DIREZIONE	PRESIDI
<ul style="list-style-type: none"> Gestione dei sistemi informativi, della sicurezza informatica e trattamento illecito delle informazioni 	<ul style="list-style-type: none"> Amministratore di Sistema Consulente esterno 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Gestione del profilo utente e del processo di autenticazione 	<ul style="list-style-type: none"> Amministratore di Sistema Consulente esterno 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Gestione e protezione della postazione di lavoro 	<ul style="list-style-type: none"> Singolo utente 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Utilizzo di firma elettronica 	<ul style="list-style-type: none"> Legale Rappresentante 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Predisposizione ed invio telematico di scritture private e/o attestazioni e/o dichiarazioni sostitutive di certif. o atto di notorietà DPR 445/2000 	<ul style="list-style-type: none"> Consulente esterno 	<ul style="list-style-type: none"> Codice Etico PS Codice di condotta per parti terze
<ul style="list-style-type: none"> Gestione degli output di sistema e dei sistemi di memorizzazione 	<ul style="list-style-type: none"> Amministratore di Sistema Consulente esterno 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Gestione e protezione delle reti 	<ul style="list-style-type: none"> Amministratore di Sistema Consulente esterno 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Gestione acquisti programmi software 	<ul style="list-style-type: none"> Amministratore di Sistema 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Gestione accesso ad internet 	<ul style="list-style-type: none"> Amministratore di Sistema Consulente esterno 	<ul style="list-style-type: none"> Codice Etico PS
<ul style="list-style-type: none"> Elaborazione documenti digitali 	<ul style="list-style-type: none"> Singolo utente 	<ul style="list-style-type: none"> Codice Etico PS

Con specifico riguardo alle problematiche connesse al rischio informatico CEP EUROPE S.R.L., conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso (i) la protezione dei sistemi e delle informazioni dai potenziali attacchi attraverso la 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; e (ii) la garanzia della massima continuità del servizio. La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dai dirigenti e dai dipendenti "esponenti aziendali" della Società nelle aree di attività a rischio, nonché dai collaboratori esterni e *partners*, già definiti nella Parte Generale (i "Destinatari"). Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

IL SISTEMA DEI CONTROLLI

Il sistema dei controlli, perfezionato dalla Società sulla base delle indicazioni fornite dalle principali associazioni di categoria, quali le Linee Guida Confindustria, nonché dalle "best practice" internazionali, prevede con riferimento alle attività sensibili e ai processi strumentali individuati.

1) Principi generali degli standard di controllo relativi alle attività sensibili

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione. Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che Società si pone sono i seguenti:

- Riservatezza:** garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;

- **Integrità:** garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- **Disponibilità:** garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'esplicito divieto a carico di tutti i destinatari del Modello (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) 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:
 - alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
 - accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
 - accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
 - 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;
 - 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;
 - 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;
 - 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;
 - installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
 - svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
 - svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
 - distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
- in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
- 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 esplicito consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Amministratore di sistema o la cui provenienza sia dubbia;
- evitare di trasferire all'esterno dell'Azienda e/o trasmettere *files*, documenti, o qualsiasi altra documentazione riservata di proprietà della società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);
- 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; qualora l'utente venisse a conoscenza della password di altro utente, è tenuto a darne immediata notizia all'Amministratore di sistema;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;

- impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

2) **Standard di controllo "specifici" applicati alle singole attività sensibili**

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

- **segregazione delle attività:** si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- **esistenza di procedure/norme/circolari:** devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- **poteri autorizzativi e di firma:** i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società;
- **tracciabilità:** ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

Ai fini dell'attuazione delle regole elencate, oltre che dei principi generali contenuti nella Parte Generale del presente Modello 231 e dei principi generali di controllo, nel disciplinare la fattispecie di attività sensibile descritta, dovranno essere osservati anche i seguenti principi di riferimento.

- Gestione e monitoraggio degli accessi ai sistemi informatici e telematici.
- Esistenza di una normativa aziendale relativa alla gestione del rischio informatico che individui le seguenti fasi:
 1. identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità ovvero delle carenze di protezione relativamente a una determinata minaccia - con riferimento alle seguenti componenti: (i) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti), (ii) hardware, (iii) software, (iv) documentazione, (v) dati/informazioni, (vi) risorse umane;
 2. individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: (i) errori e malfunzionamenti, (ii) frodi e furti, (iii) software dannoso, (iv) danneggiamenti fisici, (v) sovraccarico del sistema, (vi) mancato rispetto della legislazione vigente;
 3. individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento;
 4. identificazione delle possibili contromisure;
 5. effettuazione di un'analisi costi/benefici degli investimenti per l'adozione delle contromisure;
 6. definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
 7. documentazione e accettazione del rischio residuo.
- Esistenza di una normativa aziendale nell'ambito della quale siano disciplinati i seguenti aspetti:
 1. definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
 2. costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;
 3. puntuale pianificazione delle attività di sicurezza informatica;
 4. progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
 5. definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la *business continuity* attraverso meccanismi di superamento di situazioni anomale;
 6. applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.

- Redazione, diffusione e conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.
- Attuazione di una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali.
- Attuazione di un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati.
- Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si espliciti attraverso la verifica e la gestione dei diritti d'accesso.
- Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici.
- Proceduralizzazione e espletamento di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.
- Previsione di strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).
- Previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti.
- Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di *networking*.
- Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni).
- Predisposizione e attuazione di una policy aziendale che stabilisce (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (ii) un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive.

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le funzioni preposte ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'O.d.V. al fine di ottimizzare le attività di verifica e lasciando all'O.d.V. il precipuo compito di monitorare il rispetto e l'adeguatezza del M.O.G.

I controlli svolti dall'O.d.V. saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di attività sensibili.

Di detti controlli l'O.d.V. riferisce al C.d.A. secondo le modalità previste nella Parte Generale del presente Modello 231.

PROCEDURE DI PREVENZIONE

La Società adotterà un sistema di controlli interno volto a prevenire la commissione dei reati informatici e del trattamento illecito dei dati e per la precisione attraverso gli appositi canali dedicati per il *reporting* all'Organismo di Vigilanza:

- chiunque venga a conoscenza di violazioni del Modello 231 o delle procedure adottate in materia dovrà immediatamente segnalarlo all'O.d.V.;
- chiunque venga a conoscenza di situazioni di pericolo o di inadeguatezza del sistema preventivo posto in essere contro i delitti informatici e il trattamento illecito di dati o, in ogni caso, di situazioni di pericolo o anomalie dovrà immediatamente segnalarlo all'O.d.V.