

IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO EX D. LGS. 231/2001 DI

Parte Speciale B:

Reati informatici

ex art. 24-bis Lgs. 231/2001

ESI S.p.A.

Tabella 1 - Riepilogo modifiche ed aggiornamenti

Versione	Approvato da	Motivo aggiornamento	Data validità
1.00	Consiglio di Amministrazione	Prima emissione	5 agosto 2024



Esi S.p.A.

IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Parte Speciale B: Reati informatici ex art. 24-bis D. Lgs. 231/2001

INDICE DEI CONTENUTI

1.	DEFINIZIONI.....	3
2.	PREMESSA.....	5
3.	LE FATTISPECIE DI REATI INFORMATICI (ART. 24-BIS DEL DECRETO)	6
4.	PROCESSI SENSIBILI	10
5.	PRINCIPI GENERALI DI COMPORTAMENTO	11
6.	PRINCIPI SPECIFICI E COMPONENTI DEL SISTEMA DI ORGANIZZAZIONE, GESTIONE E CONTROLLO..	12
7.	FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA.....	14



1. DEFINIZIONI

“Appaltatori”: convenzionalmente si intendono tutti gli appaltatori di opere o di servizi ai sensi del Codice civile, nonché i subappaltatori, i somministranti, i lavoratori autonomi che abbiano stipulato un contratto d’opera con la Società e di cui questa si avvale nei Processi Sensibili.

“CCNL”: Contratto Collettivo Nazionale del Lavoro.

“Comitato delle Segnalazioni”: il Comitato incaricato di ricevere e gestire le segnalazioni delle violazioni ai sensi del D. Lgs. 24/2023 (Whistleblowing).

“Consulenti”: soggetti non dipendenti della Società che agiscono in nome e/o per conto di ESI S.p.A. sulla base di un mandato o di un altro rapporto di collaborazione.

“Decreto”: il Decreto Legislativo n. 231 dell’8 giugno 2001.

“Delega”: l’atto interno di attribuzione di funzioni e compiti nell’ambito dell’organizzazione aziendale.

“Destinatari”: tutti i soggetti cui è rivolto il Modello e, in particolare: gli organi societari ed i loro componenti, i dipendenti, i Fornitori, gli Appaltatori, gli agenti della Società, i Consulenti, i collaboratori a progetto e i lavoratori somministrati, coinvolti nei Processi Sensibili, nonché i membri dell’Organismo di Vigilanza, in quanto non appartenenti alle categorie summenzionate.

“Fornitori”: i fornitori di beni (merci e materiali per la produzione) e servizi (escluse le consulenze) di cui la Società si avvale nell’ambito dei Processi Sensibili.

“Modello”: il Modello di Organizzazione, Gestione e Controllo previsto dal Decreto.

“OdV”: l’Organismo di Vigilanza previsto dal Decreto.

“Organo Dirigente”: Consiglio d’Amministrazione di ESI S.p.A.

“Processo/i Sensibile/i” l’insieme di attività ed operazioni aziendali organizzate al fine di perseguire un determinato scopo o gestire un determinato ambito aziendale di Esi S.p.A., in aree potenzialmente a rischio di commissione di uno o più reati previsti dal Decreto, così come elencate nella Parte Speciale del Modello, indicate anche genericamente e complessivamente come area/e a rischio.

“ProcessOwner” il soggetto che per posizione organizzativa ricoperta o per le attività svolte è maggiormente coinvolto nel Processo Sensibile di riferimento o ne ha maggiore visibilità ai fini del Modello 231.

“Procura” il negozio giuridico unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

“Reati”: le fattispecie di reato considerate dal Decreto.

“Società”: ESI S.p.A.



Esi S.p.A.

IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Parte Speciale B: Reati informatici ex art. 24-bis D. Lgs. 231/2001

“Società del Gruppo” tutte le società appartenenti al gruppo facente capo a Innovatec S.p.A. la quale le controlla ai sensi dell’art. 2359 c.c.

“Sistema di Whistleblowing”: sistema di segnalazione messo a disposizione dei dipendenti, nonché dei collaboratori e dei professionisti della società, finalizzato alla comunicazione di violazioni di leggi, violazioni del Modello rilevazioni di pericoli, frodi (reali o potenziali) o un qualunque altro rischio in grado di danneggiare l'azienda stessa, gli azionisti, i dipendenti, i clienti o la reputazione dell'ente.



2. PREMESSA

Il legislatore, mediante la previsione dell'art. 24-bis, ha esteso l'ambito di applicazione della responsabilità amministrativa degli enti, prevista dal D. Lgs. n. 231/2001, ai reati informatici e al trattamento illecito dei dati, a seguito del recepimento, ad opera della legge 18.03.2008, n. 48, della "Convenzione del Consiglio d'Europa sulla criminalità informatica", redatta a Budapest il 23.11.2001.

La presente Parte Speciale è destinata a tutti i soggetti di ESI siano essi Amministratori, Dirigenti, Dipendenti, Consulenti esterni e/o Collaboratori, soggetti a vigilanza operanti nelle aree o attività sensibili astrattamente o concretamente connesse alla commissione dei reati di cui alla presente Parte Speciale B.

I predetti "Destinatari", nell'ambito delle rispettive funzioni, dovranno conformarsi ai principi di comportamento ivi delineati al fine di prevenire la commissione dei reati espressamente considerati dall'art. 24-bis, D. Lgs. n. 231/2001.

In relazione all'attività aziendale svolta nello specifico da ESI Spa, i reati di cui all'art. 24-bis del D.Lgs. n. 231/2001, sono da ritenersi in effetti solo astrattamente configurabili., ma al fine di rispondere alle esigenze penal-preventive di cui al D.Lgs. n. 231/2001, la Società ha tuttavia ritenuto opportuno disciplinarli nella presente Parte Speciale con il fine specifico di evitare che eventuali condotte, possano realizzare la commissione dei reati informatici.

Dunque, la presente Parte Speciale, dedicata alla prevenzione dei reati Informatici e alla disciplina dei comportamenti ed attività che potrebbero astrattamente configurarli, è strutturata nelle seguenti sezioni:

- illustrazione delle **fattispecie di reato** ascrivibili alla famiglia degli informatici, astrattamente configurabili nella realtà ESI;
- identificazione dei processi ed attività aziendali di ESI a rischio di potenziale commissione dei suddetti reati e derivanti dalle attività di risk assessment condotte (c.d. **Processi Sensibili**).
- delineazione dei **principi di comportamento e regole di condotta** applicabili nella realizzazione delle attività entro i Processi Sensibili, ad integrazione del sistema etico e delle regole di comportamento delineati al Capitolo 4.3 della Parte Generale del presente Modello;
- per **ciascun Processo Sensibile, o per categorie omogenee di processi**, viene infine fornita la previsione di **principi specifici di comportamento e di controllo**, coerentemente con i principi ispiratori definiti all'interno del Capitolo 4 della Parte Generale, ed al fine di rappresentare aspetti peculiari delle componenti del sistema di controllo interno rilevanti ai fini della disciplina del/i Processo/i.



3. LE FATTISPECIE DI REATI INFORMATICI (ART. 24-BIS DEL DECRETO)

Come dinnanzi esposto, l'art. 7 della legge, n. 48 del 18 marzo 2008 ratificando la Convenzione del Consiglio d'Europa sui reati informatici, ha introdotto nel D.lgs. n. 231/2001, tramite l'art. 24-bis, alcune ipotesi di reato in materia di criminalità informatica, già disciplinate nel codice penale.

Per “crimine informatico” si intende ogni comportamento previsto e punito dal codice penale o da leggi speciali in cui qualsiasi strumento informatico o telematico rappresenti un elemento determinante ai fini della qualificazione del fatto-reato.

Si utilizza il termine “reato informatico” per indicare qualsiasi condotta realizzata per mezzo di nuove tecnologie o comunque rivolta contro beni informatici, sanzionata dall'ordinamento penale.

In sostanza, ricorre un crimine informatico quando un sistema di elaborazione, o ciò che viene prodotto dall'elaboratore, è usato come mezzo per commettere frodi, sabotaggi o falsificazioni.

In ordine alle sanzioni poste a carico delle società in caso di commissione, consumata o tentata, di uno dei reati ivi contemplati, l'art. 24-bis stabilisce sanzioni pecuniarie, a seconda del tipo di delitto commesso, da un minimo di cento quote sino a cinquecento quote. Inoltre, nei casi più gravi si applicano sanzioni interdittive.

Tra i reati informatici previsti dal Decreto si indicano di seguito quelli astrattamente configurabili nell'ambito delle attività svolte da ESI:

- **Falsità in un documento informatico pubblico o privato (491-bis c.p.)** – “*Se alcuna delle falsità previste dal presente capo (Capo III c.p.) riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A Tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*”.
- **Accesso abusivo ad un sistema informatico o telematico (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 due a dieci 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 minaccia o 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 ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare 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 (615-quater c.p.)** - *“Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro.*

La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (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”.*
- **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (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.*
Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni.
Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni”.
- **Danneggiamento di informazioni, dati e programmi informatici (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 la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio".

- **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635-ter 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 due a sei anni.*

La pena è della reclusione da tre a otto anni:

(i) 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;

(ii) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato".

- **Danneggiamento di sistemi informatici o telematici (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 due a sei anni.*

La pena è della reclusione da tre a otto anni:

(i) 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;

(ii) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato

- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (635 quinquies 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, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.*

La pena è della reclusione da tre a otto anni:

(i) 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;



(ii) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

(iii) 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 quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).

- **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (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”*.
- **Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 635-quater.1)** - *“Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.*

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma”.

- **Estorsione (Art. 629 terzo comma c.p.)** - *“[III]. Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità”*.



4. PROCESSI SENSIBILI

Una funzione preventiva efficace si rivela la sensibilizzazione delle aziende a potenziare una politica di sicurezza informatica, atteso che qualsiasi reato tecnologico può essere impedito soltanto con adeguate contromisure tecnologiche.

Gran parte delle aziende, oggi, sono criticamente dipendenti dall'efficace gestione delle informazioni e delle relative tecnologie informatiche, dipendenza che porta però ad una crescente vulnerabilità ad un ampio spettro di minacce, quali cyber attacchi, gravi incidenti aziendali causati dal malfunzionamento dei sistemi, ecc., anche considerando la notevole complessità portata dal moltiplicarsi di protocolli di accesso e comunicazione, dei canali di trasmissione dei dati (ADSL, fibra, satellite, bluetooth, ecc.), dei contenuti e delle applicazioni multimediali e on-line, dell'hardware disponibile per accedere ai dati (palmare, PC, notebook).

Per quanto riguarda i crimini informatici, i rischi riguardano soprattutto l'area dei dati; è dunque possibile ricondurre alle seguenti categorie le condotte che comportano seri rischi per la sicurezza:

1. eventi cagionati dai dipendenti, che possono consistere in: sottrazione di credenziali di autenticazione, distruzione o perdita di dati, trattamento dei dati non consentito, disattenzione o incuria, comportamenti sleali o fraudolenti, errore materiale;
2. eventi determinati dall'utilizzo di strumenti: azione di virus informatici, spamming, malfunzionamento, indisponibilità o degrado degli strumenti, utilizzo di codici di accesso non autorizzati, accessi esterni non autorizzati, intercettazione di informazioni in rete;
3. eventi relativi al contesto fisico-ambientale: ingressi non autorizzati a locali/aree ad accesso ristretto, sottrazione di strumenti contenenti dati, eventi distruttivi, naturali o artificiali nonché dolosi, accidentali o dovuti ad incuria, guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.), errori umani nella gestione della sicurezza fisica.

In relazione all'attività aziendale svolta nello specifico dalla Società, i reati di cui all'art. 24-bis del D.Lgs. n. 231/2001, sono da ritenersi solo astrattamente configurabili.

Seppure il rischio di commissione dei reati sia basso, con particolare riferimento alle fattispecie enunciate nella presente Parte Speciale B, le attività sensibili di ESI sono:

1. Gestione dei sistemi informatici;
2. Gestione circolazione dei dati informatici;
3. Gestione utilizzo di informazioni, dati e programmi informatici;
4. Gestione del trattamento dei dati personali.



5. PRINCIPI GENERALI DI COMPORTAMENTO

Agli Organi Sociali e ai Dirigenti di ESI Spa, in via diretta, nonché a lavoratori Dipendenti, Collaboratori e i Consulenti, soggetti a vigilanza, è fatto divieto di:

- alterare/manomettere/danneggiare il funzionamento di sistemi informatici o telematici al fine di procurare un vantaggio o un interesse per la società;
- intervenire illegalmente con qualsiasi modalità su dati, informazioni o programmi informatici, al solo fine di procurare un vantaggio o un interesse per la società;
- intercettare, impedire o interrompere illecitamente o diffondere comunicazioni informatiche o telematiche al fine di procurare un vantaggio o un interesse per la società;
- Installare nella rete aziendale un proprio software che non rientri nello scopo per cui il sistema informatico è stato assegnato all'utente per evitare che possa interrompere, danneggiare, manomettere, o impedire le comunicazioni informatiche aziendali;
- Prestare o cedere a terzi qualsiasi apparecchiatura informatica senza la preventiva autorizzazione del Responsabile interno;
- Evitare di trasferire all'esterno dell'azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'azienda stessa o di altra società collegata ESI, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del Responsabile interno;
- Astenersi dall'effettuare copie non autorizzate di dati o di software;
- Evitare l'utilizzo di password 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 Informatici;
- Alterare, contraffare, documenti informatici, pubblici o privati;
- Accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati, in ogni caso di soggetti "esterni" al fine di manomettere dati o carpire informazioni riservate;
- Accedere abusivamente al sistema informatico o telematico della società al fine di alterare e/o cancellare dati o informazioni;
- Detenere e/o utilizzare abusivamente codici di accesso di società o soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- Svolgere attività di intercettazione, impedimento, interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti pubblici o privati, al fine di acquisire informazioni riservate;
- Modificare, cancellare, danneggiare, distruggere dati, informazioni, programmi di soggetti privati, o soggetti pubblici o comunque di pubblica utilità.



6. PRINCIPI SPECIFICI E COMPONENTI DEL SISTEMA DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

L'utilizzo degli strumenti informatici - coerentemente ai principi del D.Lgs. n. 231/01 - deve avvenire seguendo le procedure interne e nel rispetto del DPS ex D. Lgs. n. 196/2003, come modificato dal D. Lgs 101/2018; di ogni contatto/passaggio deve essere data debita evidenza e conservata traccia.

Inoltre, il Responsabile della Funzione Sistemi Informativi deve:

- Comunicare, attraverso la redazione di report informativi all'Organismo di Vigilanza, e nel caso anche al Consiglio di Amministrazione, qualunque anomalia o criticità riscontrata nel corso dello svolgimento dell'attività nell'ambito della funzione di competenza;
- verificare la concreta ed efficace attuazione – nell'ambito delle funzioni di competenza – delle procedure aziendali e dei principi di cui al presente Modello di Organizzazione e Gestione.

In materia di reati informatici e trattamento illecito dei dati, occorre garantire la protezione del patrimonio informativo da parte delle singole Unità organizzative e assicurare il corretto utilizzo delle risorse tecnologiche, nonché disporre di evidenze che documentino l'efficacia dei controlli implementati.

I protocolli di controllo comuni alle attività a rischio reato devono essere volti a:

- definire politiche di sicurezza delle informazioni attraverso la corretta gestione e uso delle password, prevedendone anche l'aggiornamento periodico obbligatorio a tutti gli utenti;
- stabilire l'obbligo di mantenere la riservatezza della password;
- prevedere controlli sulla rete aziendale e sulle informazioni che vi transitano;
- prevedere corsi di aggiornamento/formazione sui principali pacchetti informativi in dotazione (in particolare sul corretto utilizzo della posta elettronica), e la distribuzione di un breviario sul corretto utilizzo delle dotazioni informatiche a ciascun dipendente;
- limitare l'accesso internet a siti aziendali utili e moralmente leciti;
- inibire, come policy aziendale, l'utilizzo delle e-mail spamming;
- prevedere l'inventario aggiornato dell'hardware e del software in uso agli utenti;
- prevedere il tracciamento degli accessi degli utenti alla rete aziendale;
- prevedere l'adozione di meccanismi di segregazione delle reti;
- prevedere la sicurezza fisica dei siti ove risiedono i sistemi IT;
- prevedere l'aggiornamento del sistema antivirus/antispamming periodico;
- stabilire l'assegnazione nominale di PC aziendali (non lasciare mai la disponibilità dei PC aziendali ad *outsoucer* etc. se non si crea una identificazione dell'utilizzatore);



- prevedere il rispetto delle leggi e dei regolamenti applicabili in tema di protezione e sicurezza dei dati informatici, di cui al D.lgs. n. 196/2003 come modificato dal D. Lgs 101/2018.

ESI si è conformata al Regolamento UE 679/2016 (GDPR), che stabilisce le misure di sicurezza, tecniche ed organizzative, che la Società ha adottato per garantire un'adeguata protezione dei dati personali trattati, a seguito dell'effettuazione della valutazione dei rischi che incombono sui trattamenti di dati personali, in funzione della relativa probabilità e gravità di verificarsi.

Tali misure di sicurezza comprendono le modalità di trattamento dei dati personali sia su supporto cartaceo, sia su supporto digitale, mediante strumenti elettronici, che tutto il personale si impegna ad adottare per garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati.

Il Regolamento si prefigge, altresì, di portare a conoscenza di tutti i Dipendenti e dei Collaboratori i limiti di utilizzo delle risorse informatiche assegnate per lo svolgimento delle mansioni lavorative, nonché di informare gli utilizzatori stessi circa la possibilità che l'azienda effettui dei controlli sulle corrette modalità di utilizzo dei beni con il solo fine di assicurare e preservare l'integrità degli strumenti stessi, evitare la commissione di illeciti e verificare la funzionalità del sistema.

La società ha individuato le varie figure preposte al trattamento dei dati ("Titolare", "Responsabile" e "Incaricati") e sono analizzate le situazioni aziendali e le misure che la stessa ha adottato, ed adotterà, a garanzia della sicurezza nel trattamento dei dati.

ESI si avvale dell'outsourcer F.C. Workgroup S.r.l. per i servizi di progettazione informatica, assistenza software client, assistenza software server, programmazione, web designer, reverse engineering, system analyzer.



7. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

In relazione alle attività sensibili ed ai relativi protocolli trattati nel presente fascicolo, devono essere trasmessi all'OdV i seguenti flussi informativi:

- Segnalazione di anomalie o criticità riscontrate nel corso dello svolgimento dell'attività nell'ambito della Gestione dei Sistemi Informatici (es, Data breach, Cyberattacchi, Incidente informatico).