

Esatto S.p.A.

ANALISI DEI RISCHI *ex* D.lgs. 231/2001

Trieste, 31 maggio 2025

SOMMARIO

1	PREMESSA.....	2
2	DESCRIZIONE DELL'ATTIVITÀ DI ANALISI	3
3	BREVE ESPOSIZIONE DEI PRINCIPI GENERALI CONTENUTI NEL D.LGS. 231/2001	3
4	METODOLOGIA DI ANALISI DEL RISCHIO DI REATO.....	6
5	EXECUTIVE SUMMARY.....	9
	5.1 TABELLA DI SINTESI DEI LIVELLI DI RISCHIO PER AREA OMOGENEA DI REATI	9
	5.2 ELENCO DEI DOCUMENTI CONSULTATI PER LA PREDISPOSIZIONE DELL'ANALISI DEI RISCHI	10
	5.3 AZIONI SUGGERITE.....	11
6	TAVOLE SINOTTICHE	13
	SEZIONE A REATI CONTRO LA PUBBLICA AMMINISTRAZIONE	13
	SEZIONE B DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI.....	15
	SEZIONE C CONCUSSIONE E CORRUZIONE – INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ'	17
	SEZIONE D FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO	19
	SEZIONE E REATI SOCIETARI	21
	SEZIONE F OMICIDIO COLPOSO LESIONI GRAVI O GRAVISSIME – SALUTE E SICUREZZA SUL LAVORO	23
	SEZIONE G RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA – AUTORICICLAGGIO DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI	26
	SEZIONE H DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE.....	28
	SEZIONE I INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA.....	29
	SEZIONE J IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE	30
	SEZIONE K REATI TRIBUTARI	32

1 PREMESSA

Il Consiglio di Amministrazione di Esatto S.p.A. (“**Esatto**” o “**Società**”) ha incaricato lo Studio Legale Associato Ferrari Pedeferrì Boni (“**FPB**”) di aggiornare il documento di analisi (“**Analisi dei Rischi**”) del rischio effettivo e concreto (“**Rischio**” o “**Rischio 231**”) per la Società di commissione dei reati previsti dal Decreto Legislativo 8 Giugno 2001, n. 231 (“**D.lgs. 231/2001**” o “**Decreto**”) nell’ambito della relativa attività e, di conseguenza, del rischio per la Società di subire le sanzioni amministrative previste dal Decreto.

L'Analisi dei Rischi svolge la funzione di consentire al Consiglio di Amministrazione della Società di adottare una decisione consapevole ed informata sulla opportunità, o necessità, per la Società di aggiornare anche il Modello di Organizzazione, Gestione e Controllo adottato ai sensi dell'Art. 6 del Decreto.

FPB ha svolto la fase di istruttoria e verifica del livello attuale di rischio di commissione, nell'ambito dell'attività aziendale di Esatto dei reati previsti dal, e puniti con sanzione amministrativa ai sensi del Decreto ("**Reati Presupposto**"), in consultazione e in contraddittorio con la dirigenza della Società e con i responsabili delle aree e delle funzioni aziendali maggiormente esposte al Rischio di commissione dei reati.

Le tavole sinottiche di analisi a corredo del presente documento, predisposte per gruppi di reati (aree omogenee), contengono un'apposita sezione di suggerimenti e di proposte di azioni correttive volte a limitare quanto più possibile il Rischio 231 fino al livello di "Rischio accettabile" definito dalle Linee Guida di Confindustria per la costruzione dei Modelli ai sensi del Decreto. In particolare, in estrema sintesi, la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente.

2 DESCRIZIONE DELL'ATTIVITÀ DI ANALISI

L'Analisi dei Rischi è stata svolta attraverso colloqui ed incontri con i responsabili dei processi aziendali esposti al rischio di commissione dei Reati Presupposto e, precisamente:

- Dott. Davide Fermo (Direttore Generale);

Per la predisposizione dell'Analisi dei Rischi sono state svolte le seguenti attività:

1. Riunione con intervista al Direttore Generale del 4 aprile 2025;
2. Acquisizione e studio delle procedure, regolamenti, istruzioni operative attualmente esistenti.

3 BREVE ESPOSIZIONE DEI PRINCIPI GENERALI CONTENUTI NEL D.LGS. 231/2001

In breve, il D.lgs. n. 231/2001 prevede che, qualora:

- nello svolgimento dell'attività sociale, sia commesso un reato; e
- tale reato sia incluso tra i Reati Presupposto richiamati dal medesimo Decreto; e
- sia stato commesso nell'interesse o a vantaggio, anche indiretto, della Società; e
- sia stato commesso da un soggetto in posizione apicale (o da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale);

la Società è responsabile (unitamente all'autore materiale del reato che rimane personalmente responsabile) per la commissione del Reato Presupposto e, conseguentemente, diviene esposta al rischio, ai sensi dell'art. 9 del Decreto, di essere condannata a:

- SANZIONE PECUNIARIA, sempre applicabile in caso di illecito amministrativo dipendente da reato;
- SANZIONE INTERDITTIVA;
- CONFISCA;
- PUBBLICAZIONE DELLA SENTENZA.

La Società, tuttavia, non risponde della commissione di un Reato Presupposto (e conseguentemente non è esposta al rischio di subire le relative sanzioni), solo nel caso in cui possa dimostrare, ai sensi dell'art. 6 del Decreto, in modo oggettivo e documentato che:

- l'organo amministrativo della Società ha adottato ed attuato, prima della commissione del fatto costituente reato, un idoneo Modello di Organizzazione, Gestione e Controllo ("**Modello Organizzativo**" o "**Modello**");
- sul funzionamento e sulla osservanza del Modello Organizzativo vigila un organismo di vigilanza ("**Organismo di Vigilanza**" o "**OdV**") rispondente alle caratteristiche indicate in Decreto e dotato di autonomi poteri di iniziativa e di controllo;
- i dipendenti della Società e tutti i destinatari del Modello sono stati efficacemente informati e formati circa i contenuti del Modello Organizzativo stesso;
- sono state previste sanzioni disciplinari per i dipendenti (e gli altri destinatari, quando possibile) in caso di mancata osservanza del Modello.

Il pregiudizio degli enti per la mancata adozione del Modello potrà, quindi, verificarsi solo nel caso in cui sia stato commesso uno dei Reati Presupposto, ricorrendo contestualmente le altre condizioni sopra indicate. In questa evenienza, la Società sarà ritenuta responsabile e soggetta alle conseguenti sanzioni amministrative.

In estrema sintesi, secondo quanto previsto dalle norme applicabili e da consolidati orientamenti giurisprudenziali un modello può dirsi adottato ed efficacemente attuato se funzionale:

- a garantire l'osservanza di **principi generali** di comportamento, conformi alla migliore etica societaria e degli affari, attraverso un'autoregolamentazione codificata nel Modello stesso e, con maggiore dettaglio, nel Codice Etico aziendale;
- a garantire l'impegno all'osservanza di **modelli particolari e specifici** di comportamento delineati *ad hoc* per ciascuna delle attività aziendali "sensibili" perché maggiormente esposte al rischio di commissione di un Reato Presupposto. Tali modelli devono essere formalizzati in procedure di comportamento ("**Procedure**") che formano un allegato fondamentale del Modello Organizzativo;
 - in linea di massima, le Procedure:
 - si sostanziano in una serie di protocolli comportamentali, diretti a regolare e programmare le modalità pratiche di realizzazione delle attività della Società, nonché le fasi di formazione e di attuazione delle decisioni della Società;
 - sono altresì dirette a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

- sono strutturate in modo da fissare dei modelli comportamentali applicabili a tutti coloro parte del processo di ideazione, pianificazione, esecuzione e controllo delle singole attività sociali;
 - stabiliscono i criteri per la ripartizione - tra vari soggetti coinvolti - delle mansioni di ciascuno di essi e delle diverse fasi delle attività che risultano a rischio di una commissione di un Reato Presupposto;
 - implementano un sistema di controllo interno e di verifica degli adempimenti agli obblighi posti a carico di ciascun soggetto nel porre in essere attività rilevanti nell'ambito del perseguimento dell'attività sociale;
 - impegnano alla loro osservanza ogni soggetto coinvolto, anche occasionalmente, nel processo aziendale considerato;
 - individuano un (o più) referente/i quale responsabile/i della Procedura;
 - fissano metodologie di tracciabilità oggettiva e documentale dello svolgimento delle azioni e dei comportamenti che regolano;
 - in ragione della loro natura di direttive datoriali, sono obbligatorie a pena di applicazione di sanzioni di natura giuslavorista, in caso di inosservanza di quanto in esse previsto;
 - sono soggette ad aggiornamento, e relativa evoluzione, sia in relazione ad ogni mutamento delle condizioni oggettive in cui operano, sia in relazione all'ottimizzazione del procedimento, derivante dall'esperienza applicativa e della funzione da esse svolta.
- ad assicurare la puntuale e adeguata formazione del personale della Società sui contenuti, principi e finalità del Decreto, del Modello Organizzativo e, singolarmente, delle Procedure, con verifica della piena comprensione della formazione ricevuta;
 - a garantire la costante valutazione del Modello da parte dell'Organismo di Vigilanza (di struttura monocratica o plurisoggettiva) relativamente alla adeguatezza, efficacia ed eventuale necessità di aggiornamento delle Procedure, così come del Modello stesso.

Il Modello, infine, deve essere completato da un **sistema disciplinare**, costituito da sanzioni applicabili ai responsabili delle violazioni del Modello stesso, a prescindere dall'eventuale instaurazione di un giudizio penale ed a prescindere dall'esito di tale eventuale procedimento penale.

Il D.Lgs. 24/2023, adottato in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali, al fine di assicurare un'efficace tutela del soggetto che segnali un illecito o una violazione del Modello di cui sia venuto a conoscenza in ragione delle funzioni svolte nell'ambito di un rapporto di impiego privato, impone che i Modelli Organizzativi di Gestione e Controllo ex D.lgs. 231/2001 prevedano:

- specifici canali informativi dedicati alle segnalazioni, tali da garantire la riservatezza dell'identità del segnalante;
- il divieto di atti di ritorsione o discriminatori nei confronti del segnalante;
- l'inserimento all'interno del sistema disciplinare del modello organizzativo di sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni poi rivelatesi infondate.

L'insieme di tali previsioni costituisce la disciplina del *whistleblowing*, già introdotta dalla legge 190/2012, con riferimento all'impiego pubblico, dalla legge 30 novembre 2017, n. 179.

Per quanto riguarda le tutele accordate al "*whistleblower*" privato, esse si sostanziano ne:

- la tutela della riservatezza del segnalante, del facilitatore, della persona coinvolta e delle persone menzionate nella segnalazione;
- la tutela da eventuali ritorsioni adottate dall'ente in ragione della segnalazione, divulgazione pubblica o denuncia effettuata e le condizioni per la sua applicazione;
- le limitazioni della responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni (e.g. informazioni coperte da segreto).

4 METODOLOGIA DI ANALISI DEL RISCHIO DI REATO

L'Analisi del Rischio è un'attività che ha in primo luogo l'obiettivo di individuare e contestualizzare il rischio di reato in relazione all'assetto organizzativo e all'attività dell'ente. In secondo luogo, attraverso tale attività si possono ottenere informazioni utili a supportare le scelte dell'organo dirigente in merito alle azioni di adeguamento e miglioramento del modello di organizzazione, nonché di gestione e controllo dell'ente rispetto alle finalità preventive indicate dal D.lgs. 231/2001 (quali, in via esemplificativa, i livelli di esposizione ai singoli rischi di reato).

L'Analisi del Rischio consiste nella valutazione sistematica dei seguenti fattori:

1. **PROBABILITÀ DELL'ACCADIMENTO DELL'EVENTO A RISCHIO**, con ciò intendendo la probabilità e la frequenza di accadimento delle situazioni operative tipiche in cui solitamente, ed in linea generale, possa eventualmente essere commesso un evento illecito. Essa, pertanto, rappresenta la frequenza di accadimento nel contesto operativo in cui una minaccia, un'azione, un'attività, un processo o un potenziale evento nocivo possa intervenire e possa integrare la fattispecie criminosa del Reato Presupposto stesso.
2. **IMPATTO**, con ciò intendendo principalmente il possibile beneficio atteso dall'autore del reato e/o dalla Società a seguito dalla realizzazione un Reato Presupposto: esso, pertanto, consiste nel beneficio atteso che induce un soggetto alla commissione del reato a cui si affianca una analisi secondaria sull'impatto dell'eventuale sanzione comminabile alla Società e sui riflessi di questa sull'attività e sull'organizzazione aziendale.
3. **LIVELLO DI VULNERABILITÀ**, ovvero il livello dei protocolli di prevenzione aziendali di natura etica od organizzativa: le vulnerabilità aumentano il rischio di commissione dei Reati Presupposto e consistono nella mancanza di misure preventive o in un clima etico aziendale carente, rendendo così più agevole o facile l'accadimento di una minaccia e la conseguente realizzazione del Reato Presupposto.

Per analizzare il Rischio di Reato si è proceduto eseguendo le fasi operative di seguito descritte:

1. identificazione della fattispecie di Reato Presupposto e conseguente individuazione delle minacce che permettono la commissione dei fatti di reato (in termini di condotte o attività operative).

2. contestualizzazione delle minacce che permettono la potenziale commissione dei fatti di Reato rispetto alla Società tramite tecniche di valutazione di condotte da team formati da avvocati.
3. valutazione della probabilità delle minacce: assegnazione a ciascuna minaccia di un valore probabilistico circa il relativo verificarsi.
4. valutazione del livello di vulnerabilità rispetto a ciascuna minaccia, tramite l'identificazione delle misure preventive attuate e l'analisi del clima etico e organizzativo.
5. valutazione del possibile impatto: valutazione dei potenziali benefici attesi dai potenziali autori di reato, valutando altresì i possibili danni derivanti alla Società in caso di commissione di Reati Presupposto in termini di sanzioni pecuniarie e/o interdittive e/o di perdite di immagine o fatturato.

L'analisi delle attività sensibili è stata effettuata tenendo altresì in considerazione i seguenti principi generali degli standard di controllo ad esso associati:

- **Separazione dei compiti:** separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Norme:** esistenza di disposizioni aziendali e/o di 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 (poteri di spesa) e di firma (procure):** i poteri autorizzativi e di firma devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società.
- **Tracciabilità:** i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile *ex post*, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

La presente Analisi dei Rischi è stata quindi svolta analizzando le caratteristiche dell'attività aziendale di Esatto nelle aree esposte al rischio di commissione di Reati Presupposto, con l'intento di fornire la seguente classificazione:

1	TRASCURABILE
2	BASSO
3	MEDIO
4	ALTO

In sintesi:

1. Individuazione, nell'ambito dell'attività aziendale di Esatto e dei suoi contesti operativi, dei Reati Presupposto per i quali il rischio di commissione è altamente improbabile, essendo la fattispecie costitutiva del reato stesso del tutto estranea (se non in casi rarissimi) all'attività aziendale o alla sua operatività. Per tali reati è stata attribuita la qualifica di rischio: **Trascurabile**.
2. Individuazione, nell'ambito dell'attività aziendale di Esatto e dei suoi contesti operativi, dei Reati Presupposto per i quali non può essere escluso a priori il rischio di commissione, ma che, per le valutazioni evidenziate nello svolgimento dell'Analisi del Rischio, trovano nel contesto aziendale, nelle modalità operative, nelle

procedure e nel livello di responsabilità presenti in Società, forti elementi deterrenti o protettivi rispetto alla loro concreta commissione, tali da renderne improbabile il loro verificarsi. A tali reati è stata attribuita la qualifica di rischio: **Basso**.

3. Individuazione, nell'ambito dell'attività aziendale di Esatto e dei suoi contesti operativi, dei Reati Presupposto per i quali la Società è esposta al rischio di commissione, sia per la frequenza dei casi in cui si possono manifestare le modalità operative in cui le fattispecie criminosi possano essere commesse, sia per la difficoltà oggettiva di presidiare sufficientemente le aree di rischio, sia per la dipendenza della loro potenziale commissione da procedure aziendali, coinvolgenti un ampio numero di soggetti, anche estranei al mero organigramma aziendale, sia, infine, per la particolare insidiosità delle fattispecie considerate. Per tali reati è stata attribuita la qualifica di rischio: **Medio**.
4. Individuazione nell'ambito dell'attività aziendale Società e dei suoi contesti operativi, dei Reati Presupposto per i quali la Società è gravemente esposta al rischio di commissione, sia per la frequenza dei casi in cui si possono manifestare le modalità operative in cui le fattispecie criminosi possano essere commesse, sia per la difficoltà oggettiva di presidiare efficacemente le aree di rischio, sia per la dipendenza della loro potenziale commissione da processi aziendali difficilmente modificabili con l'introduzione di punti di controlli e altri standard di sicurezza. Tali processi coinvolgono, infatti, un ampio numero di soggetti, anche estranei al mero organigramma aziendale e, insieme agli altri fattori ricordati, ciò rende particolarmente insidiosa la modalità di realizzazione delle fattispecie considerate. Per tali reati è stata attribuita la qualifica di Rischio: **Alto**.

La stima del rischio è svolta senza valutazioni inerenti a differenze di gravità fra i diversi Reati Presupposto.

5 EXECUTIVE SUMMARY

Il presente sommario presenta in breve le risultanze e le conclusioni dell'attività di identificazione, valutazione e stima del grado di accadimento dei rischi di commissione dei Reati Presupposto di applicazione della disciplina della responsabilità amministrativa di cui al D.lgs. 231/2001 sulla base sia del Decreto stesso sia delle Linee Guida di Confindustria per la costruzione dei Modelli Organizzativi.

5.1 TABELLA DI SINTESI DEI LIVELLI DI RISCHIO PER AREA OMOGENEA DI REATI

REATO PRESUPPOSTO		RISCHIO 231
Art. 24 D.lgs. 231/2001	Reati contro la PA	MEDIO
Art. 24-bis D.lgs. 231/2001	Delitti informatici e trattamento illecito di dati	MEDIO
Art. 24-ter D.lgs. 231/2001	Delitti di criminalità organizzata	TRASCURABILE
Art. 25 D.lgs. 231/2001	Peculato, indebita destinazione di denaro e cose mobili, concussione e corruzione - Induzione indebita a dare o promettere utilità	MEDIO
Art. 25-bis D.lgs. 231/2001	Falsità in monete, in carte di pubblico credito, in valori di bollo	BASSO
Art. 25-bis.1 D.lgs. 231/2001	Delitti contro l'industria e commercio	TRASCURABILE
Art. 25-ter D.lgs. 231/2001	Reati societari	MEDIO
Art. 25-quater D.lgs. 231/2001	Delitti con finalità di terrorismo o di eversione dell'ordine democratico	TRASCURABILE
Art. 25-quater.1 D.lgs. 231/2001	Pratiche di mutilazione degli organi genitali femminili	TRASCURABILE
Art. 25-quinquies D.lgs. 231/2001	Delitti contro la personalità individuale	TRASCURABILE
Art. 25-sexies D.lgs. 231/2001	Reati di abuso di mercato	TRASCURABILE
Art. 25-septies D.lgs. 231/2001	Omicidio colposo o lesioni gravi o gravissime - salute e sicurezza sul lavoro	MEDIO
Art. 25-octies D.lgs. 231/2001	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita Autoriciclaggio	MEDIO
Art. 25-octies.1 D.lgs. 231/2001	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	MEDIO
Art. 25-novies D.lgs. 231/2001	Delitti in materia di violazione del diritto d'autore	BASSO
Art. 25-decies D.lgs. 231/2001	Induzione a non rendere dichiarazioni o a renderle mendaci all'autorità	MEDIO
Art. 25-undecies D.lgs. 231/2001	Reati ambientali	TRASCURABILE
Art. 25-duodecies D.lgs. 231/2001	Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare	MEDIO
Art. 25-terdecies D.lgs. 231/2001	Razzismo e xenofobia	TRASCURABILE

Art. 10 L. 16.3.2006 n. 146	Reati transnazionali	TRASCURABILE
Art. 25 - <i>quaterdecies</i> D.lgs. 231/2001	Reati di frode in competizioni sportive	TRASCURABILE
Art. 25 - <i>quindiesdecies</i> D.lgs. 231/2001	Reati tributari	MEDIO
Art. 25 - <i>sexiesdecies</i> D.lgs. 231/2001	Contrabbando	TRASCURABILE
Art. 25 - <i>septiesdecies</i> D.lgs. 231/2001	Delitti contro il patrimonio culturale	TRASCURABILE
Art. 25 - <i>duodevicies</i> D.lgs. 231/2001		
Art. 12, L. 9/2013	Reati in materia di contraffazione delle sostanze alimentari (applicabili agli enti che operano nell'ambito della filiera degli oli vergini di oliva)	TRASCURABILE
D.Lgs. 129/2024	Reati di abuso di mercato e abuso di informazioni privilegiate (mercati di crypto-valute)	TRASCURABILE

5.2 ELENCO DEI DOCUMENTI CONSULTATI PER LA PREDISPOSIZIONE DELL'ANALISI DEI RISCHI

PRINCIPALE DOCUMENTAZIONE DI RIFERIMENTO UTILIZZATA PER L'ANALISI DEL RISCHIO	
1.	Organigramma
2.	Visura Camerale
3.	Atto costitutivo
4.	Statuto
5.	Contratto di servizio tra il Comune di Trieste ed Esatto S.p.A. e successivi addendum
6.	Procura rep. 3467 del 30.05.2017 dott. Davide Fermo
7.	Codice Etico
8.	Codice di Comportamento Aziendale del Comune di Trieste
9.	Regolamento aziendale
10.	Modello di Organizzazione, Gestione e Controllo e relativi allegati
11.	Procedure e regolamenti aziendali di Esatto S.p.A.
12.	Documento Valutazione Rischi ex D.Lgs 81/2008 e relativi allegati

5.3 AZIONI SUGGERITE

Di seguito, vengono elencate alcune azioni suggerite per limitare il rischio Reato, meglio descritte in dettaglio nel corso dell'analisi che segue.

1. Previsione di misure minime di sicurezza indeterminate dall'art. 24 del D.Lgs. 138/2024, che recepisce la Direttiva (UE) 2022/2555 (Direttiva NIS 2) in materia di cybersicurezza e **predisposizione di specifiche procedure di prevenzione dei rischi informatici**, come:
 - Adozione di procedure di *cybersecurity* e *incident response plan*, compresi piani di gestione delle crisi informatiche, con indicazioni chiare quanto a doveri e responsabilità delle funzioni coinvolte;
 - Definizione di procedure per la segnalazione di incidenti informatici e gestione delle vulnerabilità;
 - Implementazione di un sistema di gestione della sicurezza informatica (ISMS) conforme agli standard internazionali, nonché di un sistema di monitoraggio e auditing periodico;
 - Nomina di un responsabile della sicurezza delle informazioni (CISO) e creazione di un team interno per la gestione della sicurezza informatica;
 - Formazione obbligatoria del personale su sicurezza informatica e protezione dei dati, con sessione di aggiornamento periodiche;
 - Adozione di misure disciplinari interne per i dipendenti che non rispettano le politiche di cybersecurity aziendali.
2. Aggiornamento della **procedura** che disciplina la **selezione del personale**, stabilendo preventivamente i requisiti minimi per rivestire il ruolo di membro di una Commissione esaminatrice in ragione del livello e delle mansioni dell'unità di personale oggetto del reclutamento, nonché prevedendo in capo alla commissione esaminatrice l'attività di verifica delle domande e dei relativi documenti presentati dai candidati.
3. Adozione di una **procedura** che disciplini gli **acquisti sotto soglia**.
4. Adozione di un sistema c.d. "**whistleblowing**", in conformità al D.Lgs. 24/2023, adottato in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali, al fine di assicurare un'efficace tutela del soggetto che segnali un illecito o una violazione del Modello di cui sia venuto a conoscenza in ragione delle funzioni svolte nell'ambito di un rapporto di impiego privato. In particolare, introduzione di:
 - a) obbligo di attivazione, mediante atto organizzativo e sentite le rappresentanze o le organizzazioni sindacali di cui all'art. 51 del d.lgs. n.81/2015, di canali di segnalazione interna;
 - b) affidamento del canale di segnalazione interna al Responsabile della Prevenzione della Corruzione e della Trasparenza, ove nominato;
 - c) implementazione di una specifica procedura per la gestione delle segnalazioni;
 - d) pubblicazione di informazioni chiare sul canale di segnalazione, sulle procedure e sui presupposti delle segnalazioni interne ed esterne, da (i) esporre nei luoghi di lavoro; (ii) rendere accessibili a chi, pur intrattenendo un rapporto giuridico con il soggetto obbligato, non lo frequenta abitualmente; (iii) pubblicare in una sezione dedicata del sito internet aziendale; e (iv) includere nei corsi e nelle formazioni in materia di etica e integrità;

- e) aggiornamento del sistema disciplinare adottato ai sensi dell'art. 6, c. 2, lett. e) del Decreto 231;
- f) redazione di specifica informativa ex artt. 13 e 14 del Regolamento UE n. 679/2016 ("GDPR") da fornire alle persone segnalanti e alle persone comunque coinvolte nella segnalazione;
- g) previsione e adozione di specifiche misure tecniche e organizzative per la gestione dei dati personali raccolti e trattati nel processo di segnalazione, ex art. 32 GDPR;
- h) effettuazione di una valutazione di impatto sulla protezione dei dati (c.d. "DPIA"), ex art. 35 GDPR;
- i) nomina formale degli incaricati al trattamento – ex art. 29 del GDPR ed art. 2-quaterdecies del D. Lgs. 196/2003 – e dei responsabili del trattamento – ex art. 28 del GDPR;
- j) aggiornamento del registro dei trattamenti, ex art. 30 GDPR;
- k) aggiornamento della policy sulla conservazione dei dati personali.

6 TAVOLE SINOTTICHE

SEZIONE A REATI CONTRO LA PUBBLICA AMMINISTRAZIONE		
Art. 24 D.lgs. 231/2001 - Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. Malversazione di erogazioni pubbliche (art. 316-bis c.p.) 2. Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.) 3. Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, comma 2, n.1, c.p.) 4. Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.) 5. Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.) 6. Frode nelle pubbliche forniture (art. 356 c.p.) 7. Frode ai danni del Fondo Europeo Agricolo di Garanzia e del Fondo Europeo Agricolo per lo Sviluppo Rurale (art. 2 L. 898/1986) 8. Turbata libertà degli incanti (art. 353 c.p.) 9. Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.)	
CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE
Attività sensibili	1. Utilizzo di software o banche dati della pubblica amministrazione: gestione di servizi informatici, con particolare riferimento ai diversi servizi forniti in favore del Comune di Trieste (trasmissione e acquisizione di dati; implementazione e modifica archivi e banche dati); 2. Contributi e finanziamenti pubblici: gestione delle attività di richiesta di contributi e/o finanziamenti pubblici;	

	3. Affidamento di incarichi esterni per attività di consulenza (rappresentazione del fabbisogno, scelta del contraente, obblighi di pubblicità ecc.); 4. Acquisizione di beni e servizi; 5. Gestione delle attività di aggiornamento e formazione.	
<i>Esistenza di Norme</i>	La Società ha adottato i seguenti Regolamenti e Procedure: 1. Codice Etico; 2. Procedure Rapporti con Pubblica Amministrazione; 3. Procedura Ispezioni, accessi, controlli e richieste di autorità pubbliche; 4. Regolamento per l'affidamento degli incarichi esterni; 5. Regolamento per il reclutamento del personale, in ossequio alle disposizioni del d.lgs. 175/2916 (Testo unico delle Società a partecipazione pubblica); 6. Procedura Conflitti di Interesse; 7. Procedura Liberalità, donazioni, regali e omaggi; 8. Procedura per Regali e Ospitalità ricevuti dai Dipendenti di Esatto S.p.A.; 9. Procedura Tracciabilità dei flussi finanziari, uso del contante e contributi economici pubblici; 10. Regolamento aziendale per la corretta gestione della Privacy e della Sicurezza Informatica nei luoghi di lavoro.	Il Regolamento aziendale per la corretta gestione della Privacy e della Sicurezza Informatica nei luoghi di lavoro prevede misure interne di sicurezza diffuse. Considerando che la Società gestisce i sistemi informatici impiegati nell'erogazione dei servizi in favore del Comune di Trieste, si consiglia di implementare il suddetto Regolamento mediante: (1) l'inserimento di strumenti per la tracciabilità degli accessi ai sistemi informatici; (2) la conservazione e il controllo della registrazione degli accessi al fine di favorire un controllo a posteriori in caso di frode.
<i>Separazione dei compiti</i>	È definita all'interno delle procedure adottate dalla Società. In generale, la presenza di un unico dirigente che riveste altresì il ruolo di Direttore Generale determina l'accentramento di molti poteri e funzioni in capo a quest'ultimo. Il principio organizzativo con funzione preventiva della segregazione delle funzioni trova pertanto uno spazio applicativo limitato.	Tenuto conto dell'impossibilità pratica di realizzare una rigida separazione dei compiti e dei ruoli, <u>il sistema di reporting verso l'Organismo di Vigilanza e la formazione continua risultano i più efficaci protocolli applicabili.</u>

SEZIONE B DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI		
<i>Art. 24-bis D.lgs. 231/2001 - Delitti informatici e trattamento illecito di dati</i>		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. Documenti informatici (art. 491-bis c.p.) 2. Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) 3. Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) 4. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) 5. Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) 6. Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) 7. 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.) 8. Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) 9. 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 c.p.) 10. Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.) 11. Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.) 12. Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 105/2019) 13. Estorsione (art. 629, comma 3, c.p.)	
CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE
<i>Attività sensibili</i>	1. Gestione dei servizi informatici: gestione e utilizzo degli account e del processo di autenticazione; gestione del processo di creazione, trattamento, archiviazione di documenti	

	elettronici con valore probatorio; gestione e profili e degli accessi agli strumenti informatici aziendali e protezione della postazione di lavoro; gestione dei sistemi hardware e software; gestione e protezione della rete telematica, banche dati e/o sistemi informativi della P.A; gestione degli output di sistema e dei dispositivi di memorizzazione; sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.). I reati compresi in questa area omogenea potrebbero essere astrattamente configurabili nello svolgimento delle attività svolte dalla Esatto S.p.A. dal momento che lo strumento informatico (software e hardware) risulta, infatti, essenziale per il raggiungimento di gran parte delle finalità istituzionali. La Società inoltre, in ragione dell'attività svolta in favore del Comune di Trieste socio unico, conserva e amministra archivi informatici di rilevante entità.	
Esistenza di Norme	La Società ha adottato un Regolamento per la corretta gestione della privacy e della sicurezza informatica nei luoghi di lavoro con particolare riferimento alle modalità di utilizzo degli strumenti di lavoro da parte del personale della Società per rendere la prestazione lavorativa (rev. 2 approvata con Delibera del CdA del 9 giugno 2017). Il predetto Regolamento prevede misure interne di sicurezza diffuse.	<u>Prevedere delle misure minime di sicurezza indeterminate dall'art. 24 del D.Lgs. 138/2024, che recepisce la Direttiva (UE) 2022/2555 (Direttiva NIS 2) in materia di cybersicurezza e predisporre, pertanto, specifiche procedure di prevenzione dei rischi informatici, come:</u> - Adozione di procedure di <i>cybersecurity</i> e <i>incident response plan</i>, compresi piani di gestione delle crisi informatiche, con indicazioni chiare quanto a doveri e responsabilità delle funzioni coinvolte; - Definizione di procedure per la segnalazione di incidenti informatici e gestione delle vulnerabilità; - Implementazione di un sistema di gestione della sicurezza informatica (ISMS) conforme agli standard internazionali, nonché di un sistema di monitoraggio e auditing periodico;

		- Nomina di un responsabile della sicurezza delle informazioni (CISO) e creazione di un team interno per la gestione della sicurezza informatica; - Formazione obbligatoria del personale su sicurezza informatica e protezione dei dati, con sessione di aggiornamento periodiche; - Adozione di misure disciplinari interne per i dipendenti che non rispettano le politiche di cybersecurity aziendali.
<i>Separazione dei compiti</i>	Non definita	
SEZIONE C CONCUSSIONE E CORRUZIONE – INDUZIONE INDEBITA A DARE O PROMETTERE UTILITA'		
Art. 25 D.lgs. 231/2001 Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. Concussione (art. 317 c.p.) 2. Corruzione per l'esercizio della funzione (art. 318 c.p.) 3. Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) 4. Corruzione in atti giudiziari (art. 319-ter c.p.) 5. Induzione indebita a dare o promettere utilità (art. 319-quater c.p.) 6. Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.) 7. Istigazione alla corruzione (art. 322 c.p.) 8. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.) 9. Traffico di influenze illecite (art. 346-bis c.p.)	

	10. Peculato (art. 314, comma 1, c.p.) 11. Peculato mediante profitto dell'errore altrui (art. 316 c.p.) 12. Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.)	
CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE
<i>Attività sensibili</i>	1. Rapporti istituzionali: gestione dei rapporti con il Comune di Trieste finalizzati alla gestione del Contratto di servizio e con altri enti pubblici; 2. Rapporti con il pubblico e con gli utenti: gestione delle attività di front office e di relazione con i cittadini contribuenti; 3. Richieste di provvedimenti: richiesta di provvedimenti amministrativi occasionali/ad hoc necessari allo svolgimento delle attività societarie; 4. Verifiche e Ispezioni da parte di autorità esterne: gestione di tutte le attività ispettive e di controllo effettuate presso la Società da parte di soggetti pubblici esterni; 5. Rapporti con autorità giudiziarie: gestione del contenzioso; 6. Contributi e finanziamenti pubblici: gestione delle attività di richiesta di contributi e/o finanziamenti pubblici; 7. Affidamento di incarichi esterni per attività di consulenza (rappresentazione del fabbisogno, scelta del contraente, obblighi di pubblicità ecc.); 8. Assunzione e gestione del personale, progressioni di carriera; 9. Acquisizione di beni e servizi; 10. Gestione delle attività di aggiornamento e formazione; 11. Gestione omaggi e ospitalità, spese di rappresentanza, donazione e sponsorizzazioni.	
<i>Esistenza di norme</i>	La Società ha adottato i seguenti Regolamenti e Procedure: A. Codice Etico;	Il regolamento per la gestione del personale presenta alcune carenze. In particolare, il procedimento selettivo prevede che il Direttore o suoi

	B. Procedure Rapporti con Pubblica Amministrazione; C. Procedura Ispezioni, accessi, controlli e richieste di autorità pubbliche; D. Regolamento per l'affidamento degli incarichi esterni; E. Regolamento per il reclutamento del personale, in ossequio alle disposizioni del d.lgs. 175/2916 (Testo unico delle Società a partecipazione pubblica); F. Procedura Conflitti di Interesse; G. Procedura Liberalità, donazioni, regali e omaggi; H. Procedura per Regali e Ospitalità ricevuti dai Dipendenti di Esatto S.p.A.; I. Procedura Tracciabilità dei flussi finanziari, uso del contante e contributi economici pubblici;	delegati procedono alla verifica delle domande e dei relativi documenti presentati. Si ritiene opportuno trasferire tale attività di valutazione preliminare in capo alla commissione esaminatrice. Non sono definiti preventivamente i requisiti minimi per rivestire il ruolo di membro di una Commissione esaminatrice in ragione del livello e delle mansioni dell'unità di personale oggetto del reclutamento. Non è previsto un Regolamento acquisti "sotto soglia". In ragione del fabbisogno di aggiornamento professionale continuo del personale, gli incarichi per attività formative sono frequenti. La previsione di un albo di esperti formatori da aggiornare periodicamente può garantire in modo più efficace la trasparenza e l'imparzialità della scelta del collaboratore.
<i>Separazione dei compiti</i>	È definita all'interno delle procedure adottate dalla Società. In generale, la presenza di un unico dirigente che riveste altresì il ruolo di Direttore Generale determina l'accentramento di molti poteri e funzioni in capo a quest'ultimo. Il principio organizzativo con funzione preventiva della segregazione delle funzioni trova pertanto uno spazio applicativo limitato.	Tenuto conto dell'impossibilità pratica di realizzare una rigida separazione dei compiti e dei ruoli, <u>il sistema di reporting verso l'Organismo di Vigilanza e la formazione continua risultano i più efficaci protocolli applicabili.</u>
SEZIONE D FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO		
Art. 25-bis D.lgs. 231/2001 - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento		

REATI PRESUPPOSTO	1. Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate 2. Alterazione di monete 3. Spendita e introduzione nello Stato, senza concerto, di monete falsificate 4. Spendita di monete falsificate ricevute in buona fede 5. Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati 6. Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo 7. Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata 8. Uso di valori di bollo contraffatti o alterati 9. Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni 10. Introduzione nello stato e commercio di prodotti con segni falsi	
VALUTAZIONE DEL RISCHIO POTENZIALE	BASSO	
CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE
<i>Attività sensibili</i>	Gestione dei pagamenti in contanti ricevuti dal pubblico agli sportelli in relazione alla possibile spendita di monete false ricevute in buona fede.	
<i>Esistenza di norme</i>	Non risultano adottati specifici protocolli o altre misure tecniche di rilevazione di monete/banconote false.	Prevedere l'introduzione di strumenti per la verifica dell'autenticità delle monete ricevute in pagamento agli sportelli e adottare un protocollo destinato ai dipendenti con responsabilità di cassa per la segnalazione delle falsità riscontrate e l'adozione dei provvedimenti conseguenti.

<i>Separazione dei compiti</i>	In mancanza di specifici protocolli, le relative responsabilità non possono essere distribuite tra soggetti diversi in una logica di processo.	Nell'elaborazione di un protocollo di prevenzione del rischio, prevedere un'adeguata separazione delle funzioni di processo tra diversi soggetti.
SEZIONE E REATI SOCIETARI		
Art. 25-ter D.lgs. 231/2001 - Reati societari.		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. False comunicazioni sociali (art. 2621 e 2621-bis c.c.) 2. False comunicazioni sociali delle società quotate (art. 2622 c.c.) 3. Impedito controllo (art. 2625, comma 2, c.c.) 4. Indebita restituzione dei conferimenti (art. 2626 c.c.) 5. Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.) 6. Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.) 7. Operazioni in pregiudizio dei creditori (art. 2629 c.c.) 8. Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) 9. Formazione fittizia del capitale (art. 2632 c.c.) 10. Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.) 11. Corruzione tra privati (art. 2635 c.c.) 12. Istigazione alla corruzione tra privati (art. 2635-bis c.c.) 13. Illecita influenza sull'assemblea (art. 2636 c.c.) 14. Aggiotaggio (art. 2637 c.c.) 15. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.) 16. False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023)	
CONTROLLI	SITUAZIONE ATTUALE	NOTE E SUGGERIMENTI

Attività sensibili	1. Gestione rapporti commerciali con i fornitori: gestione dei rapporti con i fornitori nell'ambito del processo di acquisizione di beni e servizi e relative fasi di negoziazione e contrattazione; 2. Predisposizione e gestione delle comunicazioni relative alla situazione economico-patrimoniale e finanziaria della Società: tenuta della contabilità, redazione del bilancio e delle comunicazioni sociali in genere, con particolare riferimento a quelle indirizzate al Comune di Trieste; gestione dei rapporti con il socio unico con particolare riferimento alle verifiche del budget annuale; gestione degli adempimenti relativi al funzionamento degli organi sociali; conservazione dei documenti societari visionabili da altri soggetti.	
Esistenza di Norme	La Società ha adottato i seguenti Regolamenti e Procedure: A. Codice Etico; B. Procedura Tracciabilità dei flussi finanziari, uso del contante e contributi economici pubblici; C. Regolamento per l'affidamento degli incarichi esterni; D. Procedura Conflitti di Interesse; E. Procedura Liberalità, donazioni, regali e omaggi; F. Procedura per Regali e Ospitalità ricevuti dai Dipendenti di Esatto S.p.A. Sono presenti gli organi di controllo obbligatori per legge. Il Comune di Trieste socio unico verifica, inoltre, il progetto di budget annuale.	
Separazione dei compiti	È definita all'interno delle procedure adottate dalla Società. In generale, la presenza di un unico dirigente che riveste altresì il ruolo di Direttore Generale determina l'accentramento di molti poteri e funzioni in capo a quest'ultimo. Il principio organizzativo con	Tenuto conto dell'impossibilità pratica di realizzare una rigida separazione dei compiti e dei ruoli, <u>il sistema di reporting verso l'Organismo di Vigilanza e la formazione continua risultano i più efficaci protocolli applicabili.</u>

	funzione preventiva della segregazione delle funzioni trova pertanto uno spazio applicativo limitato.	
SEZIONE F OMICIDIO COLPOSO LESIONI GRAVI O GRAVISSIME – SALUTE E SICUREZZA SUL LAVORO		
<i>Art. 25-septies D.lgs. 231/2001 - Omicidio colposo lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.</i>		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. Omicidio colposo (art. 589 c.p.) 2. Lesioni personali colpose (art. 590 c.p.)	
CONTROLLI	SITUAZIONE ATTUALE	SUGGERIMENTI E NOTE
<i>Attività sensibili</i>	Svolgimento delle mansioni assegnate ai lavoratori della Esatto S.p.A. ai fini dell'applicabilità del d.lgs. 81/2008. La natura delle attività svolte nonché la struttura delle sedi di lavoro non espongono i lavoratori ed i soggetti a questi equiparati a rischi elevati per la loro sicurezza.	
<i>Esistenza di norme</i>	Esatto S.p.A. ha formalmente identificato quale Datore di lavoro, il Direttore Generale (vd. procura), ed ha formalmente istituito il Servizio di Prevenzione e Protezione ("SPP"), esterno alla Società e composto esclusivamente dal Responsabile del Servizio	

	di Prevenzione e Protezione (“RSPP”). Non vi sono deleghe da parte del Datore di lavoro a dirigenti e/o preposti. L’incarico di RSPP è stato affidato ad un soggetto esterno alla Società e, precisamente, all’Ing. Andrea Guidolin della Società SQS S.r.l., specializzata in sicurezza sul lavoro e ambiente. Il RSPP, interfacciandosi costantemente con il Datore di lavoro e con il Responsabile HR, verifica che vengano attuate in Società le misure preventive e protettive che sono state definite nel documento di valutazione dei rischi (“DVR”) e nel piano di miglioramento. La Società ha, altresì, provveduto alla nomina del Medico competente, esterno alla Società, e dell’addetto antincendio e del primo soccorso. L’organizzazione del sistema prevenzionistico in Società è gestita dal Datore di lavoro, dal Medico competente, dagli addetti alle emergenze e dal RSPP, che suggerisce le strategie da intraprendere, ed è formalizzata nel DVR. Il Datore di lavoro ha effettuato la valutazione dei rischi. Nel processo valutativo sono stati coinvolti sia il RSPP che il Medico competente. La valutazione ha riguardato tutta la Società, tutti i rischi potenziali e tutti i lavoratori dipendenti o ad essi equiparati. È, altresì, prevista una procedura per l’aggiornamento della valutazione dei rischi nei casi di sopravvenienza di significative variazioni organizzative, degli ambienti e dei metodi di lavoro. È stata effettuata la valutazione del rischio di incendio ex DM 10/03/98, in base alla quale il luogo di lavoro è stato definito a basso rischio. In Società sono presenti sia adeguate attrezzature per il primo soccorso sia attrezzature antincendio: la manutenzione degli estintori e la gestione del Registro di Sicurezza Antincendio sono affidate ad una ditta esterna.	
--	---	--

	È previsto un dettagliato Piano di emergenza sul cui contenuto sono stati informati tutti i lavoratori. Esiste, altresì, un Piano di evacuazione, che stabilisce un programma di addestramento periodico all'evacuazione (le esercitazioni pratiche vengono effettuate annualmente). Le planimetrie di sicurezza sono affisse sul muro ed esposte al pubblico e le modalità di evacuazione vengono spiegate a tutto il personale al momento dell'assunzione nel corso della formazione. Non è previsto un vero e proprio programma formalizzato di attuazione degli interventi preventivi e protettivi, ma si interviene al bisogno. È stato attivato un sistema informativo aziendale in materia di salute e sicurezza sul lavoro, sui rischi dell'impresa e sulle misure di prevenzione adottate, mediante l'affissione di avvisi in bacheca, l'invio al personale di circolari tramite l'intranet aziendale (ad esempio, la comunicazione sulla valutazione del rischio da stress lavoro correlato) e lezioni in aula. Tale sistema informativo riguarda tutti i lavoratori dipendenti e/o ad essi equiparati (anche nel caso di lavoratori in somministrazione è il RSPP di Esatto S.p.A. a fornire le informazioni necessarie). Per quanto riguarda la formazione in materia di sicurezza sul lavoro, il calendario degli eventi formativi viene gestito di volta in volta per garantire la continuità dei servizi resi dalla Società. Viceversa, lo scadenziario della formazione è formalizzato. La formazione riguarda tutti i lavoratori della Società ed è svolta mediante lezioni frontali con il RSPP, il Medico competente e i tecnici antincendio (<i>ex</i> Vigili del Fuoco), distribuzione di materiale ed esercitazioni pratiche. Al termine della formazione sono sempre previste delle verifiche del livello di apprendimento e viene rilasciato un attestato di partecipazione al corso. Sono stati fatti corsi di formazione ed aggiornamento per quelle figure che	
--	---	--

	necessitano di una formazione aggiuntiva, quali il RSPP e gli addetti alle emergenze. Ai sensi dell'art. 30 del d.lgs. 81/2001, affinché il modello di organizzazione e di gestione ex d.lgs. 231 abbia efficacia esimente della responsabilità amministrativa della Esatto S.p.A., è necessario assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi richiamandolo nella parte speciale dello stesso modello.	
<i>Segregazione delle funzioni</i>	Nell'ambito del sistema di gestione della sicurezza sui luoghi di lavoro, i ruoli e le relative responsabilità sono ben definiti.	
SEZIONE G RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA – AUTORICICLAGGIO DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI		
<i>Art. 25-octies D.lgs. 231/2001 – Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio.</i> <i>Art. 25-octies.1 D.lgs. 231/2001 - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori.</i>		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. Ricettazione (art. 648 c.p.) 2. Riciclaggio (art. 648-bis c.p.) 3. Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) 4. Autoriciclaggio (art. 648-ter.1 c.p.) 5. Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.) 6. Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.) 7. Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)	

	8. Trasferimento fraudolento di valori (art. 512-bis c.p.)	
CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE
<i>Attività sensibili</i>	Relazioni con il pubblico (contribuenti): pagamenti e operazioni in contanti; Utilizzo del contante: pagamenti e operazioni in contanti; Ciclo passivo: identificazione fornitori, registrazione operazioni; - Gestione delle carte di credito aziendali; - Gestione dei flussi monetari e finanziari in entrata e in uscita; - Acquisto di beni come apparecchiature, dispositivi e programmi informatici; - Gestione e utilizzo degli account, profili e accessi agli strumenti informatici aziendali, gestione dei sistemi hardware e software, della rete telematica; - Gestione delle attività nell'ambito del processo di predisposizione delle dichiarazioni fiscali Iva e Ires; - Tenuta della contabilità, predisposizione del bilancio e redazione di comunicazioni sociali in genere; gestione degli adempimenti relativi al funzionamento degli organi sociali; conservazione dei documenti societari visionabili da altri soggetti; - Archiviazione dei documenti aziendali, delle scritture contabili e dei registri fiscali obbligatori, fatturazione elettronica e sistemi di backup.	
<i>Esistenza di Norme</i>	La Società ha adottato i seguenti Regolamenti e Procedure: - Codice Etico; - Procedura Tracciabilità dei flussi finanziari, uso del contante e contributi economici pubblici;	

	3. Procedura Ispezioni, accessi, controlli e richieste di autorità pubbliche; 4. Regolamento per l'affidamento degli incarichi esterni; 5. Procedura Conflitti di Interesse; 6. Procedura Liberalità, donazioni, regali e omaggi; 7. Procedura per Regali e Ospitalità ricevuti dai Dipendenti di Esatto S.p.A.; 8. Regolamento aziendale per la corretta gestione della Privacy e della Sicurezza Informatica nei luoghi di lavoro.	
<i>Separazione dei compiti</i>	È definita all'interno delle procedure adottate dalla Società. In generale, la presenza di un unico dirigente che riveste altresì il ruolo di Direttore Generale determina l'accentramento di molti poteri e funzioni in capo a quest'ultimo. Il principio organizzativo con funzione preventiva della segregazione delle funzioni trova pertanto uno spazio applicativo limitato.	Tenuto conto dell'impossibilità pratica di realizzare una rigida separazione dei compiti e dei ruoli, <u>il sistema di reporting verso l'Organismo di Vigilanza e la formazione continua risultano i più efficaci protocolli applicabili.</u>
SEZIONE H DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE		
Art. 25-novies D.lgs. 231/2001 - Delitti in materia di violazione del diritto d'autore		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATO PRESUPPOSTO	1. Violazione del diritto d'autore	
CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE

<i>Attività sensibili</i>	Utilizzo di software, di sistemi gestionali, archivi e piattaforme informatiche per lo svolgimento delle attività istituzionali della società.	
<i>Esistenza di norme</i>	La Società ha adottato un Regolamento per la corretta gestione della privacy e della sicurezza informatica nei luoghi di lavoro (rev. 2 approvata con Delibera del CdA del 9 giugno 2017. Il predetto Regolamento prevede misure interne di sicurezza diffuse.	Integrare la procedura prevedendo un sistema centralizzato per la verifica delle eventuali scadenze delle licenze software in uso presso la società al fine di poter provvedere al tempestivo rinnovo. Introdurre un registro dei software in uso presso ogni postazione del sistema informatico.
<i>Separazione dei compiti</i>	Non definita ai fini della configurabilità dei reati compresi in questa area omogenea.	Definire formalmente le responsabilità nella gestione delle licenze software.
SEZIONE I INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA		
<i>Art. 25-decies D.lgs 231/2001 - Delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.</i>		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATO PRESUPPOSTO	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)	
CONTROLLI	SITUAZIONE RISCOSTRATA	SUGGERIMENTI E NOTE
<i>Attività Sensibili</i>	a) Gestione del contenzioso giudiziale:	

	- gestione dei rapporti con amministratori, dipendenti o terzi coinvolti in procedimenti innanzi all'Autorità Giudiziaria o chiamati a rendere dichiarazioni utilizzabili in procedimenti penali innanzi all'Autorità Giudiziaria; b) Partecipazione ad indagini dell'Autorità Giudiziaria, delle Autorità di Polizia Giudiziaria e Pubblica Sicurezza: - comunicazione di informazioni o consegna di documenti alle medesime Autorità, ovvero attività prope-deutiche ad esse, per conto della Società stessa.	
<i>Esistenza di Norme</i>	Nel Modello Organizzativo è stata previsto il seguente protocollo di prevenzione: ogni notizia o notifica di indagine ovvero ogni richiesta di testimonianza o audizione derivante dall'autorità giudiziaria relativa – anche indirettamente ed in misura marginale – all'attività aziendale, è comunicata per iscritto dal soggetto interessato a: (i) il Consiglio di Amministrazione; (ii) il Direttore Generale; (iii) il Collegio Sindacale; (iv) l'Organismo di Vigilanza.	
SEZIONE J IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE		
Art. 25-duodecies D.lgs 231/2001 - Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare		
VALUTAZIONE DEL RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3-bis, 3-ter e 5, D.Lgs. 286/1998) 2. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-bis, D.Lgs. 286/1998)	

CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE
<i>Attività sensibili</i>	a) Gestione del personale: - attività di selezione e assunzione del personale. In particolare, l'eventuale assunzione di un cittadino non comunitario potrebbe generare un rischio commissione del reato richiamato nella presente sezione.	
<i>Esistenza di Norme</i>	Le attività relative al reclutamento del personale sono disciplinate da apposito Regolamento approvato con deliberazione del Consiglio di Amministrazione del 16.12.2013 e modificato con deliberazione del Consiglio di Amministrazione del 03.04.2017. Nel Modello Organizzativo adottato dalla Società sono inoltre previsti i seguenti protocolli di prevenzione: - i candidati cittadini di paesi terzi ai quali è richiesto il permesso di soggiorno per svolgere prestazioni lavorative, al momento del colloquio valutativo, devono presentare al Responsabile Risorse Umane il permesso di soggiorno in originale e la chiara indicazione della sua scadenza. Copia di tale documentazione è archiviata da Esatto S.p.A.; - la scadenza di eventuali permessi di soggiorno è scadenzata dal Responsabile Risorse Umane; - almeno annualmente il Responsabile Risorse Umane svolge un controllo "a sorpresa" circa la sussistenza del permesso di soggiorno (che potrebbe essere revocato anche precedentemente alla data di scadenza). Tale controllo avviene con la richiesta al lavoratore di produrre tale documento in originale per visione. La richiesta e l'esito sono archiviati da Esatto S.p.A.;	

	- ad ogni scadenza il Responsabile Risorse Umane richiede copia del rinnovo o del nuovo permesso di soggiorno al soggetto interessato. Copia di tale documentazione è archiviata da Esatto S.p.A.; - in caso di irregolarità dei permessi qui considerati, il Responsabile Risorse Umane avvisa immediatamente (i) il Presidente del Consiglio di Amministrazione; (ii) il Presidente del Collegio Sindacale; (iii) l'Organismo di Vigilanza; (iv) il Direttore Generale.	
SEZIONE K REATI TRIBUTARI		
Art. 25 quinquiesdecies d.lgs 231/2001 – Reati tributari.		
VALUTAZIONE RISCHIO POTENZIALE	MEDIO	
REATI PRESUPPOSTO	1. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, D.Lgs. 74/2000) 2. Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 74/2000) 3. Dichiarazione infedele (art. 4, D.Lgs. 74/2000) 4. Omessa dichiarazione (art. 5, D.Lgs. 74/2000) 5. Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.Lgs. 74/2000) 6. Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 74/2000) 7. Indebita compensazione (art. 10-quater, D.Lgs. 74/2000) 8. Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 74/2000)	
CONTROLLI	SITUAZIONE RISCONTRATA	SUGGERIMENTI E NOTE
<i>Attività sensibili</i>	1. Predisposizione e gestione delle comunicazioni relative alla situazione economico-patrimoniale e finanziaria della Società: tenuta della contabilità, redazione del bilancio	

	e delle comunicazioni sociali in genere; gestione degli adempimenti relativi al funzionamento degli organi sociali; conservazione dei documenti societari visionabili da altri soggetti; archiviazione dei documenti aziendali, delle scritture contabili e dei registri fiscali obbligatori, fatturazione elettronica e sistemi di backup; 2. Versamento imposte: gestione delle attività nell’ambito del processo di predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria; 3. Gestione rapporti commerciali con i fornitori: gestione dei rapporti con i fornitori nell’ambito del processo di acquisizione di beni e servizi e relative fasi di negoziazione e contrattazione.	
<i>Esistenza di Norme</i>	Sono presenti gli organi di controllo obbligatori per legge. La Società ha adottato le seguenti Procedure e Regolamenti: 1. Regolamento per l’affidamento degli incarichi esterni; 2. Procedura Liberalità, donazioni, regali e omaggi; 3. Procedura per Regali e Ospitalità ricevuti dai Dipendenti di Esatto S.p.A. (contenuta nel Codice etico); 4. Procedura Tracciabilità dei flussi finanziari, uso del contante e contributi economici pubblici.	