

COMPAGNIA SIDERURGICA S.P.A.

PARTE SPECIALE

Deliberato dal Consiglio di Amministrazione in data 18 dicembre 2025, sostituisce le versioni precedenti del 01.12.2021 e del settembre 2018

Sommario

1. Art. 25 – Septies: Salute e Sicurezza sul lavoro	6
1.1. Struttura organizzativa in materia di SSL	6
1.2. Aggiornamento normativo in materia di SSL	6
1.3. Modalità di valutazione del rischio	7
1.3.1. Predisposizione e aggiornamento del documento di valutazione dei rischi (DVR)	7
1.4. Individuazione, approvvigionamento, Gestione, distribuzione e mantenimento in efficienza dei dpi	8
1.5. Gestione delle emergenze, prevenzione incendi ed evacuazione dei lavoratori	8
1.6. Svolgimento delle riunioni periodiche	9
1.7. Coinvolgimento dei lavoratori	9
1.8. Gestione sorveglianza sanitaria	10
1.9. Informazione e formazione dei lavoratori	11
1.10. Rilevazione e registrazione degli infortuni e dei mancati incidenti	11
1.11. Gestione delle manutenzioni e dei controlli periodici	12
1.12. Gestione dei rapporti con i fornitori e appaltatori con riferimento alle tematiche connesse alla SSL	12
1.13. Gestione cantieri fissi o mobili (per attività rientranti nel Titolo IV del TUS) in qualità di committente delle opere	13
1.14. Gestione delle verifiche circa il rispetto delle procedure operative e istruzioni di lavoro in materia di SSL	14
1.15. Flussi informativi da e verso l' OdV	14
2. Reati nei rapporti con la Pubblica Amministrazione	15
2.1 Attività sensibili	16
2.2 Principi di comportamento	17
2.3 Nomina delle funzioni competenti e formazione	19
2.4 Flussi informativi da e verso l'Organismo di Vigilanza	20
2.5. Protocolli	21
2.5.1. Protocollo per la gestione di adempimenti verso Enti Pubblici in materia di sicurezza e igiene del lavoro (D.Lgs. 81/2008)	21
2.5.2. Protocollo per la gestione di adempimenti connessi all'assunzione di personale appartenente a categorie protette o soggetto ad agevolazioni pubbliche	22
2.5.3. Protocollo per la gestione di verifiche, controlli e accertamenti da parte della Pubblica Amministrazione	22
2.5.4. Protocollo per l'acquisizione e la gestione di contributi, sovvenzioni e finanziamenti pubblici	23
2.5.5. Protocollo per la gestione di omaggi e liberalità nei confronti di funzionari pubblici	23
2.5.6. Protocollo per la partecipazione a gare, appalti o altre procedure di aggiudicazione con la Pubblica Amministrazione	24
3. Razzismo e xenofobia	24
3.1 Attività a rischio sensibile	25

3.2 Principi di comportamento e presidi di prevenzione	25
3.3 Flussi informativi da e verso l'Organismo di Vigilanza	26
4. Delitti informatici e trattamento illecito di dati	27
4.1 Attività a rischio sensibile.....	27
4.2 Principi di comportamento e presidi di prevenzione	28
4.3 Flussi informativi da e verso l'Organismo di Vigilanza	29
4.4. Protocolli operativi.....	29
5. Reati societari	30
5.1 Attività a rischio sensibile.....	31
5.2 Principi di comportamento e presidi di prevenzione	31
5.3 Flussi informativi da e verso l'Organismo di Vigilanza	32
5.4 Protocolli di prevenzione	33
6. Delitti di criminalità organizzata.....	34
6.1 Attività a rischio sensibile.....	35
6.2 Principi di comportamento e presidi di prevenzione	35
6.3 Flussi informativi da e verso l'Organismo di Vigilanza	36
7. Falsità in monete, carte di pubblico credito e valori di bollo.....	37
7.1 Attività a rischio sensibile.....	37
7.2 Principi di comportamento e presidi di prevenzione	38
7.3 Flussi informativi da e verso l'Organismo di Vigilanza	38
8. Delitti contro l'industria e il commercio (art. 25-bis.1 D.Lgs. 231/2001)	39
8.1 Attività a rischio sensibile.....	39
8.2 Principi di comportamento e presidi di prevenzione	40
8.3 Flussi informativi da e verso l'Organismo di Vigilanza	40
8.4 Protocolli di prevenzione	41
8.4.1. Protocollo per la gestione di marchi, segni distintivi e comunicazione commerciale	41
8.4.2. Protocollo per la veridicità delle specifiche tecniche e dei documenti di fornitura.....	41
8.4.3. Protocollo per la tracciabilità dei prodotti e la gestione delle non conformità verso il mercato.....	41
8.4.4. Protocollo per la qualificazione e il monitoraggio dei fornitori	41
8.4.5. Protocollo per la gestione delle comunicazioni di marketing e comparazioni	42
8.4.6. Protocollo per le segnalazioni e i richiami di prodotto verso il mercato	42
9. Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio.....	42
9.1 Attività a rischio sensibile.....	42
9.2 Principi di comportamento e presidi di prevenzione	43
9.3 Flussi informativi da e verso l'Organismo di Vigilanza	44
9.4 Processi sensibili e Protocolli di prevenzione.....	44
9.4.1 Protocollo per la gestione dei flussi finanziari con clienti, fornitori e partner	44
9.4.2 Protocollo per la gestione delle sponsorizzazioni.....	45

9.4.3 Protocollo per l'acquisto di beni e servizi	46
9.4.4 Protocollo per l'affidamento di consulenze	46
9.4.5 Protocollo per la Selezione e Gestione dei Fornitori	46
10. Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1)	46
10.1 Attività a rischio sensibile	47
10.2 Principi di comportamento e presidi di prevenzione	47
10.3 Flussi informativi da e verso l'Organismo di Vigilanza	48
11. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies)	48
11.1 Attività a rischio sensibile	49
11.2 Principi di comportamento e presidi di prevenzione	49
11.3 Flussi informativi da e verso l'Organismo di Vigilanza	50
12. Contrabbando (art. 25-sexiesdecies)	50
12.1 Attività a rischio sensibile	51
12.2 Principi di comportamento e presidi di prevenzione	51
12.3 Flussi informativi da e verso l'Organismo di Vigilanza	52
12.4 Protocollo per le attività di registrazione e preparazione dei dati contabili	52
13. Reati ambientali (art. 25-undecies)	53
13.1 Attività a rischio sensibile	54
13.2 Principi di comportamento e presidi di prevenzione	55
13.3 Principi generali in materia di ecoreati e rapporto tra Modello 231 e Sistema di Gestione Ambientale	55
13.4 Protocollo per l'acquisto di materie prime	56
13.5 Protocollo per la classificazione e la gestione dei rifiuti	56
13.6 Flussi informativi da e verso l'Organismo di Vigilanza	57
14. Reati tributari (art. 25-quinquiesdecies)	57
14.1 Attività a rischio sensibile	58
14.2 Principi di comportamento e presidi di prevenzione	58
14.3 Flussi informativi da e verso l'Organismo di Vigilanza	59
14.4 Protocollo per le attività di registrazione e preparazione dei dati contabili	59
15. Tabella riassuntiva protocolli, flussi, responsabili e frequenze	60

La presente Parte Speciale costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo adottato da Compagnia Siderurgica S.p.A. ai sensi del Decreto Legislativo 8 giugno 2001, n. 231. Essa è stata elaborata a seguito di un'analisi dei processi aziendali e dei rischi connessi allo svolgimento delle attività, con l'obiettivo di individuare le aree operative maggiormente esposte alla possibile commissione dei reati previsti dal Decreto.

La Parte Speciale deve essere interpretata e applicata in coerenza con la Parte Generale del Modello, con il Codice Etico, con la procedura di segnalazione delle violazioni (whistleblowing) e con gli strumenti organizzativi che descrivono il sistema di gestione e valutazione dei rischi in chiave 231 adottati dalla Società.

Attraverso questo documento, Compagnia Siderurgica S.p.A. intende rafforzare il proprio sistema di prevenzione e controllo, fornendo regole chiare e comportamenti attesi in relazione alle aree sensibili, così da favorire la responsabilizzazione diffusa e garantire un presidio costante nei confronti delle attività a rischio.

1. Art. 25 – Septies: Salute e Sicurezza sul lavoro

Si provvede qui di seguito a fornire una breve descrizione dei reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'articolo 25-septies del Decreto (anche ai sensi del art. 30 del D.lgs. 81/08)

L'art. 25-septies del D.Lgs. 231/2001 disciplina la responsabilità amministrativa dell'ente nei casi in cui, in violazione della normativa sulla salute e sicurezza sul lavoro, vengano cagionate per colpa specifica la morte (art. 589 c.p.) o lesioni personali gravi o gravissime (art. 590, co. 3 c.p.) a lavoratori o terzi. Perché si configuri la responsabilità dell'ente, l'evento lesivo deve derivare dalla violazione di specifiche norme antinfortunistiche e realizzarsi nell'interesse o a vantaggio dell'organizzazione. Le sanzioni previste comprendono sia pesanti sanzioni pecuniarie (fino a 1000 quote), sia sanzioni interdittive (es. interdizione dall'attività, sospensione di autorizzazioni, esclusione da appalti o agevolazioni pubbliche), applicabili anche in assenza di dolo, in presenza di condotta colposa. La società è certificata ISO 45001, che attesta l'adozione di un Sistema di Gestione per la Salute e Sicurezza sul Lavoro volto alla prevenzione degli infortuni e delle malattie professionali, nonché al miglioramento continuo delle condizioni di lavoro e della cultura della sicurezza all'interno dell'organizzazione.

1.1. Struttura organizzativa in materia di SSL

La definizione di ruoli e responsabilità in materia di salute e sicurezza sul lavoro (SSL) avviene in conformità alle disposizioni del D.Lgs. 81/2008 e coerentemente con l'assetto organizzativo e funzionale della Società. Il Datore di Lavoro, individuato nel Consiglio di Amministrazione, detiene la responsabilità generale dell'organizzazione e i poteri decisionali e di spesa. Il Responsabile del Servizio di Prevenzione e Protezione (RSPP), in possesso dei requisiti di legge, è nominato con apposito atto scritto dal Datore di Lavoro. I Preposti sono designati formalmente e formati secondo quanto previsto dalla normativa. Il Medico Competente è incaricato per iscritto e partecipa alla valutazione dei rischi e alla sorveglianza sanitaria. Il Rappresentante dei Lavoratori per la Sicurezza (RLS) è eletto dai lavoratori ed è formato ai sensi di legge. Gli addetti al primo soccorso e alla prevenzione incendi sono designati formalmente e operano sulla base delle procedure di emergenza. L'organigramma della sicurezza, che riporta tali figure e le rispettive interrelazioni, è predisposto e reso conoscibile all'interno dell'azienda con modalità idonee. L'aggiornamento avviene in occasione di modifiche organizzative, mentre il controllo dei requisiti necessari per ciascun ruolo è curato dal Servizio di Prevenzione e Protezione nell'ambito delle verifiche periodiche previste.

1.2. Aggiornamento normativo in materia di SSL

La Società assicura un aggiornamento costante rispetto all'evoluzione della normativa in materia di salute e sicurezza sul lavoro, quale requisito fondamentale ai sensi dell'art. 30, comma 1, lett. a), del D.Lgs. 81/2008.

Il monitoraggio delle fonti legislative, regolamentari e giurisprudenziali viene svolto in modo sistematico, anche mediante il supporto di consulenti esterni e la partecipazione a percorsi formativi dedicati. In tale ambito, il RSPP rappresenta una figura strategica, fornendo assistenza tecnica qualificata nella corretta interpretazione e attuazione della normativa vigente. Le eventuali modifiche rilevanti comportano, se necessario, l'aggiornamento del DVR, delle misure di prevenzione e delle procedure aziendali. Il processo è documentato e costituisce oggetto di rendicontazione periodica all'Organismo di Vigilanza.

1.3. Modalità di valutazione del rischio

La Società ha adottato un sistema formalizzato per l'identificazione dei pericoli e la valutazione dei rischi in materia di salute e sicurezza sul lavoro, in conformità agli artt. 17 e 28 del D.Lgs. 81/2008. Tale valutazione non costituisce un mero adempimento documentale, ma un processo continuo e integrato, volto a orientare le scelte organizzative e prevenire eventi dannosi, anche ai fini del D.Lgs. 231/2001. L'approccio adottato è di tipo proattivo: l'analisi dei rischi precede e guida l'introduzione di nuovi impianti, attività o processi, promuovendo misure volte a evitare il verificarsi di eventi critici.

Il processo si articola in più fasi: identificazione dei pericoli (ambienti, mansioni, sostanze, attrezzature, DPI/DPC), individuazione dei rischi correlati, stima del rischio tramite l'applicazione di matrici che combinano probabilità e gravità, valutazione dei risultati secondo norme, buone prassi e standard interni, individuazione delle misure di prevenzione e protezione con attribuzione delle responsabilità, e programmazione degli interventi migliorativi. Per rischi specifici, vengono adottate metodologie riconosciute.

Il processo è formalizzato nel Documento di Valutazione dei Rischi (DVR), che costituisce riferimento per formazione, consultazione, sorveglianza sanitaria e gestione operativa. La valutazione tiene conto dei gruppi omogenei di lavoratori, consentendo interventi proporzionati al rischio effettivo. Il DVR è soggetto ad aggiornamento ogniqualvolta si verificano modifiche organizzative o eventi rilevanti, nel rispetto del principio di miglioramento continuo.

1.3.1. Predisposizione e aggiornamento del documento di valutazione dei rischi (DVR)

In attuazione dell'art. 17 del D.Lgs. 81/2008, il Datore di Lavoro provvede alla valutazione di tutti i rischi per la salute e sicurezza nei luoghi di lavoro, con il supporto del Responsabile del Servizio di Prevenzione e Protezione e del Medico Competente, e previa consultazione del Rappresentante dei Lavoratori per la Sicurezza. La valutazione considera la struttura aziendale, la natura delle attività svolte, la configurazione degli ambienti di lavoro, l'organizzazione del personale, le sostanze impiegate e le attrezzature utilizzate.

Il Documento di Valutazione dei Rischi (DVR) è sottoscritto dal Datore di Lavoro, dal RSPP, dal Medico Competente e dall'RLS. Esso viene aggiornato in occasione di significative modifiche organizzative o

produttive, di innovazioni normative o tecniche, in seguito a infortuni rilevanti o quando emergano criticità dalla sorveglianza sanitaria. Il contenuto del DVR è oggetto di confronto nell'ambito della riunione periodica ex art. 35 TUS. Il DVR è conservato presso la sede operativa della Società e reso accessibile ai soggetti legittimati, secondo quanto previsto dalla normativa vigente.

1.4. Individuazione, approvvigionamento, Gestione, distribuzione e mantenimento in efficienza dei dpi

Ai sensi dell'art. 74 del D.Lgs. 81/2008, i Dispositivi di Protezione Individuale (DPI) sono attrezzature destinate a essere indossate dal lavoratore per proteggerlo contro uno o più rischi che possano comprometterne la salute o la sicurezza durante l'attività lavorativa. L'individuazione dei DPI avviene in esito alla valutazione dei rischi riferita ai gruppi omogenei di lavoratori, come formalizzata nel DVR.

L'introduzione di nuovi DPI, o la modifica di quelli già in uso, è subordinata alla preventiva valutazione da parte del RSPP e del Medico Competente, con consultazione dell'RLS. L'acquisto è curato dal Datore di Lavoro sulla base delle specifiche tecniche identificate dal RSPP, nel rispetto dei requisiti normativi e con verifica della documentazione attestante la marcatura CE e la conformità del dispositivo.

La consegna dei DPI è tracciata mediante apposita modulistica. I lavoratori hanno a disposizione anche il distributore dei DPI. I lavoratori sono tenuti a utilizzare i DPI secondo le indicazioni ricevute attraverso la formazione, le istruzioni operative, la segnaletica e le schede rischio. Devono inoltre custodirli correttamente, evitare modifiche non autorizzate e segnalare tempestivamente eventuali difetti o malfunzionamenti.

La responsabilità per garantire la disponibilità, la sostituzione e la corretta manutenzione dei DPI è attribuita al datore di lavoro, secondo l'assetto organizzativo definito dalla Società.

1.5. Gestione delle emergenze, prevenzione incendi ed evacuazione dei lavoratori

La gestione delle emergenze rappresenta un presidio fondamentale del sistema aziendale di tutela della salute e sicurezza sul lavoro, volto a garantire un'efficace capacità di risposta agli eventi imprevisti e a salvaguardare l'incolumità delle persone, il patrimonio aziendale e la continuità operativa.

A tal fine, la Società adotta un Piano di emergenza aggiornato e coerente con i rischi specifici presenti nell'ambiente di lavoro. Il documento individua le possibili situazioni emergenziali (es. incendi, eventi naturali, malori improvvisi), le modalità di segnalazione e gestione degli eventi, nonché i compiti e le responsabilità delle figure coinvolte. Il Piano persegue obiettivi quali: l'immediato riconoscimento dell'emergenza, il contenimento tempestivo degli effetti, la protezione del personale presente e la salvaguardia dei beni aziendali.

Tutti i lavoratori sono informati e formati sulle procedure di emergenza. Le istruzioni operative e le norme comportamentali da seguire in caso di pericolo sono rese disponibili in azienda tramite apposita cartellonistica. La squadra di emergenza, composta da lavoratori adeguatamente selezionati, riceve specifica formazione e addestramento in materia di antincendio, primo soccorso ed evacuazione.

La Società assicura lo svolgimento di prove di evacuazione con cadenza almeno annuale, finalizzate alla verifica dell'efficacia del Piano e alla familiarizzazione del personale con le procedure di sicurezza; l'esito delle esercitazioni è formalizzato in apposito verbale a cura del RSPP.

In relazione al rischio incendio, la Società effettua una valutazione dedicata, contenuta nel DVR, la quale è oggetto di aggiornamento ogniqualvolta si verifichino modifiche significative all'organizzazione, alla struttura, ai processi o ai carichi di incendio.

1.6. Svolgimento delle riunioni periodiche

La riunione periodica in materia di salute e sicurezza sul lavoro, prevista dall'art. 35 del D.Lgs. 81/2008, costituisce un momento essenziale per garantire la partecipazione attiva delle figure aziendali coinvolte e per consolidare il sistema di gestione della sicurezza. La Società organizza tale riunione con cadenza almeno annuale o in occasione di significative variazioni normative, organizzative o produttive che possano incidere sul livello di rischio.

Alla riunione partecipano il Datore di Lavoro, il Responsabile del Servizio di Prevenzione e Protezione, il Medico Competente, il Rappresentante dei Lavoratori per la Sicurezza (RLS) e, ove necessario, altri referenti aziendali coinvolti nella gestione della SSL. Durante l'incontro vengono analizzati, tra gli altri, i seguenti temi: aggiornamento del Documento di Valutazione dei Rischi (DVR), andamento infortunistico e della sorveglianza sanitaria, stato dei dispositivi di protezione individuale, programmi di formazione e informazione, e azioni di miglioramento.

Le misure individuate nel corso della riunione vengono formalizzate in un apposito programma di miglioramento, con l'indicazione delle priorità, dei soggetti incaricati e dei tempi di attuazione. Il relativo verbale, redatto dal RSPP e controfirmato dai partecipanti, viene archiviato a cura dell'azienda.

1.7. Coinvolgimento dei lavoratori

Il coinvolgimento dei lavoratori ed in particolare dei loro Rappresentanti è un processo che non solo viene evidenziato dalle norme di legge, ma costituisce un passaggio chiave per la diffusione delle informazioni, delle novità e delle predisposizioni aziendali in materia. I RLS sono eletti dai lavoratori, conformemente alla normativa vigente (Sezione VII del TUS), e agli stessi è erogata la formazione in materia di salute e sicurezza concernente i rischi specifici esistenti negli ambiti in esercita la propria rappresentanza, in accordo con le

disposizioni dell'art. 37 del TUS. I RLS sono preventivamente consultati, dal RSPP, dal DL e dal MC, nell'ambito della valutazione dei rischi e nella scelta dei DPI. I RLS partecipano alla riunione periodica di cui all'Art. 35 del TUS, nella quale vengono esposti gli argomenti trattati nel corso dell'anno, le statistiche, la programmazione ed altri temi riguardanti la tutela della sicurezza e della salute in azienda. Il coinvolgimento degli stessi, inoltre, è attuato secondo quanto disposto dall'art. 50 del TUS.

1.8. Gestione sorveglianza sanitaria

La Società garantisce la tutela della salute dei lavoratori attraverso un'efficace attività di sorveglianza sanitaria, rivolta a prevenire l'insorgenza o l'aggravamento di patologie correlate ai rischi lavorativi. Tale attività comprende lo svolgimento di visite mediche preventive, periodiche, su richiesta del lavoratore, in occasione del cambio di mansione o del rientro al lavoro dopo un'assenza per motivi di salute superiore a 60 giorni continuativi, nonché sopralluoghi periodici negli ambienti di lavoro.

A tal fine, la Società provvede a designare un Medico Competente (MC), scelto in possesso dei requisiti previsti dall'art. 38 del D.Lgs. 81/2008, valutandone l'affidabilità tecnica e l'esperienza specifica in materia di medicina del lavoro. Il MC collabora attivamente con il Datore di Lavoro e con il RSPP, partecipando alla valutazione dei rischi aziendali e visitando almeno una volta all'anno gli ambienti di lavoro, ai sensi dell'art. 25, comma 1, lett. l) del medesimo decreto.

Le visite mediche vengono effettuate secondo protocolli sanitari calibrati sulla base dei rischi specifici a cui è esposto il personale, e includono un momento informativo in cui il MC illustra al lavoratore i rischi connessi alla mansione e le misure di tutela da adottare.

Per ciascun lavoratore sottoposto a sorveglianza sanitaria, il MC redige e aggiorna una cartella sanitaria e di rischio, custodita con garanzia del segreto professionale. In caso di cessazione dell'incarico, il MC provvede a trasferire la documentazione sanitaria al medico subentrante, secondo quanto previsto dalla normativa in materia di protezione dei dati personali.

Alla cessazione del rapporto di lavoro, la Società notifica tempestivamente al MC l'evento, affinché quest'ultimo possa rilasciare al lavoratore copia della propria cartella sanitaria, fornendo le indicazioni utili alla sua conservazione.

La sorveglianza sanitaria è quindi integrata in modo strutturato nel sistema aziendale di gestione della salute e sicurezza, e rappresenta un presidio essenziale per la prevenzione dei rischi lavorativi e per il rispetto degli obblighi normativi vigenti.

1.9. Informazione e formazione dei lavoratori

La Società garantisce a tutto il personale un'adeguata informazione e formazione in materia di salute e sicurezza sul lavoro, in funzione delle mansioni e dei rischi specifici, nel rispetto delle previsioni del D.Lgs. 81/2008.

L'obiettivo è rendere i lavoratori consapevoli dei pericoli presenti, delle norme da rispettare, delle misure di prevenzione adottate e delle conseguenze legate a comportamenti non conformi.

La formazione è prevista all'assunzione, in caso di cambio mansione, introduzione di nuove attrezzature o tecnologie, o modifiche organizzative significative, ed è aggiornata periodicamente. Il RSPP propone i programmi formativi, che vengono approvati dal Datore di Lavoro.

I lavoratori ricevono istruzioni operative, schede tecniche e documentazione specifica. Sono inoltre informati sui nominativi dei referenti per la sicurezza, sul piano di emergenza e sui rischi legati alla propria attività. Il Medico Competente contribuisce all'informazione sanitaria attraverso visite, sopralluoghi e materiale dedicato.

Tutte le attività formative sono tracciate e documentate: al termine dei corsi, vengono rilasciati e archiviati gli attestati di partecipazione.

1.10. Rilevazione e registrazione degli infortuni e dei mancati incidenti

Ai fini del Sistema di Gestione della Salute e Sicurezza sul Lavoro (SGSL), è considerato infortunio ogni evento avvenuto per causa violenta in occasione di lavoro che comporti la morte, un'inabilità permanente o un'assenza dal lavoro superiore a un giorno (oltre a quello dell'evento). Rientrano in tale definizione sia gli eventi legati al rischio specifico dell'attività svolta, sia quelli derivanti dal contesto ambientale. Per quasi incidente o near miss si intende ogni evento che avrebbe potuto generare un infortunio, ma che non ha avuto conseguenze gravi grazie a fattori favorevoli o all'efficacia delle misure di protezione, inclusi gli episodi con esito lieve e nessuna interruzione dell'attività lavorativa. Tutti gli infortuni e i near miss devono essere tempestivamente segnalati, registrati e analizzati. Il lavoratore è tenuto per legge a informare immediatamente il Datore di Lavoro dell'evento (art. 52, c. 1, D.P.R. 1124/1965); il mancato rispetto di tale obbligo può comportare la perdita dell'indennità INAIL per i giorni non denunciati. L'organizzazione provvede alla comunicazione telematica all'INAIL entro 48 ore dal ricevimento del certificato medico, in caso di assenza superiore a un giorno. L'RSPP indaga l'accaduto per identificarne le cause e proporre eventuali azioni correttive o l'aggiornamento della valutazione dei rischi. I dati raccolti sono documentati e discussi anche nell'ambito della riunione periodica annuale, per favorire il miglioramento continuo e prevenire il ripetersi di eventi analoghi.

1.11. Gestione delle manutenzioni e dei controlli periodici

La Società adotta un Piano e Registro di Manutenzione per garantire l'efficienza nel tempo delle misure tecniche di prevenzione e protezione. Le attività manutentive si distinguono in:

- Manutenzione ordinaria (programmata): volta a mantenere l'efficienza e prevenire guasti, incluse piccole modifiche impiantistiche;
- Manutenzione straordinaria (non programmata): effettuata in caso di guasti o anomalie, prevalentemente a cura di ditte esterne specializzate.

La pianificazione degli interventi avviene nel rispetto delle istruzioni dei costruttori, considerando le parti critiche e i potenziali impatti sulla salute e sicurezza. Le anomalie devono essere prontamente segnalate al Datore di Lavoro e al preposto alla manutenzione, che coordina e verifica gli interventi.

Prima dell'intervento, l'attrezzatura deve essere isolata in sicurezza; prima della rimessa in funzione, il preposto verifica l'idoneità del lavoro eseguito. Tutte le attività sono tracciate nel Registro, come previsto dall'art. 71, comma 8 del D.Lgs. 81/2008, e conservate per almeno 3 anni.

Particolare attenzione è dedicata ai sistemi antincendio e di emergenza (estintori, idranti, luci di emergenza, pulsanti di sgancio, cassette di primo soccorso, ecc.), che sono oggetto di manutenzione periodica, gestita da personale interno formato o da ditte esterne abilitate.

Il Registro antincendio documenta verifiche, controlli, manutenzioni e attività formative/informative a cura del RSPP. Il Piano e Registro di Emergenza, strutturato in schede precompilate, è aggiornato costantemente e integrato con verbali e rapporti delle ditte manutentrici, al fine di assicurare tracciabilità e prontezza operativa.

1.12. Gestione dei rapporti con i fornitori e appaltatori con riferimento alle tematiche connesse alla SSL

La Società affida appalti esclusivamente a fornitori qualificati, iscritti in apposito albo, previo accertamento dell'idoneità tecnico-professionale, anche tramite autocertificazione e raccolta della documentazione prevista dall'Allegato XVII del TUS. La verifica è obbligatoria per ogni nuovo incarico, anche per appaltatori già noti, ed è estesa a eventuali subappaltatori.

Il processo di selezione coinvolge il Servizio di Prevenzione e Protezione (SPP) e prevede contratti che disciplinano ruoli, responsabilità e costi della sicurezza, inclusi gli oneri per le interferenze, che non possono

essere soggetti a ribasso. Ogni contratto individua un “Gestore del Contratto” con compiti di sorveglianza sull’esecuzione e sul rispetto delle prescrizioni.

In presenza di interferenze tra personale interno ed esterno, viene redatto il Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI), sottoscritto dalle parti e allegato al contratto. Il DUVRI è escluso nei casi di attività urgenti, meramente intellettuali, forniture, lavori brevi (≤ 2 gg) o soggetti a PSC.

Prima dell’avvio dei lavori, viene effettuato un sopralluogo congiunto tra preposti e redatto un verbale di coordinamento. Riunioni di coordinamento possono essere convocate anche in corso d’opera. Il DUVRI è uno strumento dinamico, aggiornato in caso di variazioni delle condizioni operative o nuovi rischi.

L’organizzazione fornisce sempre alle imprese esterne informazioni sui rischi presenti nei luoghi di lavoro, anche in assenza di DUVRI, nel rispetto dell’art. 26, comma 1, lett. b) del TUS.

1.13. Gestione cantieri fissi o mobili (per attività rientranti nel Titolo IV del TUS) in qualità di committente delle opere

Per i cantieri edili o di ingegneria civile con requisiti di complessità (presenza di più imprese, durata >200 uomini/giorno, rischi particolari), la Società, in qualità di committente, nomina un Responsabile dei Lavori (RL) e, tramite esso, i Coordinatori per la Progettazione (CSP) e per l’Esecuzione (CSE), scelti tra professionisti qualificati.

Il CSP redige il Piano di Sicurezza e Coordinamento (PSC) e il fascicolo dell’opera. Il CSE, in fase esecutiva, verifica il rispetto del PSC e dei POS, coordina le imprese esecutrici, promuove la cooperazione tra datori di lavoro e rappresentanti dei lavoratori per la sicurezza.

Tutta la documentazione (PSC, POS, verbali di sopralluogo e coordinamento) è raccolta e archiviata dalla Società. Riunioni di coordinamento tra RL, CSP/CSE e unità organizzative vengono organizzate periodicamente per monitorare lo stato avanzamento lavori e gli aspetti legati alla salute e sicurezza sul lavoro (SSL).

Le non conformità (inosservanza di norme, procedure, uso improprio della documentazione, ecc.) possono essere segnalate da qualsiasi unità organizzativa. Ogni scostamento rilevato deve essere comunicato al Responsabile e al SPP.

Il RSPP, insieme al responsabile dell’unità coinvolta, valuta l’evento e può aprire un rapporto di non conformità, che descrive l’evento e definisce le azioni correttive da attuare. Ogni rapporto è numerato, monitorato e – se rilevante – discusso in sede di riunione periodica con il Datore di Lavoro.

1.14. Gestione delle verifiche circa il rispetto delle procedure operative e istruzioni di lavoro in materia di SSL

La Società effettua attività di monitoraggio continuo e periodico delle misure preventive e protettive adottate in materia di SSL, sulla base delle policy aziendali, delle procedure interne e delle normative vigenti.

Il monitoraggio è svolto:

- Continuamente, da parte dei soggetti designati;
- Periodicamente, mediante check-list strutturate.

I responsabili e preposti, formalmente incaricati e presenti nelle aree operative, verificano il rispetto delle procedure e istruzioni di sicurezza da parte dei lavoratori. In caso di anomalie, intervengono direttamente nei limiti delle loro competenze o segnalano le criticità al Servizio Prevenzione e Protezione (SPP).

Le responsabilità degli incaricati includono il controllo su:

- Uso corretto dei DPI;
- Rispetto delle limitazioni di accesso a zone pericolose;
- Adozione delle misure in caso di emergenza e di pericolo imminente;
- Divieto di ripresa dell'attività in condizioni di rischio grave;
- Rispetto della segnaletica di sicurezza e del divieto di fumo.

Le criticità rilevate sono segnalate al Datore di Lavoro e discusse durante la riunione periodica sulla SSL.

Le verifiche di sistema o quelle che richiedono competenze specialistiche possono essere affidate ad auditor esterni indipendenti e qualificati.

1.15. Flussi informativi da e verso l' OdV

Il corretto funzionamento del Modello 231 adottato dalla Società richiede che l'Organismo di Vigilanza riceva e gestisca informazioni rilevanti sul piano della conformità normativa e del rispetto delle procedure interne, nonché che possa a sua volta fornire aggiornamenti e indicazioni utili agli organi aziendali. Per questo motivo, è stato definito un sistema strutturato di flussi informativi da e verso l'OdV, il cui scopo è quello di garantire il monitoraggio costante dell'efficacia del Modello e di favorire un dialogo continuo tra l'OdV e le diverse funzioni aziendali coinvolte.

Devono essere portate all'attenzione dell'OdV tutte le informazioni che possano avere rilievo rispetto al rischio di commissione dei reati previsti dal Decreto, o che segnalino comportamenti in contrasto con il

Codice Etico, il Modello stesso o altre disposizioni interne rilevanti. Tra queste, rientrano ad esempio le segnalazioni di eventuali violazioni, gli esiti di audit o ispezioni, le contestazioni disciplinari legate a condotte non conformi, le comunicazioni con le autorità di controllo, le variazioni organizzative che impattano sui processi sensibili, o ancora eventi come infortuni.

Le funzioni aziendali competenti trasmettono tali informazioni all'Organismo secondo modalità idonee a garantire la tracciabilità e la riservatezza dei contenuti. I flussi possono avvenire sia in forma periodica – secondo una cadenza predefinita, generalmente semestrale – sia ogniqualvolta emergano situazioni che richiedano un intervento immediato. Il tutto avviene anche mediante un canale dedicato di comunicazione, nel rispetto delle regole interne e della normativa sulla protezione dei dati personali.

L'Organismo di Vigilanza, da parte sua, relaziona periodicamente agli organi societari – in particolare al CdA in merito alle attività svolte, alle eventuali criticità rilevate e alle proposte di adeguamento o miglioramento del Modello. In presenza di fatti di particolare rilevanza, l'OdV informa tempestivamente la governance aziendale, affinché possano essere adottati i provvedimenti opportuni.

In tale contesto, l'OdV è chiamato a effettuare controlli mirati su tutti i punti richiamati nella presente Parte Speciale – corrispondenti agli elementi previsti dall'art. 30 – al fine di accertare l'effettiva attuazione.

L'insieme di questi flussi rappresenta un pilastro fondamentale del sistema di controllo preventivo previsto dal Decreto 231, contribuendo alla sua efficacia e alla diffusione della cultura della legalità all'interno della Società.

2. Reati nei rapporti con la Pubblica Amministrazione

La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo è dedicata ai reati che possono configurarsi nei rapporti tra Compagnia Siderurgica S.p.A. e la Pubblica Amministrazione, come disciplinati dal d.lgs. 8 giugno 2001 n. 231.

L'inclusione di tali fattispecie deriva dal riconoscimento che, nel contesto delle attività aziendali, la Società intrattiene rapporti continuativi con enti pubblici e autorità amministrative in diversi ambiti: dalla sicurezza sul lavoro alla tutela ambientale, dalla gestione delle autorizzazioni per gli impianti produttivi alle verifiche tecniche e fiscali, fino ai rapporti con gli enti locali e le autorità di controllo.

Le ipotesi di reato rilevanti sono in particolare quelle previste:

- dall'art. 24, che contempla l'indebita percezione di erogazioni pubbliche, la truffa ai danni dello Stato o di altri enti pubblici, la frode informatica e la frode nelle pubbliche forniture;

- dall'art. 25, che comprende i delitti di peculato, concussione, corruzione, abuso d'ufficio e induzione indebita a dare o promettere utilità;
- dall'art. 25-decies, che disciplina l'induzione a non rendere dichiarazioni o a renderle mendaci all'autorità giudiziaria.

La rilevanza di tali reati si collega al fatto che la Società, pur operando in un settore prevalentemente industriale e commerciale, è soggetta a un intenso rapporto con la Pubblica Amministrazione, necessario per il corretto esercizio delle proprie attività produttive, la gestione delle certificazioni di qualità, ambiente e sicurezza, nonché per l'ottenimento di autorizzazioni e agevolazioni economiche.

Compagnia Siderurgica S.p.A., consapevole dei rischi potenziali derivanti da tali interazioni, si impegna a garantire che ogni rapporto con soggetti pubblici sia improntato ai principi di legalità, correttezza, trasparenza e tracciabilità, prevenendo qualunque comportamento che possa anche solo astrattamente integrare una condotta illecita.

La presente Parte Speciale non si limita a elencare le fattispecie di reato, ma ha la funzione di definire le regole comportamentali e i presidi organizzativi che la Società adotta per prevenire ogni possibile violazione, delineando un sistema di controllo effettivo e coerente con il proprio assetto organizzativo e gestionale.

2.1 Attività sensibili

Nel contesto operativo di Compagnia Siderurgica S.p.A., sono considerate sensibili ai fini della possibile integrazione dei reati nei rapporti con la Pubblica Amministrazione tutte le attività che, per natura o finalità, comportano interazioni dirette o indirette con soggetti pubblici, o che implicino la formazione e la trasmissione di atti o dichiarazioni aventi rilievo per la sfera pubblica.

Tali attività comprendono, in particolare:

- la gestione dei rapporti istituzionali con enti pubblici nazionali e locali, comprese le autorità amministrative e gli organi di vigilanza in materia di ambiente, sicurezza sul lavoro, salute, prevenzione incendi, fiscalità, edilizia e produzione industriale;
- la richiesta, il rinnovo e la gestione di autorizzazioni, licenze, permessi, certificazioni o iscrizioni in albi e registri necessari allo svolgimento delle attività aziendali, comprese le pratiche relative agli impianti, alle emissioni in atmosfera, ai rifiuti e agli scarichi idrici;
- la partecipazione a procedure ad evidenza pubblica o a bandi per l'ottenimento di contributi, finanziamenti, agevolazioni o incentivi, anche in materia di innovazione tecnologica, sostenibilità ambientale ed efficientamento energetico;

- la predisposizione, sottoscrizione e trasmissione di dichiarazioni, relazioni tecniche, comunicazioni o attestazioni dirette a enti pubblici, autorità di controllo, organismi certificatori e uffici ispettivi, nonché la gestione della relativa documentazione;
- la gestione dei rapporti con l'amministrazione finanziaria, le dogane e le autorità tributarie, compresa la redazione e la trasmissione di atti aventi rilievo fiscale o doganale;
- la rappresentanza della Società in occasione di ispezioni, verifiche o controlli da parte di autorità pubbliche (ASL, ARPA, INAIL, Vigili del Fuoco, Ispettorato del Lavoro, enti locali o forze dell'ordine), comprese le attività di accompagnamento e di risposta formale a verbali o prescrizioni;
- la gestione dei rapporti con la magistratura o con le autorità inquirenti, nel caso di procedimenti, accertamenti o ispezioni che coinvolgano la Società o suoi esponenti;
- la gestione di rapporti con soggetti privati che operano per conto o nell'interesse della Pubblica Amministrazione, come società di servizi pubblici o enti a partecipazione pubblica, nell'ambito di attività tecniche, logistiche o amministrative;
- la gestione dei rapporti con organismi di certificazione e accreditamento per i sistemi di qualità, ambiente e sicurezza adottati dalla Società, nonché con eventuali enti notificati ai fini del rilascio di certificazioni di prodotto o processo.

Le attività sopra elencate possono essere svolte da amministratori, dirigenti, personale dipendente o collaboratori esterni, ciascuno nei limiti delle proprie funzioni e deleghe operative. In ogni caso, la Società richiede che tali attività siano sempre improntate a legalità, trasparenza, tracciabilità e correttezza, e che siano documentate e verificabili secondo quanto previsto dalle procedure interne e dai sistemi di gestione aziendale.

È vietata qualunque attività non autorizzata o non formalmente delegata nei rapporti con rappresentanti o funzionari pubblici, anche qualora posta in essere con finalità collaborative o di semplificazione procedurale.

2.2 Principi di comportamento

Nello svolgimento delle attività che comportano rapporti, diretti o indiretti, con la Pubblica Amministrazione, Compagnia Siderurgica S.p.A. richiede che amministratori, dipendenti, collaboratori, consulenti e chiunque operi in nome o per conto della Società si conformi ai principi di legalità, integrità, trasparenza, tracciabilità e correttezza, nel pieno rispetto del Modello 231, del Codice Etico e delle procedure aziendali vigenti.

La Società adotta un approccio di tolleranza zero verso qualunque forma di comportamento che possa, anche solo potenzialmente, integrare ipotesi di corruzione, concussione, abuso d'ufficio, frode o indebita percezione di vantaggi economici da parte di enti pubblici.

A tal fine, valgono i seguenti principi generali di condotta:

- è vietata qualsiasi promessa, offerta, corresponsione o accettazione, diretta o indiretta, di denaro, beni o altre utilità a favore o da parte di pubblici ufficiali, incaricati di pubblico servizio o soggetti ad essi assimilati, anche se posta in essere tramite intermediari, consulenti o terzi;
- è vietata ogni condotta che possa configurare, anche in via tentata, ipotesi di indebita percezione di contributi o agevolazioni pubbliche, truffa ai danni dello Stato o di altri enti pubblici, frode informatica o frode nelle pubbliche forniture;
- le relazioni con la Pubblica Amministrazione devono essere sempre gestite da soggetti formalmente incaricati o delegati, secondo le procedure interne e i poteri conferiti, garantendo la completa tracciabilità di ogni operazione e comunicazione;
- in occasione di ispezioni, controlli o verifiche, i soggetti coinvolti devono prestare la massima collaborazione, fornendo alle autorità competenti informazioni veritiere, complete e tempestive, evitando qualunque atteggiamento reticente, ostruzionistico o fuorviante;
- è vietata ogni forma di influenza indebita, pressione o promessa di vantaggi volta a condizionare decisioni o comportamenti di pubblici funzionari o incaricati di pubblico servizio;
- la documentazione destinata a enti pubblici deve essere redatta con accuratezza e coerenza rispetto ai dati aziendali, sottoposta ai necessari controlli interni e conservata secondo i criteri stabiliti dai sistemi di gestione aziendale (in particolare ISO 9001, ISO 14001 e ISO 45001);
- non sono ammesse iniziative personali non autorizzate nei rapporti con la Pubblica Amministrazione, anche qualora motivate da finalità di collaborazione o urgenza operativa;
- la scelta e la gestione dei consulenti esterni incaricati di interagire con enti pubblici devono avvenire nel rispetto dei criteri di competenza, indipendenza e correttezza, mediante contratti scritti che specifichino chiaramente l'ambito dell'incarico, i limiti operativi e gli obblighi di conformità al Modello 231 e al Codice Etico;

- è vietata la corresponsione di compensi sproporzionati o non giustificati alla natura dell'incarico o alle tariffe di mercato, soprattutto nei casi in cui tali consulenti abbiano rapporti o contatti con funzionari pubblici;
- ogni rapporto di collaborazione con ex dipendenti o ex funzionari pubblici deve essere valutato con particolare attenzione, al fine di prevenire conflitti di interesse o vantaggi indebiti.

L'osservanza dei suddetti principi costituisce parte integrante degli obblighi contrattuali e disciplinari di chiunque operi per conto della Società. Il rispetto di tali regole si coordina con quanto previsto dal Codice Etico e dai sistemi di gestione certificati adottati da Compagnia Siderurgica S.p.A., i quali assicurano la tracciabilità dei processi e la conservazione della documentazione in modo conforme alle norme vigenti.

2.3 Nomina delle funzioni competenti e formazione

Compagnia Siderurgica S.p.A. individua, all'interno della propria organizzazione, le funzioni e le figure competenti alla gestione dei rapporti con la Pubblica Amministrazione, in modo da garantire chiarezza di ruoli, separazione delle responsabilità e tracciabilità delle attività.

Le relazioni con enti pubblici, autorità e organi di controllo devono essere gestite esclusivamente da personale formalmente autorizzato o delegato, nel rispetto delle competenze e dei poteri conferiti. Le deleghe e le procure, ove previste, devono essere:

- conferite per iscritto, con indicazione puntuale dell'ambito operativo, dei limiti di spesa e delle eventuali soglie di autonomia decisionale;
- coerenti con la posizione ricoperta, le competenze tecniche e il livello di responsabilità del soggetto delegato;
- aggiornate tempestivamente in caso di modifiche organizzative o sostituzioni di personale;
- custodite presso la Direzione e messe a disposizione dell'Organismo di Vigilanza per eventuali verifiche.

L'eventuale partecipazione a procedure pubbliche, ispezioni o rapporti istituzionali deve essere sempre preventivamente comunicata alla Direzione, la quale ne autorizza la gestione e, se necessario, coordina l'intervento di consulenti tecnici o legali. In caso di procedimenti giudiziari o amministrativi che coinvolgano la Società o suoi esponenti, la rappresentanza legale e la difesa vengono gestite dalla Direzione, garantendo l'assenza di conflitti di interesse e la piena autonomia di giudizio.

La Società riconosce inoltre la formazione come elemento essenziale per la prevenzione dei reati e la diffusione di una cultura aziendale orientata alla legalità e alla trasparenza. A tale scopo, Compagnia Siderurgica S.p.A. promuove programmi formativi periodici, calibrati in funzione del ruolo e del grado di esposizione al rischio, aventi ad oggetto:

- il d.lgs. 231/2001, con particolare riferimento ai reati nei rapporti con la Pubblica Amministrazione;
- il contenuto del Modello di Organizzazione, Gestione e Controllo e del Codice Etico;
- le procedure operative interne relative alla gestione dei rapporti con enti e autorità pubbliche;
- le regole di comportamento da tenere in occasione di ispezioni o verifiche da parte di enti pubblici.

L'Organismo di Vigilanza verifica periodicamente l'efficacia e l'adeguatezza dei programmi formativi, anche attraverso l'esame della documentazione e l'eventuale proposta di interventi correttivi o di approfondimenti tematici.

2.4 Flussi informativi da e verso l'Organismo di Vigilanza

Per assicurare l'efficace attuazione e il costante aggiornamento della presente Parte Speciale, Compagnia Siderurgica S.p.A. garantisce un sistema di flussi informativi continuativi, tempestivi e verificabili tra le funzioni aziendali coinvolte e l'Organismo di Vigilanza (OdV).

Le funzioni operative e amministrative sono tenute a comunicare all'OdV, senza ritardo e con adeguata documentazione di supporto, tutte le informazioni e le evidenze che possano rilevare ai fini della prevenzione dei reati nei rapporti con la Pubblica Amministrazione. In particolare, devono essere trasmesse:

- le istanze, domande o comunicazioni presentate a enti pubblici, autorità o amministrazioni per l'ottenimento di autorizzazioni, licenze, concessioni, certificazioni o agevolazioni economiche;
- la partecipazione a gare, bandi o procedure ad evidenza pubblica, indicando il ruolo assunto dalla Società e le principali condizioni contrattuali o economiche;
- l'avvio di ispezioni, sopralluoghi, verifiche o controlli da parte di enti pubblici (ASL, ARPA, INAIL, Ispettorato del Lavoro, Vigili del Fuoco, Agenzia delle Entrate, Guardia di Finanza, enti locali o altre autorità), nonché gli esiti, i verbali o le eventuali prescrizioni ricevute;
- le interlocuzioni con la magistratura o con le autorità inquirenti, qualora riguardino procedimenti amministrativi o penali che coinvolgano la Società o suoi rappresentanti;

- i rapporti o contatti con ex funzionari pubblici o con soggetti che possano trovarsi in potenziale conflitto di interessi;
- le segnalazioni, anomalie, irregolarità o criticità riscontrate nella gestione dei rapporti con la Pubblica Amministrazione, anche se prive di conseguenze disciplinari o penali.

Le comunicazioni all'Organismo di Vigilanza devono avvenire per iscritto, anche in formato elettronico, e contenere informazioni complete, chiare e verificabili. L'OdV valuta la rilevanza delle segnalazioni, richiede eventuali chiarimenti, convoca le funzioni interessate e, se necessario, propone misure correttive o interventi di miglioramento.

L'Organismo di Vigilanza ha facoltà di accedere in ogni momento alla documentazione relativa ai rapporti con la Pubblica Amministrazione, ai fascicoli autorizzativi, ai verbali di ispezione, ai contratti con consulenti e alle evidenze delle comunicazioni trasmesse. La mancata, tardiva o incompleta trasmissione delle informazioni previste è considerata violazione delle disposizioni del Modello 231 e può essere oggetto di valutazione disciplinare e organizzativa.

I flussi informativi verso l'OdV contribuiscono al monitoraggio costante dell'efficacia del Modello e alla verifica della congruità dei presidi di controllo adottati, garantendo una supervisione autonoma e indipendente delle relazioni con la Pubblica Amministrazione e delle attività a rischio correlate.

2.5. Protocolli

2.5.1. Protocollo per la gestione di adempimenti verso Enti Pubblici in materia di sicurezza e igiene del lavoro (D.Lgs. 81/2008)

Spetta esclusivamente al Datore di Lavoro, autonomamente o su proposta del Responsabile del Servizio di Prevenzione e Protezione, gestire ogni adempimento verso enti pubblici in materia di salute, sicurezza e igiene sul lavoro, nel pieno rispetto dei principi stabiliti dal Codice Etico della Società. Ciò comprende, a titolo esemplificativo, l'ottenimento o il rinnovo del certificato di prevenzione incendi, nonché ogni altra pratica o comunicazione verso le autorità competenti.

Durante le riunioni periodiche di coordinamento, il Responsabile del Servizio di Prevenzione e Protezione sottopone eventuali questioni di rilievo all'attenzione dei partecipanti, affinché vengano esaminate, verbalizzate e approvate con la relativa attribuzione di compiti, responsabilità e tempi di esecuzione. Tali decisioni possono essere formalizzate anche mediante comunicazioni via e-mail.

Ogni altro soggetto, anche se appartenente all'organizzazione per la gestione della salute e sicurezza, deve astenersi da contatti diretti con la Pubblica Amministrazione se non nei limiti di specifica delega rilasciata dal Datore di Lavoro. Il soggetto delegato cura l'archiviazione della documentazione rilevante a supporto delle attività operative e amministrative propedeutiche all'adempimento verso gli enti pubblici competenti.

2.5.2. Protocollo per la gestione di adempimenti connessi all'assunzione di personale appartenente a categorie protette o soggetto ad agevolazioni pubbliche

Spetta al Responsabile Risorse Umane gestire ogni aspetto relativo alla selezione e all'assunzione di personale la cui assunzione possa comportare contatti o adempimenti nei confronti della Pubblica Amministrazione, come nel caso delle quote di riserva previste dalla normativa sulle categorie protette o di forme di assunzione agevolata.

Il Responsabile Risorse Umane cura la completa archiviazione della documentazione a supporto delle attività svolte e riferisce periodicamente al Consiglio di Amministrazione o a un Amministratore Delegato con delega in materia di gestione del personale, i quali autorizzano formalmente le relative assunzioni o le pratiche di agevolazione.

2.5.3. Protocollo per la gestione di verifiche, controlli e accertamenti da parte della Pubblica Amministrazione

In caso di verifiche o ispezioni da parte di enti pubblici o autorità competenti (quali ASL, ARPA, INAIL, Ispettorato del Lavoro, Agenzia delle Entrate, Guardia di Finanza o altri), è fatto obbligo:

- ai soggetti incaricati della gestione dell'ispezione di collaborare con la massima trasparenza, fornendo informazioni veritiere, aggiornate e coerenti con la documentazione aziendale;
- di far partecipare alle verifiche giudiziarie, tributarie o amministrative solo soggetti espressamente delegati o professionisti di fiducia della Società, in grado di interagire con cognizione di causa con i funzionari della Pubblica Amministrazione.

I verbali redatti dalle autorità ispettive devono essere diligentemente conservati dalla funzione aziendale che ha seguito la verifica.

In ogni caso di visita ispettiva, deve essere immediatamente informato l'Amministratore Delegato competente per materia, unico soggetto abilitato ad autorizzare la presenza di altri incaricati o consulenti durante l'ispezione. Al termine della verifica, l'Amministratore Delegato analizza e sottoscrive il verbale redatto dall'organo ispettivo, riservandosi di sottoporre la questione al Consiglio di Amministrazione qualora emergano criticità o motivi ostativi alla firma.

Copia delle richieste di informazioni e dei verbali finali di ispezione può essere trasmessa all'Organismo di Vigilanza per gli opportuni riscontri.

2.5.4. Protocollo per l'acquisizione e la gestione di contributi, sovvenzioni e finanziamenti pubblici

Ogni opportunità di finanziamento, contributo o agevolazione concessa da soggetti pubblici deve essere sottoposta al Responsabile di Ufficio competente, che ne valuta la pertinenza e la trasmette all'Amministratore Delegato o al Consiglio di Amministrazione per le determinazioni del caso.

Solo tali organi sono abilitati a deliberare l'adesione a bandi o iniziative pubbliche, nonché a individuare il Responsabile di Procedimento (RPROC), figura eventualmente nominata per seguire l'iter amministrativo connesso alla richiesta.

Il Responsabile di Procedimento redige la documentazione necessaria, predispone la domanda di finanziamento e la sottopone alla verifica e autorizzazione dell'Amministratore Delegato competente, che può, in casi di particolare rilievo, coinvolgere la Direzione Generale o il Consiglio di Amministrazione.

Il Responsabile di Procedimento, o in sua assenza il Responsabile di Ufficio competente, cura l'archiviazione della documentazione a supporto delle attività propedeutiche all'acquisizione, gestione e rendicontazione di contributi o finanziamenti pubblici.

2.5.5. Protocollo per la gestione di omaggi e liberalità nei confronti di funzionari pubblici

È severamente vietato:

- effettuare elargizioni in denaro o altre utilità a funzionari pubblici, italiani o stranieri;
- distribuire omaggi o regali al di fuori delle prassi aziendali o che possano, anche solo potenzialmente, influenzare l'indipendenza di giudizio del destinatario o ottenere vantaggi indebiti per la Società.

Sono consentiti unicamente omaggi di modico valore, conformi alle consuetudini aziendali e alle finalità di rappresentanza, promozione dell'immagine o partecipazione a iniziative benefiche o culturali.

Ogni forma di omaggio o liberalità nei confronti di soggetti collegati, anche indirettamente, alla Pubblica Amministrazione deve essere preventivamente autorizzata da un Amministratore Delegato o da un componente della Direzione Generale.

2.5.6. Protocollo per la partecipazione a gare, appalti o altre procedure di aggiudicazione con la Pubblica Amministrazione

Ogni proposta di partecipazione a gare o procedure pubbliche, ricevuta o individuata come di potenziale interesse, deve essere trasmessa al Responsabile di Ufficio Commerciale competente, che valuta la coerenza con la strategia aziendale, il carico di lavoro, la capacità produttiva e la convenienza economica.

Il Responsabile di Ufficio Commerciale cura la raccolta della documentazione di gara e l'analisi di fattibilità tecnica ed economica, verificando la capacità dell'impresa di eseguire i lavori nei tempi e secondo le modalità previste dai bandi.

Se la partecipazione viene ritenuta opportuna, il Responsabile di Ufficio predispone la documentazione tecnica, legale e amministrativa necessaria, affidandone la redazione ai professionisti interni o esterni designati.

L'intero fascicolo viene quindi sottoposto all'approvazione finale di un Amministratore Delegato, unico soggetto autorizzato a convalidare formalmente la partecipazione prima della presentazione della domanda.

Durante l'intera procedura, i rapporti con la Pubblica Amministrazione devono avvenire nel rispetto dei principi stabiliti nel Codice Etico e nelle procedure interne della Società.

3. Razzismo e xenofobia

Compagnia Siderurgica S.p.A. fonda la propria identità aziendale sui principi di rispetto della persona, integrità, collaborazione e uguaglianza. La Società riconosce che il valore della diversità rappresenta una risorsa essenziale per lo sviluppo di un ambiente di lavoro equilibrato e produttivo, e considera inaccettabile qualsiasi forma di discriminazione, diretta o indiretta, basata sull'origine etnica, la nazionalità, la lingua, la cultura o qualsiasi altra caratteristica personale o sociale.

Il razzismo e la xenofobia, anche quando si manifestano in forme sottili o non intenzionali, compromettono non solo la dignità individuale ma anche la coesione interna, la credibilità e la reputazione della Società nel suo complesso. Per tali ragioni, Compagnia Siderurgica S.p.A. assume un impegno concreto e costante nella prevenzione e nel contrasto di ogni condotta discriminatoria, integrando tale impegno nel proprio sistema di governance e nei principi fondamentali del Modello di Organizzazione, Gestione e Controllo.

L'attenzione al rispetto della dignità umana non si limita al mero adempimento normativo, ma si traduce in un orientamento etico che guida le decisioni aziendali, le relazioni interne ed esterne e i comportamenti quotidiani. La Società promuove una cultura del rispetto reciproco, della valorizzazione delle differenze e

della pari opportunità, sia nei rapporti interni sia nelle relazioni commerciali, consapevole che solo un ambiente inclusivo favorisce la sicurezza, l'efficienza e la crescita collettiva.

La presente Parte Speciale del Modello 231 assume pertanto il ruolo di strumento operativo volto a prevenire, monitorare e contrastare in modo sistematico ogni forma di razzismo o xenofobia, integrando la prospettiva della parità di trattamento nei processi gestionali, produttivi e relazionali dell'azienda.

3.1 Attività a rischio sensibile

Nell'ambito delle proprie attività, Compagnia Siderurgica S.p.A. riconosce che possono emergere, anche in modo indiretto o non intenzionale, comportamenti suscettibili di essere ricondotti a fenomeni discriminatori. Le aree maggiormente esposte sono quelle in cui prevalgono relazioni umane o scelte discrezionali, in particolare:

- la gestione delle risorse umane, che comprende le fasi di selezione, assunzione, inserimento, formazione, valutazione e cessazione del rapporto di lavoro;
- i rapporti interni tra i lavoratori e con i superiori gerarchici, dove linguaggi o atteggiamenti non rispettosi possono generare forme di disagio o discriminazione;
- i rapporti con fornitori, clienti e partner commerciali, nei quali comportamenti o comunicazioni non coerenti con i principi aziendali possono compromettere la reputazione della Società;
- la comunicazione aziendale, interna ed esterna, che deve sempre riflettere valori di rispetto e inclusione, evitando contenuti, immagini o espressioni suscettibili di interpretazioni discriminatorie;
- i rapporti con collaboratori esterni o con personale proveniente da Paesi diversi, che richiedono particolare attenzione per garantire equilibrio, correttezza e parità di trattamento.

Tali aree devono essere gestite con vigilanza costante da parte dei responsabili di funzione e, più in generale, di tutti coloro che svolgono ruoli di coordinamento, affinché ogni decisione e ogni interazione siano improntate a criteri di obiettività, trasparenza e rispetto della persona.

3.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. riconosce il valore della diversità come elemento di crescita culturale e professionale e fonda la propria azione sui principi di uguaglianza, inclusione, equità e rispetto della dignità umana.

Nessun comportamento, decisione o prassi aziendale può tradursi, anche solo indirettamente, in forme di razzismo o xenofobia.

Per dare concreta attuazione a tali principi, la Società adotta una serie di presidi organizzativi e gestionali, tra i quali:

- l'applicazione, nei processi di selezione e gestione del personale, di criteri oggettivi, verificabili e documentabili, fondati esclusivamente su competenze, esperienze e requisiti professionali;
- la promozione di un ambiente di lavoro rispettoso e inclusivo, mediante attività di sensibilizzazione e formazione rivolte a dipendenti, responsabili e collaboratori, con l'obiettivo di accrescere la consapevolezza sui temi della diversità e della non discriminazione;
- l'inserimento nei contratti e nei rapporti commerciali di clausole che richiamano il rispetto dei principi di parità, legalità e dignità della persona;
- il controllo della comunicazione aziendale affinché ogni contenuto, messaggio o immagine diffuso rifletta i valori di rispetto e inclusione che caratterizzano l'identità di Compagnia Siderurgica S.p.A.;
- la previsione di misure disciplinari e organizzative adeguate per contrastare eventuali condotte non conformi, con obbligo di segnalazione all'Organismo di Vigilanza e ai responsabili gerarchici competenti.

Il sistema di prevenzione è fondato su una responsabilità condivisa: ogni dipendente, collaboratore o consulente è tenuto ad agire nel rispetto dei principi sopra enunciati e a contribuire attivamente alla costruzione di un ambiente di lavoro improntato alla fiducia e alla correttezza. La vigilanza e il controllo sono assicurati dai responsabili di funzione e, in ultima istanza, dall'Organismo di Vigilanza, che svolge un ruolo di supervisione indipendente e continuativa.

3.3 Flussi informativi da e verso l'Organismo di Vigilanza

Il corretto funzionamento del sistema di prevenzione dei reati di razzismo e xenofobia si basa su un flusso informativo costante tra le funzioni aziendali e l'Organismo di Vigilanza. Dipendenti, collaboratori, consulenti e partner possono segnalare comportamenti, situazioni o comunicazioni che appaiano in contrasto con i principi di uguaglianza e inclusione, utilizzando i canali riservati e protetti previsti dal Modello 231 e dal sistema di whistleblowing aziendale.

Le segnalazioni devono essere circostanziate, fondate su elementi concreti e trasmesse con tempestività, al fine di consentire all'Organismo di Vigilanza di svolgere un'analisi approfondita e, se necessario, proporre misure correttive. L'Organismo di Vigilanza, a sua volta, riferisce periodicamente al Consiglio di Amministrazione circa le attività di monitoraggio svolte, le segnalazioni ricevute e gli interventi adottati.

È garantita in ogni caso la tutela della riservatezza dell'identità del segnalante e il divieto assoluto di ritorsioni o discriminazioni nei confronti di chi effettua una segnalazione in buona fede, in conformità alla normativa vigente.

Tale meccanismo rafforza il clima di fiducia e trasparenza all'interno dell'organizzazione, rendendo la collaborazione di tutti parte integrante del sistema di prevenzione e tutela della Società.

4. Delitti informatici e trattamento illecito di dati

La progressiva digitalizzazione dei processi produttivi e gestionali espone Compagnia Siderurgica S.p.A. a rischi connessi all'utilizzo delle tecnologie informatiche e alla gestione delle informazioni, incluse quelle di natura personale. La Società è consapevole che la commissione di reati informatici o di condotte illecite nel trattamento dei dati, anche se poste in essere in modo colposo o non intenzionale, può comportare conseguenze rilevanti sotto il profilo giuridico, economico e reputazionale.

Per tale motivo, Compagnia Siderurgica S.p.A. ha adottato un sistema di gestione conforme al Regolamento (UE) 2016/679 (GDPR) e alla normativa nazionale in materia di protezione dei dati personali, integrando presidi tecnici, organizzativi e procedurali finalizzati a garantire la sicurezza, la riservatezza e l'integrità dei sistemi informativi e dei dati trattati.

L'uso corretto degli strumenti informatici e la tutela dei dati aziendali e personali costituiscono non solo un dovere giuridico, ma un valore etico fondamentale per la Società, in coerenza con i principi del Codice Etico e con l'impegno verso la tutela dei diritti e della dignità delle persone. Chiunque operi per conto della Società è tenuto a comportarsi con la massima diligenza e prudenza nell'utilizzo delle risorse informatiche e nella gestione delle informazioni, evitando qualsiasi azione che possa comprometterne la sicurezza o l'affidabilità.

4.1 Attività a rischio sensibile

Le attività aziendali che implicano l'uso di strumenti informatici e il trattamento di dati aziendali o personali sono intrinsecamente esposte a rischi specifici. Nell'ambito dell'organizzazione di Compagnia Siderurgica S.p.A., assumono particolare rilievo:

- l'accesso ai sistemi gestionali e ai database aziendali, inclusa la gestione delle credenziali di autenticazione;
- l'utilizzo della posta elettronica, della rete internet e degli strumenti di comunicazione digitale;
- le operazioni di archiviazione, trasferimento e conservazione dei dati informatici;
- le attività di manutenzione, aggiornamento o installazione di software e dispositivi informatici;

- la gestione di dati personali riferiti a dipendenti, collaboratori, clienti, fornitori o altri soggetti esterni;
- la gestione di backup, log e sistemi di monitoraggio della rete aziendale.

In tali ambiti, eventuali carenze di controllo o comportamenti non conformi alle regole interne possono favorire accessi non autorizzati, manomissioni, perdite di dati, violazioni della riservatezza o altri eventi idonei a integrare fattispecie di reato ai sensi del D.Lgs. 231/2001.

4.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. si impegna a garantire un utilizzo responsabile, sicuro e conforme alla legge di tutte le risorse informatiche e digitali, attraverso un sistema di regole e controlli integrati. Ogni soggetto che utilizza gli strumenti informatici aziendali deve attenersi ai seguenti principi:

- usare le risorse informatiche esclusivamente per finalità lavorative e nel rispetto delle procedure aziendali;
- non installare o utilizzare software non autorizzati o non verificati, né introdurre programmi che possano compromettere la sicurezza o l'efficienza dei sistemi;
- non accedere, né tentare di accedere, a sistemi informativi di terzi o a dati riservati senza legittima autorizzazione;
- non diffondere, condividere o cedere a terzi le credenziali di accesso personali o aziendali;
- non utilizzare strumenti o programmi destinati a eludere i sistemi di protezione, alterare dati o intercettare comunicazioni;
- adottare una condotta diligente nella gestione della posta elettronica, evitando l'apertura di allegati o link sospetti e la trasmissione di dati sensibili a destinatari non autorizzati;
- segnalare tempestivamente al Responsabile dell'Ufficio IT o al Responsabile di Funzione qualsiasi anomalia, sospetto di intrusione o evento di sicurezza informatica.

La Società garantisce l'applicazione di misure tecniche e organizzative adeguate al rischio, quali:

- sistemi di autenticazione e autorizzazione degli utenti;
- politiche di password e di aggiornamento periodico;
- firewall, antivirus, sistemi di cifratura e backup regolari;

- controlli sul traffico di rete e monitoraggio degli accessi, effettuati nel rispetto della riservatezza dei lavoratori;
- aggiornamento costante del sistema di gestione privacy e delle misure di sicurezza informatica;
- formazione periodica del personale sui rischi informatici e sulle buone pratiche di sicurezza digitale.

Tutti i collaboratori, dipendenti e consulenti sono responsabili del corretto uso delle risorse informatiche e del rispetto delle regole sopra indicate. La violazione delle procedure può comportare l'applicazione di sanzioni disciplinari e, nei casi più gravi, la segnalazione all'Organismo di Vigilanza o alle autorità competenti.

4.3 Flussi informativi da e verso l'Organismo di Vigilanza

Il corretto presidio dei rischi informatici e la prevenzione del trattamento illecito dei dati richiedono un flusso informativo continuo e strutturato tra le funzioni competenti e l'Organismo di Vigilanza.

Il Responsabile dell'Ufficio IT e il Responsabile della Protezione dei Dati (DPO) – ove nominato – trasmettono periodicamente all'Organismo di Vigilanza informazioni relative:

- agli aggiornamenti dei sistemi informativi e di sicurezza;
- alle segnalazioni di eventi anomali o incidenti informatici;
- alle verifiche eseguite sul rispetto delle policy aziendali in materia di uso degli strumenti informatici;
- alle eventuali violazioni dei dati personali (data breach) e alle relative misure correttive adottate.

L'Organismo di Vigilanza valuta le informazioni ricevute, monitora l'efficacia dei presidi di prevenzione e riferisce periodicamente al Consiglio di Amministrazione in merito alle attività svolte e ai rischi residui individuati.

Ogni dipendente o collaboratore può inoltre segnalare, tramite i canali dedicati e riservati, eventuali condotte anomale o sospette, nel rispetto della riservatezza e del divieto di ritorsioni previsto dal sistema di whistleblowing aziendale.

4.4. Protocolli operativi

Tutti i soggetti che operano per conto di Compagnia Siderurgica S.p.A. devono attenersi ai seguenti principi:

- rispetto delle policy di sicurezza informatica e delle procedure interne per l'utilizzo degli strumenti aziendali;
- conoscenza e osservanza del Manuale Privacy e del Modello di Gestione della Sicurezza Informatica adottati dalla Società;

- divieto di installare software estranei alle finalità aziendali o privi di licenza;
- divieto di utilizzare programmi idonei a compromettere la sicurezza, rallentare o danneggiare i sistemi informativi aziendali;
- divieto di accedere o tentare di accedere a sistemi informatici esterni in modo illecito;
- divieto di acquisire, detenere o diffondere programmi, codici o strumenti atti al danneggiamento informatico o alla violazione di sistemi di sicurezza;
- divieto di fornire o condividere con soggetti interni o esterni credenziali di accesso ai sistemi aziendali o di terzi.

Il Responsabile dell'Ufficio IT è incaricato di:

- monitorare periodicamente il traffico di rete aziendale, nel rispetto della normativa privacy e della dignità dei lavoratori;
- predisporre e configurare nuovi terminali e dispositivi aziendali, installando esclusivamente applicazioni approvate;
- verificare l'aggiornamento dei software di sicurezza e il corretto funzionamento delle misure di protezione.

5. Reati societari

I reati societari, disciplinati dall'art. 25-ter del d.lgs. 8 giugno 2001, n. 231, rivestono rilievo centrale per un'impresa come Compagnia Siderurgica S.p.A., che fonda reputazione e solidità economica su correttezza, trasparenza e affidabilità nella gestione. Condotte come le false comunicazioni sociali, la comunicazione di informazioni mendaci, l'ostacolo all'attività di controllo e, più in generale, ogni alterazione della veridicità della rappresentazione aziendale, minano la fiducia di soci, mercato e interlocutori istituzionali.

Compagnia Siderurgica S.p.A. considera il rispetto delle regole societarie non solo un obbligo giuridico, ma un presupposto essenziale di continuità aziendale e tutela degli interessi dei soci e degli stakeholders. La Società si impegna affinché ogni operazione sia documentata in modo chiaro, completo e veritiero; i flussi informativi verso gli organi di controllo interni ed esterni siano corretti e tempestivi; le decisioni siano assunte nel rispetto delle procedure e delle regole di governance.

È ritenuto inammissibile qualsiasi comportamento idoneo ad alterare la chiarezza dei bilanci, falsare la situazione patrimoniale, economica o finanziaria, impedire o ostacolare i controlli degli organi competenti o creare indebiti vantaggi a discapito di trasparenza e legalità.

5.1 Attività a rischio sensibile

Nell'ambito dell'operatività societaria di Compagnia Siderurgica S.p.A., le aree che possono presentare profili di rischio ai sensi dell'art. 25-ter del Decreto riguardano innanzitutto la predisposizione, la validazione e l'approvazione dei bilanci, delle relazioni e delle comunicazioni sociali, così come la tenuta della contabilità e dei libri obbligatori. Tali attività, per la loro natura e rilevanza, richiedono particolare attenzione nella corretta rappresentazione della situazione patrimoniale, economica e finanziaria della Società.

Un ulteriore ambito sensibile è costituito dai rapporti con il Collegio Sindacale, con la società di revisione legale e con gli altri organi di controllo, i quali devono poter accedere in ogni momento a dati completi, corretti e aggiornati. Anche le decisioni assunte dal Consiglio di Amministrazione, soprattutto quando riguardano operazioni straordinarie, conferimenti, distribuzioni di utili o la gestione delle riserve, possono esporre la Società a rischi di natura societaria qualora non siano fondate su informazioni veritiere, documentate e coerenti con la realtà gestionale.

Rilevano, inoltre, le attività quotidiane di natura amministrativo-finanziaria, comprendenti la formazione e l'archiviazione dei documenti contabili, le procedure di autorizzazione e registrazione delle operazioni economiche, nonché le comunicazioni verso soggetti pubblici o privati che richiedono dati di carattere societario.

In tutti questi processi è essenziale garantire la tracciabilità delle fonti, la coerenza dei dati tra i diversi sistemi informativi e la chiara segregazione delle funzioni tra chi elabora le informazioni e chi le valida, in modo da assicurare un controllo effettivo e ridurre il rischio di errori, omissioni o comportamenti dolosi.

5.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. ispira la propria gestione a principi di correttezza, trasparenza e veridicità, elementi che costituiscono il fondamento della fiducia che la Società intende mantenere nei confronti di soci, organi di controllo, istituzioni e mercato. Tutti coloro che, a diverso titolo, partecipano alla formazione, alla comunicazione o alla conservazione dei dati contabili e societari sono tenuti a operare con la massima diligenza e integrità, assicurando che ogni documento, atto o informazione rappresenti fedelmente la realtà aziendale.

Ogni operazione deve essere supportata da un'adeguata documentazione, idonea a garantire la tracciabilità delle decisioni e delle fonti utilizzate. È fatto espresso divieto di porre in essere comportamenti che possano alterare la chiarezza dei bilanci, falsare la rappresentazione della situazione patrimoniale o economica, ostacolare l'attività di controllo degli organi competenti o generare indebiti vantaggi a scapito della trasparenza e della legalità.

Le decisioni assunte dagli organi amministrativi devono fondarsi su informazioni complete, attendibili e verificabili, nel pieno rispetto delle regole statutarie e normative. La Società assicura che i processi di approvazione delle operazioni, sia ordinarie che straordinarie, siano supportati da flussi informativi strutturati e da un sistema di responsabilità chiaramente definito, in modo da evitare sovrapposizioni o lacune nei poteri decisionali.

Un ruolo di rilievo è attribuito al sistema di deleghe e procure, che viene costantemente aggiornato e calibrato in funzione delle competenze e delle responsabilità effettivamente attribuite, garantendo la separazione tra le funzioni di elaborazione, validazione e controllo. Parallelamente, le procedure amministrative interne assicurano la correttezza delle scritture contabili e la coerenza delle informazioni tra i diversi registri e sistemi informativi.

La trasparenza nella comunicazione verso i soci e gli organi di controllo rappresenta un ulteriore presidio di prevenzione: essa consente di esercitare in modo effettivo i poteri di vigilanza e rafforza la cultura della responsabilità e della legalità all'interno dell'organizzazione. L'osservanza di tali principi è parte integrante del modello di governance adottato dalla Società e costituisce una condizione essenziale per la tutela del patrimonio, della reputazione e della continuità aziendale.

5.3 Flussi informativi da e verso l'Organismo di Vigilanza

Affinché il sistema di prevenzione dei reati societari sia realmente efficace, è indispensabile che l'Organismo di Vigilanza riceva con continuità e tempestività tutte le informazioni utili a verificare l'osservanza del Modello e a monitorare le aree di rischio individuate. La collaborazione tra i soggetti aziendali e l'Organismo rappresenta, infatti, un elemento fondamentale del sistema di controllo interno, volto a garantire la trasparenza e la correttezza della gestione societaria.

Tutti coloro che, nell'ambito delle proprie funzioni, vengano a conoscenza di fatti, comportamenti o anomalie che possano anche solo potenzialmente integrare una violazione delle disposizioni in materia di reati societari, sono tenuti a informarne senza indugio l'Organismo di Vigilanza. In particolare, devono essere oggetto di comunicazione le eventuali irregolarità contabili, le anomalie nei flussi amministrativi e finanziari, le carenze nella documentazione di supporto o le criticità riscontrate nella rappresentazione dei dati di bilancio e nelle scritture sociali.

Devono inoltre essere trasmesse all'Organismo le informazioni relative al processo di approvazione dei bilanci e delle relazioni sociali, alle operazioni sul capitale, alle modifiche statutarie e, più in generale, a qualsiasi evento che possa incidere in modo rilevante sulla veridicità e trasparenza della rappresentazione societaria. Analogamente, gli esiti delle verifiche e delle osservazioni formulate dal Collegio Sindacale o dalla

società di revisione legale devono essere messi a disposizione dell'Organismo, affinché quest'ultimo possa valutarne l'impatto in termini di conformità e di rischio.

L'Organismo di Vigilanza, dal canto suo, è tenuto a garantire la riservatezza delle informazioni ricevute, ad attivare gli approfondimenti ritenuti necessari e a riferire periodicamente al Consiglio di Amministrazione in merito alle risultanze delle proprie attività di monitoraggio. Tali relazioni periodiche hanno lo scopo di evidenziare eventuali criticità emerse e di formulare raccomandazioni utili al miglioramento dei presidi organizzativi e procedurali.

Il rapporto tra i soggetti aziendali e l'Organismo di Vigilanza deve essere sempre improntato a trasparenza, collaborazione e senso di responsabilità, nella consapevolezza che la corretta circolazione delle informazioni costituisce il presupposto per un'efficace prevenzione dei reati e per il consolidamento di una cultura aziendale basata sulla legalità e sulla correttezza dei comportamenti.

5.4 Protocolli di prevenzione

Compagnia Siderurgica S.p.A., pur non essendo una società quotata e quindi non esposta ai rischi tipici delle realtà che operano su mercati regolamentati, considera comunque essenziale presidiare in modo rigoroso i processi che possono esporla a responsabilità ai sensi dell'art. 25-ter del Decreto. La presenza del Collegio Sindacale e della società di revisione legale, rappresenta un importante elemento di garanzia in quanto consente di assicurare un controllo indipendente e costante sulla veridicità dei bilanci, sull'affidabilità dei dati contabili e sulla correttezza delle procedure amministrative.

La struttura organizzativa della Società, caratterizzata da dimensioni contenute e da un sistema decisionale accentrato ma trasparente, consente di esercitare un efficace monitoraggio su tutte le operazioni di natura ordinaria e straordinaria. Tale configurazione, unita alla presenza di un responsabile amministrativo e finanziario (CFO) e di un Consiglio di Amministrazione snello e operativo, permette di mantenere sotto controllo l'intero ciclo contabile e di garantire che ogni attività sia tracciabile, documentata e coerente con le regole interne.

In quest'ottica, la Società ha adottato protocolli operativi specifici volti a disciplinare la registrazione e la validazione dei dati contabili, la formazione delle scritture di bilancio e la gestione delle operazioni economiche. Ogni fattura, sia attiva che passiva, viene registrata a sistema previa verifica della sua correttezza formale e sostanziale; vengono inoltre effettuati controlli periodici per individuare eventuali duplicazioni o incongruenze nei dati contabili, nonché per segnalare tempestivamente importi anomali o non coerenti con l'andamento ordinario della gestione.

Le operazioni di pagamento e contabilizzazione delle poste passive sono subordinate all'autorizzazione preventiva degli organi competenti, al fine di evitare approvazioni generiche o reiterate che possano compromettere la chiarezza e la tracciabilità delle decisioni. Ogni variazione dei conti contabili è sottoposta al controllo del CFO, che ne autorizza la creazione o la modifica solo a seguito di opportune verifiche.

La Società adotta criteri uniformi per l'imputazione dei costi e regola con contratti formalizzati le eventuali attività esternalizzate, garantendo la piena tracciabilità delle informazioni e il rispetto delle regole di governance interna. Tutta la documentazione contabile è archiviata secondo procedure che assicurano integrità, reperibilità e riservatezza dei dati, consentendo l'accesso esclusivamente al personale autorizzato.

Nel processo di formazione del bilancio, ogni funzione aziendale coinvolta è tenuta a trasmettere tempestivamente i dati di propria competenza, rispettando le tempistiche e le modalità previste dalle procedure interne. Le informazioni vengono validate dal CFO, che ne verifica la completezza e la coerenza prima dell'invio al Consiglio di Amministrazione per l'approvazione. Tale iter garantisce una chiara attribuzione delle responsabilità, la tracciabilità dei controlli eseguiti e la disponibilità di adeguata documentazione di supporto.

Infine, il progetto di bilancio viene trasmesso ai componenti del Consiglio di Amministrazione secondo modalità che ne assicurano la ricezione tracciabile, consentendo a ciascun amministratore di formulare eventuali osservazioni o richieste di chiarimento. Questo processo, trasparente e documentato, costituisce uno dei presidi più efficaci per prevenire il rischio di false comunicazioni sociali, di corruzione tra privati e, più in generale, di ogni comportamento idoneo a compromettere la correttezza e la veridicità delle informazioni societarie.

6. Delitti di criminalità organizzata

L'articolo 24-ter del Decreto Legislativo 8 giugno 2001, n. 231, individua una serie di reati riconducibili a fenomeni di criminalità organizzata, tra cui le associazioni di tipo mafioso, le associazioni finalizzate al traffico illecito di sostanze stupefacenti, al contrabbando, alla tratta di persone o ad altre attività delittuose strutturate in modo stabile e coordinato.

Pur operando in un contesto industriale nel quale il rischio di tali condotte non risulta elevato, Compagnia Siderurgica S.p.A. riconosce che l'eventualità di infiltrazioni o interferenze di natura criminale non può essere completamente esclusa, soprattutto nei rapporti con fornitori, subappaltatori, intermediari o altri soggetti terzi che operano lungo la filiera produttiva o commerciale.

La Società adotta pertanto una posizione di assoluta fermezza e intransigenza nei confronti di ogni forma di criminalità organizzata, rifiutando qualsiasi relazione, anche indiretta o occasionale, con soggetti riconducibili

a contesti illeciti o che possano determinare rischi reputazionali, economici o legali. Tale impegno si traduce in procedure di controllo rigorose, nella tracciabilità dei rapporti economici e nella costante vigilanza su tutte le attività che comportano interazioni con controparti esterne.

Il Modello 231, unitamente al Codice Etico e al sistema di segnalazione delle violazioni, costituisce il principale strumento attraverso il quale Compagnia Siderurgica S.p.A. previene e contrasta qualunque forma di infiltrazione criminale. Ogni soggetto che opera per conto o nell'interesse della Società è tenuto a mantenere comportamenti improntati alla legalità e alla correttezza, evitando qualsiasi condotta che possa, anche solo indirettamente, agevolare attività riconducibili alla criminalità organizzata.

6.1 Attività a rischio sensibile

Le attività che, nell'ambito operativo di Compagnia Siderurgica S.p.A., possono presentare profili di rischio in relazione ai delitti di criminalità organizzata riguardano principalmente la gestione dei rapporti economici e contrattuali con soggetti terzi.

Particolare attenzione è richiesta nella selezione e nella qualificazione dei fornitori, dei subappaltatori e dei partner commerciali, soprattutto in fase di avvio di nuovi rapporti o di affidamento di commesse significative. In tali momenti, la mancanza di adeguate verifiche sulla reputazione o sulla provenienza dei soggetti coinvolti potrebbe esporre la Società al rischio di instaurare relazioni con controparti collegate a contesti illeciti.

Anche la gestione dei flussi finanziari connessi a forniture e prestazioni di servizi costituisce un'area sensibile, in quanto eventuali pagamenti non tracciabili, modalità di regolazione in contanti o utilizzo di intermediari non verificati potrebbero fungere da veicolo per operazioni opache o di riciclaggio. Analogamente, la scelta di nuovi interlocutori commerciali o logistici richiede un controllo preventivo accurato, volto a verificare l'assenza di procedimenti penali o interdittive antimafia.

Pur operando in una filiera industriale consolidata e composta da partner tradizionalmente affidabili, Compagnia Siderurgica S.p.A. mantiene un atteggiamento di costante vigilanza, consapevole che la prevenzione di tali rischi richiede un controllo continuo e una piena tracciabilità di ogni operazione economica e contrattuale.

6.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. ripudia in modo assoluto qualsiasi forma di criminalità organizzata e si impegna a garantire la massima trasparenza e legalità in ogni rapporto economico e commerciale. Tutte le decisioni relative alla selezione, alla qualificazione e alla gestione dei fornitori e dei partner devono essere fondate su criteri oggettivi, documentabili e conformi alle procedure aziendali.

Prima dell'instaurazione di un nuovo rapporto contrattuale, la Società effettua verifiche sulla reputazione, sulla solidità economica e sull'affidabilità del soggetto terzo, con particolare attenzione all'eventuale presenza di segnalazioni negative, procedimenti giudiziari o iscrizioni in elenchi antimafia. In ogni caso, i rapporti economici devono essere regolati mediante contratti scritti che prevedano clausole di rispetto delle leggi e dei principi etici aziendali, con possibilità di risoluzione immediata in caso di violazioni.

I pagamenti e le movimentazioni finanziarie devono avvenire esclusivamente tramite canali tracciabili, nel rispetto delle procedure interne e delle normative vigenti in materia di antiriciclaggio. È vietato l'uso di contanti o di strumenti che possano compromettere la trasparenza delle operazioni. I responsabili di funzione vigilano sul rispetto di tali regole e sono tenuti a segnalare tempestivamente all'Organismo di Vigilanza qualsiasi anomalia o situazione potenzialmente sospetta.

La Società promuove inoltre una cultura aziendale fondata sulla legalità e sulla collaborazione, favorendo la sensibilizzazione del personale e dei collaboratori rispetto ai rischi connessi alla criminalità organizzata. Ogni comportamento, decisione o prassi che possa anche solo apparire in contrasto con tali principi è considerato inaccettabile e può costituire motivo di sanzione disciplinare o di interruzione del rapporto contrattuale.

6.3 Flussi informativi da e verso l'Organismo di Vigilanza

Per assicurare un controllo efficace sulle aree a rischio, Compagnia Siderurgica S.p.A. garantisce flussi informativi costanti e puntuali da e verso l'Organismo di Vigilanza. Devono essere tempestivamente comunicati all'Organismo i dati relativi alle verifiche di qualificazione e affidabilità dei fornitori, dei subappaltatori e dei partner commerciali, nonché eventuali anomalie, irregolarità o segnalazioni provenienti da dipendenti o da soggetti esterni.

Rientrano tra i flussi informativi anche le comunicazioni riguardanti contratti risolti per violazioni delle clausole etiche o per sospetti di condotte illecite, così come le segnalazioni whistleblowing concernenti possibili contatti con soggetti collegati, direttamente o indirettamente, a fenomeni di criminalità organizzata.

L'Organismo di Vigilanza, nel rispetto dei principi di indipendenza e riservatezza, analizza le informazioni ricevute e redige relazioni periodiche indirizzate al Consiglio di Amministrazione, evidenziando eventuali criticità e formulando raccomandazioni operative. Questo sistema di comunicazione e controllo continuo consente alla Società di mantenere alta la soglia di attenzione e di rafforzare, in modo strutturale, la propria capacità di prevenzione rispetto a ogni possibile forma di infiltrazione o condizionamento criminale.

7. Falsità in monete, carte di pubblico credito e valori di bollo

Le fattispecie contemplate dall'articolo 25-bis del Decreto Legislativo 8 giugno 2001, n. 231, riguardano reati di particolare gravità, collegati alla contraffazione, alterazione o messa in circolazione di monete, carte di pubblico credito, valori di bollo o strumenti simili. Si tratta di condotte che, pur non essendo in alcun modo riconducibili alle attività produttive e commerciali proprie di Compagnia Siderurgica S.p.A., devono essere considerate nell'ambito del Modello di organizzazione e gestione, in quanto ogni impresa operante sul mercato è potenzialmente esposta, anche solo in via indiretta, al rischio di utilizzo o accettazione inconsapevole di strumenti o documenti falsificati.

Per la Società, il tema assume rilievo in modo riflesso, in particolare con riferimento ai rapporti economici e commerciali con clienti, fornitori e partner, attraverso i quali potrebbero transitare mezzi di pagamento o documentazione contraffatta. È pertanto necessario che l'organizzazione aziendale preveda controlli adeguati a prevenire qualsiasi rischio di coinvolgimento, anche involontario, in condotte di questo tipo, garantendo sempre la tracciabilità delle operazioni e la verifica dell'autenticità dei documenti e dei titoli utilizzati.

L'inclusione di tali reati nel Modello 231 non risponde dunque a un'esigenza meramente formale, ma riflette la volontà della Società di mantenere elevati standard di legalità e trasparenza, promuovendo una cultura aziendale fondata sulla diligenza, sulla prudenza e sulla correttezza nella gestione dei rapporti economici e documentali.

7.1 Attività a rischio sensibile

Nel contesto operativo di Compagnia Siderurgica S.p.A., le attività che possono presentare profili di rischio, pur limitati, connessi ai reati di falsità in monete o strumenti assimilati, si riferiscono prevalentemente alla gestione dei flussi finanziari e documentali.

La fase di incasso e pagamento rappresenta l'ambito più esposto, in quanto può verificarsi — seppure in casi rari — la presentazione di titoli di credito, assegni o strumenti di pagamento non autentici. Analoghi rischi, seppur residuali, possono emergere nella gestione e archiviazione della documentazione amministrativa, laddove vengano ricevuti o utilizzati atti, certificazioni o documenti che si rivelino alterati o contraffatti.

Anche nei rapporti con istituti di credito, clienti e fornitori è fondamentale mantenere un atteggiamento prudente e verificare sempre la regolarità formale dei documenti ricevuti, al fine di evitare l'accettazione, anche inconsapevole, di strumenti non autentici.

Sebbene la Società operi con controparti consolidate e all'interno di circuiti bancari e commerciali tracciabili, l'attenzione e la diligenza nella verifica degli strumenti di pagamento e della documentazione amministrativa costituiscono presidi essenziali per la prevenzione di possibili rischi residui.

7.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. richiede a tutti i propri dipendenti, collaboratori e partner commerciali la massima correttezza e attenzione nella gestione dei flussi amministrativi e finanziari, nonché nella ricezione e nel controllo della documentazione societaria. Ogni operazione economica deve essere pienamente tracciabile, documentata e conforme alle procedure interne.

I pagamenti e gli incassi avvengono esclusivamente tramite canali bancari o strumenti di pagamento ufficiali, così da garantire trasparenza e possibilità di risalire a ogni transazione. È fatto espresso divieto di accettare o disporre pagamenti in contanti, salvo i casi autorizzati per importi marginali e conformi alla normativa vigente, previa approvazione della Direzione amministrativa.

Tutti i soggetti coinvolti nella gestione documentale o nei rapporti con clienti, fornitori e istituti di credito sono tenuti a verificare l'autenticità dei documenti e dei titoli ricevuti, adottando — ove necessario — misure di riscontro aggiuntive presso le autorità competenti o gli enti emittenti. Ogni anomalia, sospetto di irregolarità o segnalazione proveniente da terzi deve essere immediatamente comunicata al superiore gerarchico e all'Organismo di Vigilanza, che valuterà la necessità di ulteriori approfondimenti.

La Società promuove controlli periodici, anche a campione, sulla documentazione amministrativa e finanziaria, garantendo la segregazione delle funzioni tra chi dispone i pagamenti e chi li esegue, così da assicurare un sistema di controllo incrociato. La formazione del personale amministrativo include specifici moduli dedicati alla verifica documentale e alla prevenzione di condotte fraudolente, al fine di accrescere la consapevolezza e la capacità di individuare eventuali segnali di rischio.

7.3 Flussi informativi da e verso l'Organismo di Vigilanza

Compagnia Siderurgica S.p.A. assicura un costante flusso informativo tra le funzioni amministrative e finanziarie e l'Organismo di Vigilanza, in modo da garantire il tempestivo monitoraggio delle aree potenzialmente esposte. Devono essere trasmesse all'Organismo tutte le informazioni relative a comportamenti sospetti, irregolarità o segnalazioni concernenti l'utilizzo di strumenti di pagamento o di documenti contraffatti, nonché i report riepilogativi dei controlli periodici effettuati.

L'Organismo di Vigilanza analizza le informazioni ricevute, ne valuta la rilevanza rispetto al Modello 231 e riferisce periodicamente al Consiglio di Amministrazione in merito alle attività di vigilanza svolte, alle eventuali criticità riscontrate e alle raccomandazioni per il rafforzamento dei presidi di prevenzione.

Il personale della Società è tenuto a collaborare pienamente con l'Organismo, fornendo ogni informazione o documentazione utile alle verifiche, nella consapevolezza che la corretta circolazione dei dati e la tempestiva comunicazione di eventuali anomalie costituiscono elementi indispensabili per l'efficace attuazione del Modello e per la tutela della Società contro i rischi di coinvolgimento in reati di falsificazione.

8. Delitti contro l'industria e il commercio (art. 25-bis.1 D.Lgs. 231/2001)

I reati contro l'industria e il commercio assumono rilievo per Compagnia Siderurgica S.p.A. perché incidono direttamente sulla correttezza dei rapporti con clienti, fornitori, concorrenti e, più in generale, con il mercato. Fattispecie quali la contraffazione o l'alterazione di prodotti, l'impiego di segni distintivi ingannevoli, la diffusione di informazioni commerciali non veritiere o pratiche idonee a falsare la concorrenza minano l'affidabilità dell'impresa e possono determinare conseguenze gravi sul piano economico e reputazionale.

La Società, pur non operando in un comparto tipicamente esposto a tali fenomeni, individua e presidia le aree in cui, anche solo in via astratta, potrebbero manifestarsi condotte riconducibili a queste fattispecie, adottando regole chiare e controlli adeguati. Ogni informazione resa al mercato, sia tecnica sia promozionale, deve essere accurata, verificabile e coerente con le reali caratteristiche dei prodotti e dei servizi offerti. La comunicazione commerciale si svolge nel rispetto della normativa a tutela dei consumatori, della proprietà industriale e della concorrenza leale, evitando espressioni ambigue, denigratorie o idonee a trarre in inganno.

Particolare attenzione è rivolta ai segni distintivi e ai marchi, propri e altrui: è vietato ogni uso improprio o ingannevole, così come ogni condotta che possa determinare confusione con i marchi di terzi o sfruttarne indebitamente la notorietà. La Società non tollera la commercializzazione di prodotti non conformi agli standard dichiarati o accompagnati da certificazioni, marcature o attestazioni non corrispondenti alla realtà.

Questi principi trovano attuazione attraverso procedure interne che garantiscono tracciabilità delle operazioni e verifica di conformità della documentazione tecnica e commerciale. Ogni anomalia o irregolarità è segnalata ai responsabili competenti e all'Organismo di Vigilanza, per i conseguenti approfondimenti e le eventuali misure correttive.

8.1 Attività a rischio sensibile

I profili di rischio possono emergere nelle attività che comportano contatti diretti con il mercato e con soggetti esterni: gestione dei rapporti commerciali, predisposizione della documentazione contrattuale, comunicazione esterna, attività di vendita e approvvigionamento. In tali contesti, un'informazione non pienamente corrispondente alla realtà, anche non intenzionale, può ingannare i destinatari o incidere sulla leale concorrenza.

Ulteriore area sensibile è la gestione dei marchi, loghi e segni distintivi, propri e di terzi: utilizzi non autorizzati o impropri possono integrare condotte vietate. Rileva anche la corretta qualificazione e tracciabilità dei prodotti e dei servizi, inclusa la coerenza tra specifiche tecniche, certificazioni e documenti commerciali, poiché attestazioni inesatte possono, in astratto, assumere rilievo penale.

Infine, la selezione di fornitori e partner contrattuali richiede verifiche preventive su reputazione e conformità normativa degli interlocutori, per evitare il rischio di coinvolgimento, seppur indiretto, in pratiche scorrette o illecite.

8.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. imposta i rapporti con il mercato sui principi di veridicità, trasparenza e lealtà. Le informazioni commerciali, tecniche o promozionali sono redatte con chiarezza e completezza; il principio di veridicità vale per ogni forma di comunicazione, anche informale. L'uso dei segni distintivi aziendali avviene nel rispetto delle registrazioni e delle regole interne; è vietato utilizzare marchi o denominazioni di terzi senza idoneo titolo.

Prima di instaurare nuove collaborazioni, la Società svolge verifiche sull'affidabilità e sulla conformità dei partner, anche mediante strumenti di valutazione reputazionale e, quando opportuno, dichiarazioni formali di impegno al rispetto della legalità e della trasparenza. Sul piano organizzativo, le procedure interne assicurano tracciabilità e corretta conservazione della documentazione commerciale; ogni fase — dalla negoziazione alla consegna — è registrata e verificabile, in coerenza con il sistema di gestione della qualità.

L'obiettivo è consolidare una cultura d'impresa orientata all'etica degli affari, affinché chiunque operi per conto della Società sia consapevole della responsabilità di agire sempre con correttezza sul mercato.

8.3 Flussi informativi da e verso l'Organismo di Vigilanza

La prevenzione efficace richiede flussi informativi tempestivi e completi. Le funzioni coinvolte nelle attività commerciali e nella gestione dei rapporti con clienti, fornitori e partner collaborano con l'Organismo di Vigilanza, segnalando prontamente anomalie e rischi: contestazioni del mercato, sospetti di pratiche scorrette, uso non autorizzato di marchi o segni distintivi, comportamenti potenzialmente idonei a compromettere la trasparenza.

Le segnalazioni sono formalizzate attraverso i canali dedicati, nel rispetto delle procedure interne e della riservatezza. L'Organismo di Vigilanza analizza le informazioni ricevute, valuta l'efficacia dei presidi e, ove necessario, propone interventi correttivi, riferendo periodicamente al Consiglio di Amministrazione sullo stato di attuazione delle misure preventive e sulle eventuali criticità emerse.

8.4 Protocolli di prevenzione

Per rendere operativi i principi sopra enunciati, Compagnia Siderurgica S.p.A. adotta i seguenti protocolli specifici per i delitti contro l'industria e il commercio:

8.4.1. Protocollo per la gestione di marchi, segni distintivi e comunicazione commerciale

La funzione commerciale e la direzione tecnica verificano preventivamente che loghi, marchi, denominazioni e materiali promozionali siano coerenti con le registrazioni e le linee guida interne. Ogni uso di segni di terzi richiede titolo idoneo (licenza, autorizzazione scritta) archiviato in modo tracciabile. Le comunicazioni tecniche e i claim commerciali sono validati dalla funzione competente (tecnica/qualità) e dalla funzione legale o compliance, con conservazione della documentazione di supporto (test, certificazioni, report).

8.4.2. Protocollo per la veridicità delle specifiche tecniche e dei documenti di fornitura

Schede tecniche, certificazioni di materiale, attestazioni di conformità e qualsiasi documento che accompagni le forniture sono emessi o verificati dalla funzione qualità. È assicurata la coerenza tra caratteristiche dichiarate e caratteristiche effettive del prodotto; eventuali aggiornamenti sono tempestivamente recepiti nella documentazione commerciale. È previsto un sistema di campionamento e controlli a campione sulle forniture critiche.

8.4.3. Protocollo per la tracciabilità dei prodotti e la gestione delle non conformità verso il mercato

Ogni lotto/commissa è tracciato in modo da risalire a materia prima, lavorazioni e controlli effettuati. Le non conformità rilevate in fase interna o segnalate dal cliente sono registrate, analizzate e gestite con azioni correttive e, se necessario, con comunicazioni trasparenti al cliente e, nei casi più rilevanti, con informativa all'Organismo di Vigilanza.

8.4.4. Protocollo per la qualificazione e il monitoraggio dei fornitori

Prima dell'inserimento a sistema, i fornitori sono valutati su requisiti tecnico-qualitativi, legali e reputazionali;

l'uso di marchi o riferimenti di terzi da parte dei fornitori è consentito solo se legittimato. La qualifica è soggetta a riesame periodico; in presenza di segnali di rischio (contestazioni seriali, uso improprio di marchi, documenti tecnici incoerenti) la fornitura è sospesa e la posizione riesaminata.

8.4.5. Protocollo per la gestione delle comunicazioni di marketing e comparazioni

Le comparazioni con prodotti/concorrenti, se utilizzate, sono ammesse solo se oggettive, verificabili e non denigratorie; ogni materiale comparativo è sottoposto a doppia validazione (tecnica e legale/compliance) prima della diffusione. Sono vietate espressioni idonee a creare confusione o a sfruttare indebitamente la notorietà altrui.

8.4.6. Protocollo per le segnalazioni e i richiami di prodotto verso il mercato

È istituito un canale interno per la segnalazione di sospette non conformità idonee a incidere su qualità, sicurezza o correttezza dell'informazione verso il mercato. In caso di necessità, è attivata una procedura di informazione ai clienti e di eventuale richiamo, con gestione centralizzata della comunicazione e tracciatura completa delle azioni intraprese.

9. Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio

La prevenzione dei fenomeni di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio, di cui all'art. 25-octies del d.lgs. 231/2001, rappresenta un presidio essenziale per garantire legalità, reputazione e solidità gestionale di Compagnia Siderurgica S.p.A.. Tali fattispecie mirano a immettere nel circuito economico risorse di origine criminale alterandone o occultandone la provenienza; per questo la Società adotta regole e controlli idonei a scongiurare qualsiasi coinvolgimento, anche indiretto, in pratiche illecite.

In quest'ottica, assumono rilievo la tracciabilità dei pagamenti, la verifica dell'affidabilità delle controparti e la piena giustificazione economica delle operazioni, affinché ogni flusso finanziario e ogni trasferimento di beni o utilità risultino leciti, documentati e coerenti con l'attività aziendale.

9.1 Attività a rischio sensibile

I profili di rischio possono emergere soprattutto nella gestione dei rapporti economici e finanziari con clienti, fornitori, distributori e partner, nonché nella gestione della tesoreria e nelle operazioni bancarie. Particolare attenzione è richiesta per incassi e pagamenti, specie quando si prospettino modalità non tracciabili o non usuali, e in occasione dell'avvio di relazioni con controparti non adeguatamente verificate sotto il profilo reputazionale, amministrativo e finanziario.

Ulteriori aree sensibili riguardano i movimenti infragruppo o con soggetti collegati, le operazioni di finanziamento e, più in generale, qualunque transazione che implichi trasferimenti transfrontalieri o rapporti con controparti ubicate in Paesi a rischio elevato in materia di antiriciclaggio. Anche condotte prive di intento

illecito possono determinare rilevanti conseguenze penali e reputazionali, se non presidiate da adeguati controlli.

9.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. considera la prevenzione dei rischi di cui all'art. 25-octies parte integrante della propria governance. I principi operativi sono i seguenti:

- Giustificazione economica e documentazione: ogni operazione finanziaria o commerciale deve rispondere a effettive esigenze aziendali ed essere correttamente documentata, con causali chiare, verificabili e coerenti con l'attività sociale.
- Tracciabilità dei flussi: pagamenti e incassi avvengono esclusivamente tramite strumenti tracciabili (es. circuiti bancari o mezzi equiparati). L'uso del contante è limitato ai soli casi consentiti dalla normativa e secondo le procedure interne, previa autorizzazione della funzione amministrativa competente.
- Selezione e valutazione delle controparti (due diligence): prima di instaurare rapporti con clienti, fornitori, agenti o partner, la Società effettua verifiche reputazionali, amministrative e finanziarie; nei casi di Paesi ad alto rischio o di profili sensibili (ad es. persone politicamente esposte), adotta misure di adeguata verifica rafforzata e richiede l'approvazione preventiva degli organi competenti.
- Segregazione dei compiti e controlli: nessun soggetto gestisce in autonomia tutte le fasi di una stessa operazione economico-finanziaria. Sono previste soglie di autorizzazione, firme congiunte e controlli a campione.
- Divieti espressi: è vietato destinare fondi, beni o utilità per finalità estranee all'attività sociale; è vietato occultare o dissimulare la provenienza di risorse di origine sospetta, anche tramite operazioni solo apparentemente regolari.
- Segnalazioni e whistleblowing: ogni dipendente o collaboratore segnala tempestivamente situazioni anomale o sospette ai responsabili interni e, se del caso, all'Organismo di Vigilanza (OdV), con tutela del segnalante e divieto di ritorsioni.
- Formazione: sono previsti programmi formativi dedicati e modulati per ruolo e rischio, volti a diffondere consapevolezza sui segnali di anomalia e sulle corrette cautele operative.

9.3 Flussi informativi da e verso l'Organismo di Vigilanza

Il presidio è fondato su un flusso informativo costante e bidirezionale con l'OdV. Le funzioni competenti trasmettono periodicamente (o a seguito di eventi rilevanti) informazioni su operazioni atipiche o incoerenti rispetto alla normale operatività: pagamenti o incassi verso/da Paesi a rischio, modalità di regolamento non usuali o di difficile tracciabilità, rapporti con controparti la cui affidabilità non risulti adeguatamente comprovata.

L'OdV può richiedere chiarimenti e documentazione alle funzioni interessate; la Società assicura collaborazione piena, risposte puntuali e complete. Sono inoltre valorizzate le segnalazioni whistleblowing provenienti da personale interno o partner, gestite con riservatezza e imparzialità.

L'OdV riferisce periodicamente al Consiglio di Amministrazione esiti, criticità e raccomandazioni, così da mantenere il Modello aggiornato e coerente con l'operatività.

9.4 Processi sensibili e Protocolli di prevenzione

Di seguito sono disciplinati i processi maggiormente esposti e i relativi protocolli operativi, redatti in forma chiara e applicativa.

9.4.1 Protocollo per la gestione dei flussi finanziari con clienti, fornitori e partner

Per prevenire rischi di riciclaggio nei flussi in entrata:

- la funzione amministrazione (alle dipendenze del Responsabile Amministrativo e Finanza – CFO) effettua controlli formali e sostanziali sugli incassi, verificando la coerenza della controparte, le banche utilizzate e l'eventuale presenza di schermi societari;
- non si accettano pagamenti in contanti oltre le soglie di legge; per titoli al portatore si ricorre, ove consentito, solo a intermediari abilitati;
- sono mantenute registrazioni su archivi informatici idonee a tracciare movimentazioni collegate a conti esteri o giurisdizioni a rischio, secondo le procedure AML interne.

Per i rapporti con fornitori e partner:

- il Responsabile di Ufficio competente, insieme al Responsabile Acquisti, identifica il responsabile dell'esecuzione contrattuale, con compiti e responsabilità definiti;
- è garantita la tracciabilità degli accordi e la congruità economica delle transazioni (prezzi di mercato, uso di professionisti di fiducia, benchmark);

- si verifica la piena coincidenza tra ordinanti/destinatari dei pagamenti e controparti effettive; sono vietati strumenti anonimi; l'utilizzo di contante o titoli al portatore oltre le soglie legali è escluso;
- si monitora l'operatività su conti in giurisdizioni con minori standard di trasparenza, con registrazioni dedicate e controlli rafforzati.

Requisiti AML trasversali (in coerenza con la normativa vigente):

- adeguata verifica della clientela (quando e come identificare cliente e titolare effettivo, scopo e natura della transazione);
- approccio basato sul rischio (obblighi semplificati per soggetti a loro volta vigilati; verifica rafforzata per clienti non presenti fisicamente, PEP, non residenti o intermediari extra-UE ad alto rischio);
- obbligo di astensione dall'aprire/mantenere rapporti quando non sia possibile svolgere correttamente l'adeguata verifica o sussista il sospetto di riciclaggio/finanziamento del terrorismo;
- segnalazione di operazioni sospette e comunicazione delle infrazioni in materia di limiti all'uso del contante e dei titoli al portatore;
- monitoraggio delle transazioni con Paesi oggetto di restrizioni o sanzioni internazionali;
- formazione periodica del personale sulle misure AML interne.

9.4.2 Protocollo per la gestione delle sponsorizzazioni

Le sponsorizzazioni (fornitura di denaro, beni o servizi in cambio di promozione del nome/marchio) sono ammesse solo se:

- deliberata da un Amministratore Delegato (AD), in presenza di un interesse concreto e attuale e di un ritorno di immagine proporzionato;
- precedute dalla stipula di un contratto scritto con clausole etiche e facoltà di recesso/risoluzione in caso di violazioni;
- oggetto di verifica di congruità tra contributo e controprestazione sulla base di parametri di mercato;
- supportate da documentazione completa (contratto, piani promozionali, rendiconti), archiviata presso l'AD e/o l'Ufficio Commerciale / Amministrazione.

È esclusa ogni sponsorizzazione verso soggetti/enti non verificati o riconducibili a contesti a rischio reputazionale o AML.

9.4.3 Protocollo per l'acquisto di beni e servizi

Selezione fornitori: si utilizza la Lista Fornitori Qualificati; per nuovi o occasionali, si svolgono controlli preliminari (legali, reputazionali e tecnici). Valutazione offerte: criteri preventivi e trasparenti; prevale l'offerta economicamente più vantaggiosa a parità di standard qualitativi. Offerte anomale o eccessivamente basse sono segnalate al Responsabile di Ufficio per approfondimenti.

Profilo di legalità e provenienza beni: in caso di dubbi sulla lecita provenienza, si informa immediatamente il CFO o un Amministratore Delegato che, effettuate le verifiche, può interrompere la trattativa. Si verifica la residenza/Paese della controparte e si raccolgono informazioni utili a valutarne l'affidabilità (anche mediante dichiarazioni sostitutive). La documentazione è mantenuta aggiornata lungo il rapporto.

Archiviazione: tutta la documentazione del processo di acquisto è archiviata in modo completo, tracciabile e con accesso riservato.

9.4.4 Protocollo per l'affidamento di consulenze

Le consulenze sono attivate solo quando esista un interesse concreto e attuale e non sia efficiente l'uso di risorse interne.

- Avvio sempre successivo a contratto scritto, con oggetto, durata, deliverable e clausole etiche.
- Congruità del compenso valutata rispetto a: tariffe di mercato, competenze richieste, durata, complessità, contenuto della prestazione (con relazione finale misurabile).
- Prova dell'effettività: si archivia documentazione delle attività svolte (rapporti, verbali, output).

9.4.5 Protocollo per la Selezione e Gestione dei Fornitori

In ogni caso, resta fermo l'obbligo di: due diligence proporzionata al rischio; clausole contrattuali di legalità e risoluzione; tracciabilità dei pagamenti; monitoraggio periodico della performance e della conformità.

10. Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1)

La crescente diffusione di strumenti di pagamento alternativi al contante — carte di credito e di debito, bonifici elettronici, wallet digitali, piattaforme di pagamento e applicazioni connesse — ha migliorato l'efficienza dei processi amministrativi, ma ha introdotto nuove superfici di rischio. L'art. 25-octies.1 del d.lgs. 231/2001 ricomprende tra i reati presupposto le condotte fraudolente commesse mediante l'uso o la falsificazione di tali strumenti.

Pur non operando in un settore tipicamente esposto alle frodi di pagamento, Compagnia Siderurgica S.p.A. è consapevole che l'impiego quotidiano di strumenti elettronici verso fornitori, dipendenti e partner richiede

presidi organizzativi adeguati. Le vulnerabilità possono emergere tanto dall'interno quanto dall'esterno, specie se i controlli sulle autorizzazioni di spesa, sull'abilitazione agli strumenti, sulle piattaforme utilizzate e sulla gestione delle credenziali non sono sufficientemente robusti. La Società fa quindi propri i principi di tracciabilità, trasparenza e segregazione dei compiti, affinché ogni operazione sia documentata, giustificata e gestita esclusivamente tramite canali autorizzati e sicuri.

Un ruolo centrale è attribuito alla formazione del personale amministrativo e contabile e alla sensibilizzazione sull'uso corretto delle credenziali e sul riconoscimento dei segnali di frode (ad es. richieste atipiche di variazione IBAN, urgenze anomale, tentativi di business e-mail compromise). Le segnalazioni tempestive — anche attraverso i canali di whistleblowing — e i flussi informativi verso l'Organismo di Vigilanza consentono il monitoraggio continuo e l'adozione di misure correttive mirate.

10.1 Attività a rischio sensibile

I rischi connessi ai delitti in materia di strumenti di pagamento diversi dal contante non sono strutturali, ma possono manifestarsi in alcune aree: in primo luogo, nella gestione dei rapporti economici con clienti e fornitori, dove carte aziendali, bonifici e piattaforme digitali possono essere esposti a utilizzi non autorizzati, appropriazioni indebite o frodi informatiche; quindi nelle procedure di acquisto di materiali, componenti o servizi, se i passaggi di autorizzazione e verifica non sono adeguatamente presidiati; infine nella gestione tecnica degli account e dei sistemi collegati ai pagamenti elettronici, che potrebbero subire accessi abusivi, furto di credenziali o manomissioni dei dati.

Un'ulteriore area di attenzione riguarda le operazioni non ricorrenti o di importo significativo, i pagamenti urgenti disposti fuori flusso, le richieste di variazione delle coordinate bancarie dei fornitori, nonché i rapporti con controparti ubicate in Paesi a maggior rischio. Anche se residuale rispetto all'attività manifatturiera, il rischio che terzi tentino di utilizzare l'azienda come canale per movimentare fondi illeciti mediante strumenti elettronici impone un presidio minimo e costante.

10.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. imposta la gestione degli strumenti di pagamento elettronici su legalità, trasparenza e correttezza. Ogni operazione deve essere tracciabile, autorizzata da soggetti competenti in base alla matrice dei poteri e supportata da documentazione idonea a consentire controlli e verifiche successive.

La Società adotta piattaforme di pagamento sicure e certificate, limita l'accesso agli strumenti ai soli soggetti espressamente abilitati, applica criteri di segregazione dei compiti tra chi richiede, chi autorizza e chi esegue i pagamenti, e disciplina con procedure interne la conservazione delle evidenze (ordini, contratti, DDT,

fatture, approvazioni, esiti bancari). È fatto espresso divieto di qualunque uso improprio o fraudolento di carte, wallet o credenziali digitali, come pure di gestire rapporti economici che generino dubbi sulla liceità della controparte o dell'operazione.

Gli accessi informatici ai sistemi di pagamento sono protetti da credenziali personali, autenticazione forte quando disponibile, politiche di password aggiornate, limitazione dei privilegi ("least privilege") e controlli periodici sulle utenze attive. La formazione periodica del personale copre le tecniche di frode più ricorrenti (phishing, spear-phishing, BEC), le buone pratiche di verifica (callback indipendente, controllo IBAN su fonte terza, doppi consensi) e i canali di segnalazione interna.

10.3 Flussi informativi da e verso l'Organismo di Vigilanza

Per garantire effettività ai presidi, la Società assicura un flusso informativo costante tra le funzioni amministrative/IT e l'Organismo di Vigilanza (OdV). Sono messi a disposizione dell'OdV, con cadenza periodica o su evento, i report su: operazioni di pagamento elettronico, anomalie o incidenti che abbiano impattato la sicurezza dei sistemi, richieste atipiche di variazione coordinate bancarie, respinte/chargeback e risultati dei controlli a campione.

Ogni irregolarità rilevata — ad esempio pagamenti non autorizzati, transazioni sospette, scostamenti tra autorizzato e pagato, tentativi di intrusione informatica — è tempestivamente segnalata all'OdV, che ne valuta la rilevanza 231 e propone, se del caso, azioni correttive. L'OdV mantiene un dialogo continuo con il Consiglio di Amministrazione e le funzioni interessate, può richiedere dati e convocare riunioni di approfondimento e riferisce periodicamente sugli esiti della propria vigilanza.

11. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies)

L'articolo 25-duodecies del Decreto Legislativo 231/2001 prevede la responsabilità dell'ente nel caso di impiego, in qualsiasi forma, di cittadini di paesi terzi il cui soggiorno nel territorio dello Stato sia irregolare. Questa previsione richiama l'attenzione di Compagnia Siderurgica S.p.A. sull'esigenza di mantenere procedure rigorose e trasparenti nella gestione del personale, con particolare riferimento alla fase di selezione e assunzione dei lavoratori, al fine di evitare il rischio di instaurare rapporti di lavoro con soggetti non regolarmente soggiornanti.

Pur operando in un contesto produttivo che si avvale prevalentemente di personale qualificato e di rapporti di lavoro formalizzati, la Società riconosce l'importanza di un presidio costante e documentato di questo ambito.

La corretta verifica della regolarità dei titoli di soggiorno dei cittadini extracomunitari, così come l'adozione di misure di controllo anche nei confronti di eventuali collaboratori esterni o fornitori di manodopera,

rappresentano elementi essenziali per prevenire il rischio di violazioni e per salvaguardare la reputazione e l'affidabilità dell'azienda.

Compagnia Siderurgica S.p.A. si impegna pertanto ad assicurare che ogni rapporto di lavoro, subordinato o di collaborazione, sia instaurato esclusivamente dopo un controllo accurato della documentazione personale e del titolo di soggiorno, verificandone autenticità, validità e conformità alle disposizioni di legge. La Società considera il rispetto delle norme in materia di immigrazione un dovere giuridico e morale, nonché un presupposto fondamentale della propria cultura d'impresa.

11.1 Attività a rischio sensibile

Le attività maggiormente esposte al rischio di commissione del reato di cui all'articolo 25-duodecies riguardano, in primo luogo, le fasi di selezione, assunzione e gestione del personale. In tali momenti può accadere che vengano presentati documenti di soggiorno non autentici, scaduti o non conformi ai requisiti richiesti dalla normativa vigente.

Un'ulteriore area sensibile è rappresentata dalle collaborazioni esterne e dall'impiego di personale tramite contratti di appalto o somministrazione, nei quali l'eventuale assenza di controlli adeguati sulla regolarità dei lavoratori impiegati dai partner contrattuali potrebbe esporre la Società al rischio di impiego indiretto di cittadini non in regola con le norme sul soggiorno. Attenzione deve essere riservata anche alla fase di rinnovo dei documenti di soggiorno, che richiede un costante monitoraggio per evitare la prosecuzione del rapporto di lavoro in mancanza dei requisiti legali.

Infine, anche la gestione amministrativa e documentale del personale rappresenta un ambito rilevante: la mancanza di tracciabilità o di archiviazione ordinata delle verifiche effettuate potrebbe compromettere la capacità della Società di dimostrare la propria conformità normativa e la diligenza adottata nei controlli.

11.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. considera il rispetto delle norme in materia di immigrazione e soggiorno un principio inderogabile.

È quindi vietato, in ogni circostanza, instaurare o mantenere rapporti di lavoro, anche indiretti, con cittadini di paesi terzi che non siano in possesso di un regolare permesso di soggiorno idoneo allo svolgimento dell'attività lavorativa prevista.

Per garantire il rispetto di questo principio, i processi di selezione e assunzione sono disciplinati da procedure interne che prevedono la raccolta e la verifica preventiva della documentazione anagrafica e del titolo di soggiorno, controllandone l'autenticità, la validità temporale e la coerenza con la mansione da svolgere. Tali

documenti vengono conservati in archivi dedicati, in modo ordinato e riservato, così da garantire la tracciabilità delle verifiche eseguite.

Analoghe cautele sono adottate nei rapporti con appaltatori e fornitori di servizi, i cui contratti contengono specifiche clausole che impongono il rispetto delle norme vigenti e la produzione, su richiesta, della documentazione attestante la regolarità del personale impiegato. In caso di mancato rispetto di tali obblighi, la Società si riserva la facoltà di attivare le misure contrattuali più idonee, inclusa la risoluzione del rapporto e la richiesta di risarcimento dei danni.

La responsabilità operativa delle verifiche è affidata all'ufficio del personale o, in assenza, al soggetto incaricato della gestione amministrativa dei rapporti di lavoro. Tale funzione ha il compito di monitorare periodicamente la validità dei titoli di soggiorno e di segnalare tempestivamente eventuali irregolarità o anomalie alla Direzione e all'Organismo di Vigilanza, affinché possano essere adottate le opportune misure correttive.

11.3 Flussi informativi da e verso l'Organismo di Vigilanza

Un presidio efficace di questo rischio richiede un flusso informativo costante e documentato tra la funzione del personale e l'Organismo di Vigilanza. Quest'ultimo deve ricevere regolarmente le evidenze delle verifiche svolte in sede di assunzione, le risultanze dei controlli periodici sulla validità dei permessi di soggiorno, nonché la segnalazione di eventuali anomalie, scadenze non rinnovate o inadempienze da parte di fornitori e appaltatori.

L'Organismo di Vigilanza ha la facoltà di richiedere in ogni momento chiarimenti o documentazione integrativa e di effettuare verifiche mirate sull'osservanza delle procedure interne. Tutti i flussi informativi devono essere formalizzati e archiviati in modo ordinato, così da costituire una base certa per le attività di vigilanza e per l'aggiornamento del Modello 231.

12. Contrabbando (art. 25-sexiesdecies)

Il reato di contrabbando, disciplinato dall'articolo 25-sexiesdecies del Decreto Legislativo 231/2001, riguarda le condotte finalizzate a eludere i controlli doganali o a sottrarsi al pagamento dei diritti e delle imposte dovute in occasione dell'introduzione o dell'estrazione di merci dal territorio dello Stato. Si tratta di fattispecie che, pur potendo apparire distanti dall'attività ordinaria di Compagnia Siderurgica S.p.A., assumono comunque rilievo poiché la Società, nel corso delle proprie operazioni commerciali, può intrattenere rapporti con fornitori o partner che importano o esportano beni, materiali o componenti, oppure può ricevere merci di provenienza estera.

Il rischio connesso al contrabbando non si limita alla mera movimentazione irregolare delle merci, ma si estende anche a condotte correlate, come la falsa dichiarazione doganale, l'indicazione di valori difforni rispetto a quelli effettivi, l'occultamento dell'origine o della destinazione delle merci e, più in generale, l'utilizzo di documentazione non veritiera finalizzata a eludere i controlli delle autorità competenti. In tale contesto, la Società svolge le proprie attività nel pieno rispetto della normativa doganale e tributaria, adottando procedure interne improntate a trasparenza, correttezza e tracciabilità di tutte le operazioni che, anche indirettamente, possano avere rilievo doganale.

Compagnia Siderurgica S.p.A. richiede altresì che fornitori, collaboratori e partner commerciali condividano e rispettino gli stessi principi di legalità e correttezza, riservandosi la facoltà di interrompere ogni rapporto con soggetti coinvolti in pratiche illecite o non conformi alle disposizioni di legge.

12.1 Attività a rischio sensibile

Le attività potenzialmente esposte al rischio di contrabbando riguardano principalmente i rapporti commerciali che, direttamente o indirettamente, possono coinvolgere merci di provenienza estera. Rientrano in tale ambito l'approvvigionamento di materiali o componenti acquistati da fornitori internazionali, l'utilizzo di spedizionieri o operatori doganali per la gestione delle pratiche di importazione ed esportazione, nonché i rapporti con partner che operano in settori caratterizzati da frequenti interazioni con le dogane.

Un ulteriore profilo di rischio può emergere in relazione alla documentazione amministrativa e fiscale connessa alla movimentazione dei beni, come le dichiarazioni doganali, le fatture, le bolle di accompagnamento e le certificazioni di origine. La gestione non corretta di tali documenti o la presenza di irregolarità nella loro compilazione possono esporre la Società a rischi di contestazione, anche quando le condotte illecite siano poste in essere da soggetti terzi con cui essa intrattiene rapporti contrattuali.

La particolare attenzione della Società si concentra pertanto sulla selezione e sul monitoraggio dei fornitori, sulla gestione dei contratti con partner che operano su scala internazionale e sul controllo della regolarità della documentazione doganale e di accompagnamento delle merci. Eventuali carenze in questi ambiti possono determinare conseguenze rilevanti ai sensi del Decreto Legislativo 231/2001, rendendo necessario un presidio costante e strutturato.

12.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. adotta un approccio di assoluta legalità e trasparenza nella gestione di ogni rapporto che possa avere collegamenti, anche indiretti, con attività di importazione o esportazione. È fatto divieto di intrattenere relazioni con soggetti coinvolti in pratiche di contrabbando o con operatori che non

offrano garanzie adeguate di conformità alle normative doganali e fiscali. Ogni transazione commerciale deve essere correttamente documentata e coerente con la natura, l'origine e la destinazione dei beni trattati.

Per ridurre il rischio di esposizione a condotte illecite, la Società richiede che i fornitori e i partner esteri adottino standard di comportamento conformi ai principi di correttezza e trasparenza, prevedendo nei contratti apposite clausole volte a garantire il rispetto delle normative doganali e tributarie. Le funzioni aziendali competenti devono verificare la regolarità delle dichiarazioni e dei documenti di accompagnamento delle merci, prestando particolare attenzione alla corretta indicazione dell'origine, della natura e del valore dei beni, nonché alla coerenza tra i dati dichiarati e quelli effettivi.

Il rispetto delle procedure interne in materia di approvvigionamenti, gestione contrattuale e verifica documentale rappresenta un presidio fondamentale di prevenzione. Ogni anomalia, incoerenza o segnale di rischio rilevato nella documentazione o nei rapporti con operatori internazionali deve essere tempestivamente segnalato alla Direzione e all'Organismo di Vigilanza, al fine di consentire l'adozione delle necessarie misure di approfondimento e di mitigazione del rischio.

12.3 Flussi informativi da e verso l'Organismo di Vigilanza

L'efficacia del sistema di prevenzione in materia di contrabbando dipende da un flusso informativo costante e completo tra le funzioni aziendali coinvolte e l'Organismo di Vigilanza. Quest'ultimo deve essere informato in modo tempestivo di eventuali criticità, irregolarità o anomalie riscontrate nella gestione dei rapporti con operatori esteri o nella verifica della documentazione doganale.

Le funzioni amministrative, contabili e contrattuali sono tenute a comunicare all'Organismo di Vigilanza ogni situazione che possa far emergere rischi di non conformità, come discrepanze tra i documenti di trasporto e le fatture, incongruenze relative alla provenienza delle merci o rapporti con partner caratterizzati da scarsa trasparenza.

Le risultanze delle verifiche svolte dall'Organismo e le segnalazioni ricevute vengono riportate in apposite relazioni indirizzate al Consiglio di Amministrazione, così da consentire una valutazione continua dell'efficacia del sistema di controllo interno e l'adozione tempestiva di eventuali interventi correttivi.

12.4 Protocollo per le attività di registrazione e preparazione dei dati contabili

Compagnia Siderurgica S.p.A. è strutturata in modo da garantire un sistema di gestione contabile e amministrativa efficiente, tracciabile e conforme alla normativa vigente. L'organizzazione interna prevede l'impiego di risorse informatiche adeguate e di personale qualificato, in grado di assicurare la corretta registrazione, verifica e controllo delle operazioni che possono avere rilievo ai fini doganali e contabili.

La Società intrattiene rapporti codificati e continuativi con spedizionieri e importatori internazionali, normalmente individuati tra soggetti di comprovata affidabilità e già fiduciari dell'azienda. Tali rapporti sono gestiti verificando la completezza e la correttezza della documentazione accompagnatoria, così da garantire la piena conformità delle operazioni ai requisiti doganali e fiscali.

Le fatture, sia di vendita sia di acquisto, vengono registrate in contabilità mediante caricamento a sistema solo dopo un'attenta verifica della correttezza formale e di merito. Particolare attenzione è dedicata ai casi in cui pervengano fatture passive da fornitori non presenti in anagrafica, o fatture emesse da terzi che, per contenuto, importi o natura delle operazioni, si discostino da quanto abitualmente fatturato. In tali circostanze, viene immediatamente effettuata una segnalazione al Chief Financial Officer o a un Amministratore Delegato, affinché siano svolte le opportune verifiche.

È inoltre previsto un controllo puntuale sulla destinazione delle merci, con specifica attenzione ai casi in cui essa risulti localizzata al di fuori dell'Unione Europea, al fine di garantire la corretta gestione delle pratiche doganali e l'adempimento degli obblighi fiscali connessi. A completamento del presidio, la Società esegue verifiche periodiche sulle merci presenti in azienda, al fine di accertare la corrispondenza tra giacenze fisiche e dati contabili e di individuare eventuali anomalie che possano costituire indicatori di rischio.

Tale sistema integrato di controlli, basato sulla collaborazione tra le funzioni amministrative, contabili e logistiche, consente a Compagnia Siderurgica S.p.A. di assicurare la tracciabilità, la trasparenza e la correttezza di tutte le operazioni che possono avere riflessi in materia doganale, fiscale o contabile, costituendo così un presidio concreto e costante di prevenzione rispetto ai reati di contrabbando.

13. Reati ambientali (art. 25-undecies)

La tutela dell'ambiente rappresenta per Compagnia Siderurgica S.p.A. non solo un obbligo giuridico, ma anche un principio etico e un valore identitario che ispira ogni aspetto della propria attività. L'articolo 25-undecies del Decreto Legislativo 231/2001 annovera tra i reati presupposto una serie di condotte che arrecano danno o pericolo per l'ambiente, richiedendo alle imprese l'adozione di modelli organizzativi capaci di prevenirne la commissione.

La Società, certificata secondo lo standard UNI EN ISO 14001, opera in un settore – quello della lavorazione e del taglio delle lamiere – nel quale l'impatto ambientale rappresenta una dimensione significativa. La gestione dei rifiuti metallici e di quelli speciali, il controllo delle emissioni, lo stoccaggio delle sostanze pericolose, la manutenzione degli impianti e la conformità delle autorizzazioni ambientali sono elementi che richiedono un'attenzione costante e una struttura organizzativa in grado di assicurare il pieno rispetto della normativa.

Compagnia Siderurgica S.p.A. adotta procedure interne che garantiscono la tracciabilità delle operazioni, la correttezza formale della documentazione e il rispetto di ogni prescrizione prevista dal Testo Unico Ambientale. La prevenzione dei reati ambientali è integrata nel Modello 231 attraverso un insieme coordinato di responsabilità, controlli e protocolli che consentono di gestire i rischi in modo sistematico e trasparente. L'obiettivo è quello di coniugare lo sviluppo produttivo con la tutela del territorio e della salute, rafforzando la credibilità dell'azienda nei confronti dei clienti, dei partner commerciali e delle istituzioni pubbliche.

13.1 Attività a rischio sensibile

Le attività considerate sensibili ai fini della commissione dei reati ambientali comprendono tutte quelle fasi operative in cui si gestiscono materiali, sostanze o processi che possono determinare, anche indirettamente, un impatto sull'ambiente.

Una prima area di rischio riguarda l'approvvigionamento delle materie prime. Laddove la Società si rifornisca di materiali provenienti da fornitori nazionali o esteri, è necessario verificare che essi operino nel rispetto delle normative ambientali, evitando di alimentare catene di fornitura che implicino la distruzione di habitat naturali o la compromissione di aree protette.

Un secondo ambito di rilievo riguarda la classificazione e la gestione dei rifiuti prodotti durante le lavorazioni meccaniche e termiche. I rifiuti metallici e gli eventuali rifiuti speciali o pericolosi devono essere raccolti, stoccati e smaltiti secondo modalità conformi alla normativa vigente e in collaborazione con soggetti autorizzati. La tenuta dei registri di carico e scarico, la compilazione dei formulari e la conservazione delle relative evidenze documentali rappresentano strumenti essenziali per assicurare la tracciabilità dei flussi e prevenire condotte illecite.

Ulteriori profili di rischio possono emergere dalla gestione delle emissioni convogliate e diffuse, dagli scarichi idrici e dall'uso di impianti e serbatoi interrati. In tali ambiti, la mancata manutenzione o il difetto di controllo possono determinare contaminazioni del suolo o dell'aria. Anche la gestione amministrativa delle autorizzazioni ambientali riveste un ruolo critico, poiché l'omessa richiesta o il ritardo nel rinnovo può comportare violazioni sanzionabili ai sensi del Decreto.

Infine, sono considerate attività sensibili tutte le comunicazioni e gli adempimenti verso le autorità competenti, come la presentazione delle dichiarazioni MUD o le relazioni periodiche sugli scarichi e sulle emissioni. Tali comunicazioni devono essere sempre accurate, veritiere e tempestive, in modo da escludere il rischio di omissioni o falsificazioni.

13.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. considera la tutela dell'ambiente un valore imprescindibile e un elemento di responsabilità sociale. Ogni dipendente e collaboratore è tenuto a contribuire attivamente al mantenimento di elevati standard di sicurezza ambientale, adottando comportamenti corretti e segnalando senza indugio eventuali situazioni di rischio o irregolarità.

È fatto divieto di smaltire rifiuti in modo non autorizzato, di alterare dati ambientali o di trasmettere informazioni non veritiere alle autorità di controllo. Le attività di gestione dei rifiuti, di monitoraggio delle emissioni e di manutenzione degli impianti devono svolgersi nel pieno rispetto delle normative vigenti e delle istruzioni operative aziendali.

La Società ha sviluppato un insieme di procedure interne che disciplinano la gestione dei rifiuti, l'utilizzo delle sostanze pericolose, lo stoccaggio dei materiali e la manutenzione delle apparecchiature. Tutte le attività sono tracciate e documentate, così da consentire controlli successivi e dimostrare la conformità dei comportamenti alle regole ambientali.

Particolare attenzione è dedicata alla scelta dei fornitori e dei trasportatori incaricati dello smaltimento, i quali devono essere in possesso delle autorizzazioni richieste e rispettare standard di affidabilità e trasparenza. Nei contratti di appalto o di fornitura vengono inserite clausole di responsabilità ambientale che prevedono la risoluzione del rapporto in caso di violazione delle norme o dei principi etici della Società.

La prevenzione si fonda anche sulla formazione periodica dei dipendenti coinvolti nei processi a rischio, finalizzata a garantire la conoscenza delle procedure e la consapevolezza delle proprie responsabilità. Le funzioni aziendali competenti effettuano controlli regolari sulla corretta applicazione delle regole interne e sul rispetto delle autorizzazioni ambientali, attivando tempestivamente azioni correttive in caso di criticità.

13.3 Principi generali in materia di ecoreati e rapporto tra Modello 231 e Sistema di Gestione Ambientale

Il Sistema di Gestione Ambientale adottato da Compagnia Siderurgica S.p.A. in conformità alla norma UNI EN ISO 14001 costituisce un presidio organizzativo di primaria importanza per la corretta attuazione del Modello 231.

Il sistema di gestione ambientale e il Modello 231 perseguono finalità diverse ma strettamente interconnesse: il primo organizza e razionalizza i processi aziendali al fine di garantire la conformità normativa e il miglioramento continuo delle prestazioni ambientali, mentre il secondo mira a prevenire la commissione di reati da parte di soggetti che agiscano nell'interesse o a vantaggio della Società.

L'interazione tra i due strumenti consente di rafforzare l'efficacia complessiva dei controlli e di ridurre in modo significativo il rischio di comportamenti illeciti. Le procedure previste dal Sistema di Gestione Ambientale forniscono al Modello 231 elementi tecnici e metodologici per individuare le aree a rischio, definire le responsabilità operative e pianificare gli interventi correttivi. Parallelamente, il Modello 231 garantisce la tracciabilità delle decisioni e la responsabilità individuale di chi opera nei processi a rilevanza ambientale.

13.4 Protocollo per l'acquisto di materie prime

Nel processo di approvvigionamento delle materie prime, Compagnia Siderurgica S.p.A. adotta criteri che tengono conto non solo della qualità dei materiali, ma anche della sostenibilità delle fonti e del rispetto delle normative ambientali da parte dei fornitori.

La selezione dei partner commerciali avviene previa verifica della loro affidabilità e, ove possibile, dell'adozione di sistemi di gestione ambientale. La Società si riserva di interrompere i rapporti con soggetti che risultino coinvolti in pratiche di approvvigionamento non conformi o che non garantiscano la tracciabilità dei materiali forniti.

Queste scelte mirano a promuovere una catena di fornitura trasparente e sostenibile, coerente con i principi di responsabilità ambientale che orientano la gestione aziendale.

13.5 Protocollo per la classificazione e la gestione dei rifiuti

La gestione dei rifiuti rappresenta uno dei principali presidi di prevenzione dei reati ambientali. Compagnia Siderurgica S.p.A. assicura che tutti i rifiuti prodotti, siano essi pericolosi o non pericolosi, siano correttamente classificati, stoccati e smaltiti in conformità alla normativa.

L'obiettivo è garantire la massima protezione della salute umana e dell'ambiente, promuovendo il recupero, il reimpiego e il riciclo dei materiali ove possibile. Ogni fase del ciclo di gestione è accompagnata da controlli documentali e operativi: la compilazione dei registri di carico e scarico e dei formulari di identificazione deve avvenire in modo accurato e veritiero; i documenti devono essere conservati e verificati periodicamente; eventuali irregolarità devono essere immediatamente segnalate alle funzioni competenti e all'Organismo di Vigilanza.

La Società si avvale esclusivamente di imprese autorizzate per il trasporto, il recupero e lo smaltimento dei rifiuti, verificando la validità delle autorizzazioni e il rispetto delle prescrizioni normative. Viene inoltre garantita la compilazione annuale del Modello Unico di Dichiarazione Ambientale e la tracciabilità di tutti i flussi di rifiuti generati.

Attraverso questi presidi, Compagnia Siderurgica S.p.A. assicura la piena conformità alle disposizioni del Testo Unico Ambientale e la costante prevenzione di comportamenti che possano configurare violazioni penalmente rilevanti.

13.6 Flussi informativi da e verso l'Organismo di Vigilanza

Il corretto funzionamento del sistema di prevenzione dei reati ambientali presuppone un flusso informativo continuo e strutturato tra le funzioni aziendali e l'Organismo di Vigilanza. Quest'ultimo deve ricevere regolarmente informazioni sugli adempimenti ambientali, sulle verifiche interne, sulle eventuali prescrizioni ricevute dagli enti di controllo e su ogni criticità riscontrata nella gestione dei rifiuti o degli impianti.

Le segnalazioni devono riguardare anche anomalie documentali, mancate restituzioni di formulari, irregolarità nella tenuta dei registri o sospetti di comportamenti illeciti da parte di fornitori o trasportatori. L'Organismo di Vigilanza, sulla base delle informazioni acquisite, effettua verifiche e propone, ove necessario, azioni correttive o aggiornamenti delle procedure.

Parallelamente, l'OdV mantiene un dialogo costante con il Consiglio di Amministrazione, relazionando periodicamente sull'efficacia dei presidi ambientali e contribuendo al miglioramento del Modello 231. Questo sistema di comunicazione e controllo consente alla Società di garantire la piena tracciabilità delle informazioni, di rafforzare la propria cultura ambientale e di prevenire in modo concreto la commissione dei reati di cui all'art. 25-undecies del Decreto Legislativo 231/2001.

14. Reati tributari (art. 25-quinquiesdecies)

L'inclusione dei reati tributari nel catalogo del D.Lgs. 231/2001 impone a Compagnia Siderurgica S.p.A. un presidio particolarmente rigoroso sulla correttezza fiscale e sulla trasparenza dei rapporti con l'Amministrazione finanziaria. L'obiettivo della Società è che ogni attività connessa alla funzione tributaria—dalla rilevazione contabile delle operazioni alla predisposizione delle dichiarazioni, dalla gestione dei flussi finanziari alla conservazione della documentazione—sia condotta con criteri di veridicità, completezza e tracciabilità, assicurando la piena cooperazione con l'Agenzia delle Entrate, la Guardia di Finanza e gli altri organi preposti ai controlli.

La Società si avvale di professionisti qualificati per la predisposizione e il controllo degli adempimenti fiscali; ciò non esonera l'organizzazione dalle proprie responsabilità, che rimangono in capo agli organi aziendali competenti. Ne discende l'esigenza di garantire la qualità e l'integrità dei dati forniti al consulente, la conservazione ordinata delle evidenze e un sistema di verifiche incrociate che riduca al minimo il rischio di errori materiali o di condotte suscettibili di integrare fattispecie penalmente rilevanti ai sensi dell'art. 25-quinquiesdecies.

14.1 Attività a rischio sensibile

I profili di rischio, per Compagnia Siderurgica S.p.A., si concentrano nelle aree amministrativa, contabile e fiscale. Rilevano, in particolare, la corretta registrazione delle operazioni economiche nei sistemi contabili, la tempestiva e fedele trasmissione dei dati al consulente incaricato della compliance tributaria, la predisposizione delle dichiarazioni e delle comunicazioni periodiche, la gestione dei versamenti e la tenuta delle scritture obbligatorie.

Ulteriori esposizioni derivano dall'uso di documentazione non corretta o incompleta, dall'omessa o irregolare contabilizzazione di componenti di reddito e dall'adozione di prassi non trasparenti nella regolazione di incassi e pagamenti. Delicati sono anche i rapporti con clienti, fornitori e consulenti esterni: informazioni lacunose o operazioni prive di adeguata giustificazione economica e documentale possono tradursi in errori contabili o, nei casi più gravi, in condotte a rilevanza penale. Nei confronti dell'Amministrazione finanziaria e degli organi ispettivi, infine, la Società deve garantire comunicazioni sempre complete, veritiere e tempestive, evitando omissioni o reticenze che possano ostacolare l'attività di controllo.

14.2 Principi di comportamento e presidi di prevenzione

Compagnia Siderurgica S.p.A. considera la correttezza fiscale un dovere inderogabile. Chiunque operi nei processi amministrativi e contabili è tenuto a rispettare i principi di verità, completezza e tracciabilità dei dati, astenendosi da condotte anche solo potenzialmente idonee a violare la normativa tributaria. Le scritture contabili devono rappresentare fedelmente le operazioni e trovare riscontro in giustificativi chiari e verificabili; è vietato predisporre o utilizzare documenti falsi o alterati, ovvero riferiti a operazioni inesistenti, così come è vietato occultare o omettere informazioni rilevanti nei confronti dell'Amministrazione finanziaria.

Gli adempimenti fiscali sono affidati a consulenti abilitati, ai quali gli uffici interni forniscono dati completi e nei tempi stabiliti. La trasmissione delle informazioni al consulente è tracciata e sottoposta a controllo secondo il principio di separazione delle funzioni, in modo che la raccolta dei dati, la loro validazione e l'autorizzazione finale non gravino sulla medesima persona. La Direzione Amministrazione e Finanza cura la conservazione ordinata della documentazione contabile e fiscale, effettua verifiche periodiche di coerenza tra registrazioni e dichiarazioni e presidia il rispetto rigoroso delle scadenze di legge per versamenti e filing. Tali cautele organizzative riducono gli spazi per errori materiali, incongruenze informative o manipolazioni dolose.

14.3 Flussi informativi da e verso l’Organismo di Vigilanza

Per assicurare un presidio effettivo, l’Organismo di Vigilanza riceve con periodicità informazioni sulla gestione fiscale: stato degli adempimenti, dichiarazioni predisposte e presentate, comunicazioni dell’Amministrazione finanziaria, esiti delle verifiche interne e dei controlli eseguiti dai consulenti. Ogni anomalia, anche se già sanata, è comunicata tempestivamente all’OdV, così come l’avvio di accessi, ispezioni o contenziosi tributari.

L’Organismo verifica la regolarità e la completezza dei flussi, può richiedere chiarimenti e documentazione integrativa e, ove necessario, formulare raccomandazioni per l’adeguamento dei presidi interni. Questo circuito informativo consente un monitoraggio continuativo e contribuisce a prevenire condotte irregolari potenzialmente rilevanti ai sensi del D.Lgs. 231/2001.

14.4 Protocollo per le attività di registrazione e preparazione dei dati contabili

Compagnia Siderurgica S.p.A. è organizzata, sotto il profilo informatico e delle risorse umane, per assicurare una gestione contabile affidabile, tracciabile e conforme. In questo quadro, le fatture di vendita e di acquisto sono registrate a sistema solo dopo la verifica della correttezza formale e sostanziale del documento; l’ufficio amministrativo effettua controlli per intercettare eventuali duplicazioni di registrazioni e, quando pervengono fatture passive da fornitori non presenti in anagrafica o documenti che si discostano per contenuto, importi o tipologia dalle ordinarie forniture, procede a una segnalazione immediata al Chief Financial Officer o a un Amministratore Delegato, così da attivare le verifiche di merito.

Il sistema prevede, inoltre, controlli orientati a individuare importi anomali o non congrui, con obbligo di escalation alla funzione finance o alla Direzione. La contabilizzazione e il pagamento di poste passive avvengono soltanto dopo specifica approvazione degli organi competenti (di regola un Amministratore Delegato o, a seconda dei casi, il CFO), limitando autorizzazioni “una tantum” o generalizzate che coprano più operazioni. La creazione o la modifica dei conti contabili richiede un’autorizzazione preventiva del CFO; l’imputazione dei costi segue prassi e criteri uniformi, definiti in procedure interne.

La documentazione contabile è archiviata in modo da garantire integrità, reperibilità e tracciabilità delle informazioni. La conservazione avviene secondo misure organizzative e tecniche coerenti con il Regolamento (UE) 2016/679, riducendo al minimo il rischio di perdita, distruzione o alterazione dei documenti e assicurando la disponibilità delle evidenze a supporto delle dichiarazioni fiscali e dei controlli interni ed esterni.

Con questo protocollo operativo—fondato su verifiche ex ante, segregazione dei compiti, autorizzazioni formalizzate e tracciabilità completa—la Società presidia i punti di rischio tipici dei processi contabili e fiscali, rafforzando la prevenzione delle fattispecie rilevanti ai sensi dell’art. 25-quinquiesdecies.

15. Tabella riassuntiva protocolli, flussi, responsabili e frequenze

Il presente schema ha valore puramente esemplificativo e di sintesi. Esso riassume alcuni dei flussi informativi verso l'Organismo di Vigilanza e le funzioni aziendali coinvolte o responsabili della loro attuazione. Le informazioni qui riportate non sostituiscono le specifiche indicazioni contenute nella Parte Speciale del Modello 231, dove ciascuna macro-area di rischio e di vigilanza è descritta in modo analitico. Il documento intende fornire un quadro di riferimento operativo per l'OdV, agevolando le attività di controllo e di pianificazione delle verifiche periodiche.

Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Aggiornamento normativo SSL	Rendicontazione sulle novità legislative e aggiornamenti di DVR o procedure adottati per adeguamento	RSPP	Periodica (almeno semestrale) o immediata in caso di novità rilevanti
Documento di Valutazione dei Rischi (DVR)	Copia o estratto del DVR aggiornato, motivazione dell'aggiornamento, sottoscrizioni DL-RSPP-MC-RLS	Datore di Lavoro / RSPP	Annuale e in caso di aggiornamento
Dispositivi di Protezione Individuale (DPI)	Evidenze di consegna, sostituzioni, segnalazioni di guasti o non conformità	Datore di Lavoro / RSPP / Preposti	Periodica (semestrale) e immediata per criticità
Piano di emergenza e prove di evacuazione	Piano aggiornato ed esito delle prove di evacuazione (verbali)	RSPP	Annuale e in caso di aggiornamento del Piano
Riunione periodica ex art. 35 D.Lgs. 81/08	Verbale della riunione, programma di miglioramento con priorità e tempi di attuazione	RSPP	Annuale o in occasione di variazioni organizzative/normative
Consultazione RLS	Evidenze di consultazioni su DVR, DPI e iniziative di sicurezza	RSPP / Datore di Lavoro	Periodica (almeno semestrale)
Sorveglianza sanitaria	Dati aggregati sulle idoneità e sopralluoghi del MC (senza dati sanitari personali)	Medico Competente / RSPP	Annuale (in occasione della riunione periodica)
Formazione e informazione dei lavoratori	Elenco corsi erogati, attestati, aggiornamenti formativi	RSPP	Periodica (almeno semestrale)
Infortuni e near miss	Segnalazioni, registrazioni, analisi delle cause, azioni correttive e comunicazioni all'INAIL	RSPP / Preposti	Immediata in caso di evento, riepilogo semestrale per l'OdV
Manutenzioni e controlli periodici	Piano e Registro delle manutenzioni, registro antincendio, eventuali criticità rilevate	RSPP / Preposti	Periodica (semestrale) e immediata per anomalie rilevanti
Rapporti con fornitori e appaltatori	Verifica idoneità tecnico-professionale, DUVRI, verbali di coordinamento	Datore di Lavoro / RSPP	Prima dell'avvio lavori e aggiornamento al variare delle condizioni operative

Parte Speciale

Cantieri (Titolo IV TUS)	PSC, POS, verbali CSE/CSP, eventuali non conformità	Datore di Lavoro / RSPP	Periodica (durata lavori) e immediata per criticità
Verifiche su procedure e istruzioni di lavoro	Esiti di controlli, check-list, audit interni, non conformità e azioni correttive	RSPP / Preposti	Continuamente e riepilogo semestrale
Eventi, segnalazioni e informazioni rilevanti ai fini 231	Segnalazioni violazioni, esiti audit, contestazioni disciplinari, comunicazioni con autorità, infortuni rilevanti	Datore di Lavoro / RSPP / Preposti / RLS / Medico Competente	Periodica (almeno semestrale) e immediata per fatti di rilievo
Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Autorizzazioni, licenze, permessi e certificazioni	Copia delle istanze, domande o comunicazioni inviate a enti pubblici e degli atti di rilascio/rinnovo; eventuali prescrizioni o verbali ricevuti	Datore di Lavoro / RSPP	Immediata in caso di richiesta o rilascio; riepilogo semestrale
Partecipazione a gare o bandi pubblici	Elenco gare/bandi, ruolo assunto, condizioni economiche e principali documenti trasmessi	Amministratore Delegato / Ufficio Commerciale	Ogni nuova procedura; riepilogo semestrale
Ispezioni, sopralluoghi, verifiche o controlli di enti pubblici (ASL, ARPA, INAIL, ecc.)	Comunicazione dell'avvio dell'ispezione, copia dei verbali e delle eventuali prescrizioni o osservazioni	Datore di Lavoro / RSPP	Immediata (entro 48 ore dall'ispezione o ricezione del verbale)
Procedimenti giudiziari o amministrativi	Notifica dell'avvio di procedimenti o accertamenti che coinvolgano la società o suoi esponenti; atti principali	Amministratore Delegato / Direzione	Immediata al momento della notifica
Rapporti o contatti con ex funzionari pubblici o soggetti in potenziale conflitto di interessi	Comunicazione scritta con descrizione del rapporto o dell'incarico	Amministratore Delegato	Immediata al momento dell'instaurazione del rapporto
Segnalazioni o irregolarità nei rapporti con la Pubblica Amministrazione	Descrizione di anomalie, violazioni o criticità anche prive di rilievo disciplinare	Qualsiasi dipendente o dirigente, tramite Datore di Lavoro o OdV	Immediata
Delega e procure	Elenco aggiornato delle deleghe conferite per la gestione dei rapporti con la PA; eventuali modifiche o revoche	Datore di Lavoro / Direzione	Aggiornamento tempestivo e comunque riepilogo semestrale
Programmi di formazione su reati contro la PA	Report su corsi effettuati, presenze e materiali formativi;	Datore di Lavoro / RSPP / OdV	Annuale

Parte Speciale

	eventuali revisioni dei programmi		
Adempimenti verso enti pubblici in materia di sicurezza e igiene del lavoro (D.Lgs. 81/08)	Comunicazioni, certificazioni o pratiche inviate alle autorità competenti (es. prevenzione incendi, ASL, INAIL)	Datore di Lavoro / RSPP	Immediata per ogni nuova pratica o rinnovo
Assunzione di personale appartenente a categorie protette o soggetto ad agevolazioni pubbliche	Documentazione relativa all'assunzione, pratiche di agevolazione e autorizzazioni rilasciate	Amministratore Delegato (poiché non esiste HR interno)	Ogni pratica completata
Verifiche e controlli ispettivi da parte di enti pubblici	Copia richieste di informazioni, verbali di ispezione e note conclusive	Datore di Lavoro / Amministratore Delegato	Immediata dopo la visita ispettiva
Acquisizione e gestione di contributi o finanziamenti pubblici	Copia domande, comunicazioni, delibere di concessione e rendicontazioni	Amministratore Delegato / Consiglio di Amministrazione	Immediata all'avvio e al termine della procedura
Omaggi o liberalità verso funzionari pubblici	Autorizzazioni concesse e motivazioni dell'omaggio o liberalità	Amministratore Delegato / Direzione	Immediata
Partecipazione a gare, appalti o procedure di aggiudicazione pubblica	Documentazione di gara, verbali, contratti aggiudicati e corrispondenza con enti pubblici	Amministratore Delegato / Ufficio Commerciale (se esistente)	Immediata per ogni procedura; riepilogo semestrale
Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Bilancio e scritture contabili	Copia del bilancio approvato, segnalazione di eventuali rilievi del revisore o anomalie contabili	Amministratore Delegato / Consiglio di Amministrazione	Annuale, dopo l'approvazione del bilancio
Operazioni straordinarie o societarie rilevanti	Informativa su fusioni, scissioni, modifiche statutarie o variazioni nella compagine sociale	Amministratore Delegato	Immediata al momento della delibera o progetto
Conflitti di interesse e operazioni con parti correlate	Comunicazione di eventuali situazioni di conflitto o operazioni con soggetti collegati	Amministratore Delegato / Membri del CdA	Immediata, non appena nota la situazione

Parte Speciale

Nomine e deleghe societarie	Elenco aggiornato di procure e deleghe operative con eventuali modifiche o revoche	Consiglio di Amministrazione / Amministratore Delegato	Aggiornamento tempestivo e riepilogo semestrale
Relazioni con organi di controllo	Copia di eventuali comunicazioni o verbali con revisore legale o organi di controllo esterni	Amministratore Delegato	Immediata in caso di rilievi o segnalazioni
Segnalazioni interne o irregolarità contabili	Informazioni su anomalie, errori o comportamenti difforni dalle procedure amministrativo-contabili	Amministratore Delegato / Personale amministrativo	Immediata per fatti rilevanti; riepilogo semestrale
Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Autorizzazioni ambientali (emissioni, scarichi, rifiuti)	Copia delle autorizzazioni ambientali, dei rinnovi e delle eventuali prescrizioni o comunicazioni ricevute dagli enti competenti	Datore di Lavoro / Responsabile sistema ambientale	Immediata in caso di rilascio o rinnovo; riepilogo semestrale
Gestione rifiuti e registri ambientali	Riepilogo quantitativo annuale rifiuti, formulari, MUD e tracciabilità; eventuali non conformità riscontrate	RSPP / Responsabile sistema ambientale	Annuale (in coincidenza con la dichiarazione MUD) e immediata per irregolarità
Controlli e ispezioni ambientali (ARPA, Provincia, ecc.)	Comunicazione dell'avvio dell'ispezione, copia del verbale, prescrizioni e azioni correttive adottate	Datore di Lavoro / Responsabile sistema ambientale	Immediata entro 48 ore dall'ispezione
Emergenze ambientali o incidenti (sversamenti, dispersioni, ecc.)	Segnalazione dell'evento, cause, misure di contenimento e prevenzione futura	RSPP / Datore di Lavoro	Immediata (entro 24 ore dall'evento)
Audit interni ed esterni ISO 14001	Esiti degli audit ambientali, non conformità, azioni correttive e stato di avanzamento	Responsabile sistema ambientale	Periodica (almeno annuale)
Formazione e sensibilizzazione ambientale	Evidenze della formazione periodica in materia ambientale e aggiornamenti del personale	Responsabile sistema ambientale	Annuale
Segnalazioni di non conformità o anomalie ambientali	Descrizione delle criticità rilevate e misure adottate per la risoluzione	Responsabile sistema ambientale	Immediata e riepilogo semestrale

Parte Speciale

Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Gestione della qualità del prodotto e delle certificazioni	Segnalazione di non conformità di prodotto, reclami di clienti o contestazioni relative alla qualità o conformità	Responsabile Qualità	Immediata per eventi rilevanti; riepilogo semestrale
Utilizzo di marchi, loghi e segni distintivi	Comunicazione di nuove registrazioni, modifiche o contestazioni su marchi e denominazioni aziendali	Direzione / Amministratore Delegato	Immediata in caso di variazione o contenzioso
Pubblicità, comunicazioni e presentazioni commerciali	Verifica preventiva o successiva di eventuali comunicazioni commerciali o promozionali verso clienti e terzi	Amministratore Delegato	Periodica o al verificarsi dell'evento
Contenziosi o reclami per prodotti non conformi	Documentazione relativa a richieste di risarcimento o segnalazioni di danni da prodotto difettoso	Amministratore Delegato	Immediata alla ricezione
Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Operazioni economiche e finanziarie anomale	Comunicazione di operazioni di pagamento o incasso non usuali per importo, modalità o provenienza	Amministratore Delegato / Ufficio Amministrativo	Immediata, appena rilevata l'anomalia
Gestione rapporti con istituti bancari e finanziari	Elenco dei conti correnti attivi, variazioni dei referenti bancari o condizioni particolari applicate	Amministratore Delegato	Annuale o al momento di variazione rilevante
Pagamenti a fornitori e incassi da clienti	Segnalazione di pagamenti o incassi in contanti, su conti esteri o verso soggetti non abituali	Ufficio Amministrativo / Amministratore Delegato	Immediata per operazioni anomale; riepilogo semestrale
Rapporti con consulenti o intermediari	Elenco aggiornato di consulenti o intermediari coinvolti in operazioni economiche; verifica compensi e regolarità contrattuale	Amministratore Delegato	Annuale e in caso di nuovi incarichi
Segnalazioni di operazioni sospette	Comunicazioni interne su situazioni potenzialmente illecite o a rischio di riciclaggio	Qualsiasi dipendente tramite Amministratore Delegato o OdV	Immediata, tramite canale riservato

Parte Speciale

Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Violazioni o incidenti informatici	Segnalazione di accessi non autorizzati, tentativi di intrusione, perdita o compromissione di dati aziendali	Direzione / Personale amministrativo (referente informativo)	Immediata al rilevamento dell'evento
Eventuali violazioni dei dati personali (data breach)	Descrizione dell'evento, categorie di dati coinvolti e misure correttive adottate	Direzione / Personale amministrativo (referente informativo)	Immediata (entro 24 ore dalla conoscenza del fatto)
Gestione e aggiornamento delle utenze	Elenco aggiornato degli account attivi, modifiche o revocche di credenziali e profili di accesso	Direzione / Personale amministrativo (referente informativo)	Trimestrale
Interventi tecnici e manutenzioni straordinarie	Comunicazione degli interventi effettuati sui server o postazioni, con nominativi dei tecnici intervenuti	Direzione / Personale amministrativo (referente informativo)	Immediata in caso di interventi straordinari
Comportamenti anomali nell'uso dei sistemi aziendali	Segnalazioni relative a utilizzi impropri dei sistemi informatici o accessi non autorizzati a dati aziendali	Direzione / Personale amministrativo (referente informativo)	Immediata
Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Segnalazioni di comportamenti lesivi della dignità personale o discriminatori	Comunicazioni relative a molestie, abusi, comportamenti vessatori o discriminatori sul luogo di lavoro	Direzione / Personale dipendente tramite canale dedicato OdV	Immediata alla ricezione o conoscenza
Provvedimenti disciplinari o contestazioni rilevanti	Copia dei provvedimenti disciplinari emessi per condotte lesive della persona o violazioni del Codice Etico	Direzione	Semestrale
Attività formative e informative sul rispetto della dignità e dei diritti della persona	Elenco corsi svolti e materiale formativo relativo a etica, rispetto interpersonale e tutela dei lavoratori	Direzione	Annuale
Segnalazioni o indagini interne su comportamenti scorretti	Esito di eventuali verifiche interne o azioni correttive	Direzione	Immediata alla conclusione dell'indagine

Parte Speciale

	adottate per prevenire o reprimere condotte lesive		
Coinvolgimento delle autorità in procedimenti penali o civili	Comunicazione di eventuali procedimenti giudiziari riguardanti violazioni della libertà o dignità dei lavoratori	Direzione	Immediata alla notifica dell'atto
Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Verifiche su nuovi fornitori o clienti	Comunicazione delle verifiche effettuate sull'affidabilità e provenienza dei partner commerciali (es. visure, blacklist, anomalie nei rapporti)	Direzione / Amministrazione	Immediata in caso di nuove collaborazioni o criticità riscontrate
Operazioni economiche o commerciali anomale	Segnalazione di operazioni di acquisto, vendita o pagamento sospette per importo, modalità o controparti	Amministrazione / Direzione	Immediata al rilevamento; riepilogo semestrale
Rapporti con intermediari o soggetti terzi non abituali	Comunicazione di incarichi a soggetti esterni non ricorrenti o operanti in aree a rischio	Direzione	Immediata alla stipula dell'incarico
Contenziosi o indagini connesse a ipotesi di riciclaggio o criminalità organizzata	Informazione sull'avvio di indagini, richieste delle autorità o segnalazioni da organi investigativi	Direzione	Immediata alla ricezione
Segnalazioni interne di operazioni sospette	Comunicazioni riservate relative a condotte o transazioni potenzialmente riconducibili a riciclaggio o intermediazioni illecite	Qualsiasi dipendente, tramite canale OdV	Immediata tramite canale riservato
Controlli periodici sull'integrità dei rapporti commerciali	Sintesi delle verifiche periodiche sull'affidabilità di clienti e fornitori	Amministrazione	Annuale
Argomento / Documento	Contenuto del flusso verso l'OdV	Funzione interna che trasmette	Tempistiche
Procedimenti giudiziari o amministrativi	Comunicazione dell'avvio di indagini, procedimenti o richieste da parte dell'autorità giudiziaria che coinvolgano la società o suoi esponenti	Direzione / Amministratore Delegato	Immediata alla notifica o conoscenza dell'atto
Richieste di informazioni o documentazione da	Copia delle richieste ricevute e delle risposte fornite, con	Direzione	Immediata

Parte Speciale

parte di autorità giudiziarie	indicazione del soggetto che ha gestito la pratica		
Eventuali rapporti con soggetti coinvolti in procedimenti giudiziari	Comunicazione di contatti o collaborazioni con persone sottoposte a indagine o condanna	Direzione	Immediata alla conoscenza del fatto
Segnalazioni di possibili pressioni o influenze indebite	Comunicazioni relative a tentativi di condizionare dichiarazioni o testimonianze in procedimenti che riguardano la società	Direzione / Qualsiasi dipendente tramite OdV	Immediata tramite canale riservato
Azioni correttive o informative conseguenti a procedimenti	Sintesi delle misure organizzative o procedurali adottate a seguito di procedimenti giudiziari o ispezioni	Direzione	Immediata dopo la definizione del procedimento o nel riepilogo semestrale