Parte Specifica A, B, C, D, E

La Fabbrica di Lampadine Srl

Viale Sarca 96, 20126 Milano
Via Pescantina 8, 20162 Milano
www.fabbricadilampadine.it
formazione@fabbricadilampadine.it

Sommario

Parte speciale A

Reati contro la Pubblica Ammnistrazione

I reati contro la Pubblica Amministrazione richiamati dall'art. 24 del Decreto, ed applicabili alle attività di La Fabbrica di Lampadine sono i seguenti:

Reati in tema di erogazioni pubbliche

1. Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)
2. Indebita percezione di erogazioni a danno dello Stato (art 316-ter c.p.)
3. Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)

Truffa aggravata ai danni dello Stato

4. Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, comma 2, n. 1, c.p.)

Frode informatica ai danni dello Stato

5. Frode informatica in danno dello Stato e di altro Ente Pubblico (art. 640-ter c.p.)

Corruzione e concussione

6. Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318, 319 e 319-bis c.p.)
7. Corruzione in atti giudiziari (art 319-ter c.p.)
8. Corruzione di persona incaricata di un pubblico servizio (art 320 c.p.)
9. Pene per il corruttore (art. 321 c.p.)
10. Istigazione alla corruzione (art. 322 c.p.)

Processi a rischio reati

Secondo quanto stabilito nella Parte Generale, i processi, i processi a rischio reati contro la Pubblica Amministrazione sono:

Processi principali	Processi di supporto
Reati in tema di erogazioni pubbliche/Truffa aggravata ai danni dello Stato	
• Servizi per l'orientamento formativo: organizzazione ed erogazione • Servizi formativi: progettazione, organizzazione ed erogazione	• Gestione della documentazione: identificazione, rintracciabilità, rintracciabilità, conservazione • Selezione e valutazione dei fornitori – Approvvigionamento • Gestione della contabilità e degli adempimenti normativi • Rendicontazione delle spese • Gestione amministrativa del personale • Controllo di gestione
Frode informatica ai danni dello Stato	
• Servizi per l'orientamento formativo: organizzazione ed erogazione • Servizi formativi: progettazione, organizzazione ed erogazione	• Gestione della documentazione: identificazione, rintracciabilità, rintracciabilità, conservazione • Selezione e valutazione dei fornitori – Approvvigionamento • Gestione della contabilità e degli adempimenti normativi • Rendicontazione delle spese • Gestione amministrativa del personale • Controllo di gestione
Corruzione e concussione	
• Servizi per l'orientamento formativo: organizzazione ed erogazione • Servizi formativi: progettazione, organizzazione ed erogazione	• Gestione della documentazione: identificazione, rintracciabilità, rintracciabilità, conservazione • Selezione e valutazione dei fornitori – Approvvigionamento • Gestione della contabilità e degli adempimenti normativi • Rendicontazione delle spese • Gestione amministrativa del personale • Controllo di gestione

Aree a rischio reati

Secondo quanto stabili to nella Parte Generale, le aree a rischio reati contro la Pubblica Amministrazione sono:

Reati in temi di erogazioni pubbliche	DG – Form. – Amm.
Truffa aggravata ai danni dello Stato	DG
Frode informatica ai danni dello Stato	IT
Corruzione e concussione	**DG – Form. – Amm**

Attività a rischio reati

Le attività considerate a rischio reato contro la Pubblica Amministrazione sono le seguenti:

- Processo di accreditamento presso la Regione Lombardia: requisiti giuridici, finanziari di onorabilità, certificazione UNI ENI ISO 9001, capacità logistica e gestionale, disponibilità di competenze professionali, relazioni con il territorio; Gestione del processo di rendicontazione nei confronti della Pubblica Amministrazione; Gestione della produzione di documenti per l'ottenimento di autorizzazioni, licenze, permessi da parte della Pubblica Amministrazione.
- Gestione delle attività relative all'invio della documentazione mediante il sistema telematico della Regione Lombardia.
- Gestione delle visite ispettive effettuate dalla Regione Lombardia per la verifica del mantenimento dei requisiti previsti per l'accreditamento; Gestione dei rapporti con le autorità di vigilanza; Gestione delle forniture da parte di Enti Pubblici.

Protocolli di prevenzione e controllo

Sulla base della valutazione di rischio reato, dei processi, aree e attività sensibili vengono individuati i protocolli riportati di seguito:

Reati in temi di erogazioni pubbliche e Truffa aggravata ai danni dello Stato	- Esplicita indicazione nel Codice Etico di specifiche regole di condotta nei confronti della Pubblica Amministrazione - Diffusione del Codice Etico verso tutti i dipendenti ed i collaboratori esterni - Definizione del mansionario e della struttura organizzativa relativi al processo di accreditamento, ottenimento autorizzazioni, licenze, permessi da parte della Pubblica Amministrazione - Coerenza tra le procure verso l'esterno ed il sistema di responsabilità interne - Separazione funzionale tra chi gestisce l'erogazione dei servizi, che predispone e chi approva la documentazione attestante lo stato di avanzamento delle attività - Definizione ed applicazione di procedure organizzative (Sistema Qualità) relative a: gestione offerte e ordini, gestione attività di segreteria, controllo della progettazione ed erogazione dei servizi formativi, valutazione delle competenze del personale, selezione e valutazione dei fornitori, gestione acquisti, gestione della contabilità e degli adempimenti normativi, gestione della documentazione, trattamento dei dati nel rispetto della privacy - Definizione di un sistema di auditing interno atto a monitorare la corretta applicazione dei protocolli
Frode informatica ai danni dello Stato	- Definizione di un sistema di controlli interno che, ai fini del corretto e legittimo accesso ai sistemi informativi della Pubblica Amministrazione preveda: un adeguato riscontro delle Password di abilitazione all'accesso al sistema informativo della Regione, possedute per ragioni di servizio da ben indicati dipendenti appartenenti a specifiche aree; la puntuale verifica da parte dei dipendenti delle ulteriori misure di sicurezza adottate. - Definizione di un sistema di auditing interno atto a monitorare la corretta applicazione dei protocolli

Corruzione e concussione	- Esplicita indicazione nel Codice Etico del divieto di pratiche corruttive, che i rapporti nei confronti della Pubblica Amministrazione debbano essere improntati alla massima trasparenza, correttezza e collaborazione. - Diffusione del Codice Etico verso tutti i dipendenti ed i collaboratori esterni. - Definizione del mansionario e della struttura organizzativa relativi al processo di accreditamento, ottenimento autorizzazioni, licenza, permessi da parte della Pubblica Amministrazione. - Definizione di un sistema di auditing interno atto a monitorare la corretta applicazione dei protocolli

Analisi del rischio residuo-rischio accettabile

Nella tabella che segue è riportata la valutazione dell'efficacia dei protocolli di prevenzione e delle procedure organizzative.

Reati in tema di erogazioni pubbliche	Valore del rischio	Efficacia dei protocolli	Rischio residuo	Accettabilità del rischio residuo
1 Malversazione a danno dello Stato o dell'Unione Europea	12	5	2,4	Riesame OdV
2 Indebita percezione di erogazioni a danno dello Stato	6	5	1,2	Riesame OdV
9 Truffa aggravata per il conseguimento di erogazioni pubbliche	18	5	3,6	Riesame OdV
Truffa aggravata ai danni dello Stato				
4 Truffa in danno dello Stato o di altro Ente Pubblico	12	5	2,4	Riesame OdV
Frode informatica ai danni dello Stato				
5 Frode informatica ai danni dello Stato e di altro Ente Pubblico	6	10	0,6	Si
Corruzione e concussione				
6 Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio	6	10	0,6	Si
9 Corruzione in atti giudiziari	3	10	0,3	Si
8 Corruzione di persona incaricata di un pubblico servizio	6	10	0,6	Si
9 Pene per il corruttore	6	10	0,6	Si
10 Istigazione alla corruzione	4	10	0,4	Si

Tenendo conto che i protocolli di prevenzione e controllo previsti dal Modello sono tuti quelli implementabili senza creare intralcio al flusso delle attività; che è prevista una adeguata formazione del personale; che sono previste attività di monitoraggio sulla reale applicazione dei protocolli, l'Organismo di vigilanza ritiene che il rischio residuo relativo ai reati in tema di erogazioni pubbliche e truffa aggravata ai danni dello Stato sia accettabile in quanto il Modello garantisce ragionevolmente di non poter essere eluso se non fraudolentemente.

Parte speciale B

Reati societari

I reati societari richiamati dall'art. 25-ter del D. Lgs 231/01 ed applicabili alle attività di La Fabbrica di Lampadine sono i seguenti:

1. False comunicazioni sociali (art. 2621 c.c.)
2. False comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.)
3. Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624, commi 1 e 2, c.c.)
4. Impedito controllo (art. 2625, comma 2, c.c.)
5. Formazione fittizia del capitale (art. 2632 c.c.)
6. Indebita restituzione di conferimenti (art. 2626 c.c.)
7. Illegale ripartizione degli utili e delle riserve (art 2629 c.c.)
8. Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
9. Operazioni in pregiudizio ai creditori (art. 2629 c.c.)
10. Indebita ripartizione dei beni sociali da parte dei liquidatori (art 2633 c.c.)
11. Illecita influenza sull'assemblea (art. 2636 c.c.)
12. Aggiotaggio (art. 2639 c.c.)
13. Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.)
14. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 commi 1 e 2, c.c.)

Il grado di esposizione al rischio

In conformità alla metodologia per il calcolo del rischio reato descritta, per i reati societari sono stati calcolati i rischi riportati nella tabella seguente:

Reato presupposto	Grado di gravità	Tasso di frequenza	Valutazione impatto	Valore del rischio	Necessità protocollo
False comunicazioni sociali	2	1	3	6	Si
False comunicazioni sociali in danno dei soci o dei creditori	2	1	3	6	Si
Falsità nelle relazioni o nelle comunicazioni delle società di revisione	3	1	2	6	Si
Impedito controllo	2	1	2	4	Si
Formazione fittizia del capitale	2	1	1	2	Si
Indebita restituzione di conferimenti	2	1	1	2	Si
Illegale ripartizione degli utili e delle riserve	2	1	1	2	Si
Illecite operazioni sulle azioni o quote sociali o della società controllante	2	1	1	2	Si
Operazioni in pregiudizio ai creditori	3	2	1	6	Si
Indebita ripartizione dei beni sociali da parte dei liquidatori	3	1	1	3	Si
Illecita influenza sull'assemblea	2	1	1	2	Si
Aggiotaggio	3	1	1	3	Si
Omessa comunicazione del conflitto d'interessi	3	2	1	5	Si
Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	3	1	2	6	Si

Processi a rischio

Secondo quanto stabilito nella Parte Generale, i processi a rischio reati societari sono i processi di supporto, ovvero:

- Gestione della documentazione: identificazione, rintracciabilità, rintracciabilità, conservazione
- Selezione e valutazione dei fornitori – Approvvigionamento
- Gestione della contabilità e degli adempimenti normativi
- Rendicontazione delle spese

- Gestione amministrativa del personale
- Controllo di gestione

Aree a rischio

Secondo quanto stabilito nella Parte Generale, le aree a rischio reati sono:

- Direzione generale
- Amministrazione
- IT

Attività a rischio

Le attività considerate a rischio reati societari sono le seguenti:

- Processo di redazione de approvazione dei documenti contabili societari
- Processo di redazione ed approvazione dei bilanci, relazioni e comunicazioni sociali
- Processo di approvvigionamento e pagamento delle forniture

Protocolli di prevenzione e controllo

Sulla valutazione di rischio reato, dei processi, aree e attività sensibili vengono individuati i protocolli seguenti:

- Inserimento nel Codice Etico di specifiche indicazioni riguardanti il comportamento di tutti i soggetti coinvolti nelle attività del bilancio e delle relazioni e comunicazioni societarie;
- Diffusione del Codice Etico verso tutti i soggetti interessati alla redazione del bilancio e delle relazioni e comunicazioni societarie;
- Inserimento nello Statuto delle metodologie di Corporate Governance;
- Proceduralizzazione dell'informativa al Consiglio per l'esame e l'approvazione del bilancio e delle relazioni e comunicazioni societarie
- Definizione di un sistema di auditing interno sull'Amministrazione atto a monitorare le attività di bilancio e delle relazioni e comunicazioni societarie.

Analisi del rischio residuo-rischio accettabile

Nella tabella che segue è riportata la valutazione dell'efficacia dei protocolli di prevenzione e delle procedure organizzative:

	Valore del rischio	Efficacia dei protocolli	Rischio residuo	Accettabilità del rischio residuo
False comunicazioni sociali	6	10	0,6	Si
False comunicazioni sociali in danno dei soci o dei creditori	6	10	0,6	Si
Falsità nelle relazioni o nelle comunicazioni delle società di revisione	6	10	0,6	Si
Impedito controllo	4	10	0,4	Si
Formazione fittizia del capitale	2	10	0,2	Si
Indebita restituzione di conferimenti	2	10	0,2	Si
Illegale ripartizione degli utili e delle riserve	2	10	0,2	Si
Illecite operazioni sulle azioni o quote sociali o della società controllante	2	10	0,2	Si
Operazioni in pregiudizio ai creditori	6	10	0,6	Si
Indebita ripartizione dei beni sociali da parte dei liquidatori	3	10	0,3	Si
Illecita influenza sull'assemblea	2	10	0,2	Si
Aggiotaggio	3	10	0,3	Si
Omessa comunicazione del conflitto d'interessi	6	10	0,6	Si
Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	6	10	0,6	Si

Parte speciale C

Reati informatici

I reati informatici e trattamento illecito dei dati richiamati dall'art. 24 bis del Decreto ed applicabili alle attività di La Fabbrica di Lampadine sono i seguenti:

1. Accesso abusivo a un sistema informatico o telematico (art 615-ter c.p.)
2. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art 615-quarter c.p.)
3. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
4. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art 619-quinquies c.p.)
5. Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art 619-quinquies c.p.)
6. Danneggiamento di informazioni, dati e programmi informatici (art 635-bis c.p.)
7. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art 635-ter c.p.)
8. Danneggiamento di sistemi informatici e telematici (art 35-quater c.p.)
9. Danneggiamento di sistemi informatici e telematici di pubblica utilità (art 635-quinquies c.p.)
10. Frode informatica che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)

Grado di esposizione a rischio reati

In conformità alla metodologia per il calcolo del rischio reato descritta nella Parte Generale, per i reati informatici sono stati calcolati i rischi riportati nella tabella seguente:

Reato presupposto	Grado di gravità	Tasso di frequenza	Valutazione impatto	Valore del rischio	Necessità protocollo
Accesso abusivo a un sistema informatico o telematico	3	3	1	9	Si
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	2	1	1	2	Si
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (	2	1	1	2	Si
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	2	1	1	2	Si
Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche	2	1	1	2	Si
Danneggiamento di informazioni, dati e programmi informatici	3	1	1	3	Si
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità	3	2	2	12	Si
Danneggiamento di sistemi informatici e telematici	3	1	1	3	Si
Danneggiamento di sistemi informatici e telematici di pubblica utilità	3	1	2	6	Si
Frode informatica che presta servizi di certificazione di firma elettronica	3	2	2	12	Si

Processi a rischio reati

Secondo quanto stabilito nella Parte Generale, i processi a rischio reati informatici sono:

Processi principali	Processi di supporto
• Servizi per l'orientamento formativo: organizzazione ed erogazione • Servizi formativi: progettazione, organizzazione ed erogazione	• Gestione della contabilità e degli adempimenti normativi • Rendicontazione delle spese •

Aree a rischio

Secondo quanto stabilito nella Parte Generale, le aree a rischio reati informatici sono:

- Direzione Generale
- Formazione
- Amministrazione
- IT

Attività a rischio

Le attività considerate a rischio reati informatici sono le seguenti:

- Inserimento dati per l'accreditamento presso la regione Lombardia o i fondi interprofessionali
- Inserimenti dati relativi all'erogazione di servizi di orientamento e formativi finanziati
- Inserimento dati relativi al processo di rendicontazione nei confronti della Pubblica Amministrazione
- Gestione della produzione di documenti per l'ottenimento di autorizzazioni, licenze, permessi da parte della Pubblica Amministrazione
- Utilizzo del sistema informativo per le attività di erogazione dei servizi di orientamento e formativi

Protocolli di prevenzione e controllo

Sulla base della valutazione di rischio reato, dei processi, aree e attività sensibili vengono individuati i protocolli di protezione seguenti:

- Esplicita indicazione nel Codice Etico di specifiche regole di condotta
- Diffusione del Codice Etico verso tutti i dipendenti ed i collaboratori esterni
- Nomina dell'Amministratore del Sistema Informativo
- Definizione ed applicazione di procedure organizzative relative all'utilizzo del sistema informativo e di comunicazione
- Definizione di un sistema di auditing interno atto a monitorare la corretta applicazione dei protocolli

Analisi del rischio residuo – rischio accettabile

Nella tabella che segue è riportata la valutazione dell'efficacia dei protocolli di prevenzione e delle procedure organizzative:

	Valore del rischio	Efficacia dei protocolli	Rischio residuo	Accettabilità del rischio residuo
Accesso abusivo a un sistema informatico o telematico	9	5	1,8	Riesame OdV
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	2	5	0,4	Si
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (	2	10	0,2	Si
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	2	10	0,2	Si
Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche	2	10	0,2	Si
Danneggiamento di informazioni, dati e programmi informatici	3	10	0,3	Si
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità	12	10	1,2	Riesame OdV
Danneggiamento di sistemi informatici e telematici	3	10	0,3	Si
Danneggiamento di sistemi informatici e telematici di pubblica utilità	6	5	1,2	Riesame OdV
Frode informatica che presta servizi di certificazione di firma elettronica	12	19	1,2	Riesame OdV

Tenendo conto che i protocolli di prevenzione e controllo previsti dal Modello sono tutti quelli implementabili senza creare intralcio nel flusso delle attività, che è prevista una adeguata formazione del personale, che sono previste attività di monitoraggio sulla reale applicazione dei protocolli, l'Organismo di Vigilanza ritiene che il rischio residuo relativo ai reati informatici e trattamento dati sia accettabile in quanto il Modello garantisce ragionevolmente di non poter essere eluso se non fraudolentemente.

Parte speciale D

Reati contro il diritto d'autore

I reati relativi alla violazione del diritto d'autore richiamati dall'art. 25octies del Decreto es applicabili alle attività di La Fabbrica di Lampadine sono i seguenti:

1. Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o parte di essa (art 191, l. 633/1941 comma 1 lett a) bis)
2. Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore e la reputazione (art 1919 l. 633/1941 comma 3)
3. Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 191-bis, l. 633/1941 comma 1)
4. Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati, distribuzione, vendita o concessione in locazione di banche di dati (art. 191-bis, 633/1941 comma 2)
5. Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opera dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere di un'opera dell'ingegno protetta dal diritto d'autore o parte di essa (art. 191-ter, l. 633/1941)
6. Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art 191-septies l.633/1941)
7. Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via rete, via satellite, via cavo, in forma sia analogica sia digitale (art 191-octies l.633/1941)

Grado di esposizione al rischio

In conformità alla metodologia per il calcolo del rischio reato descritta, per i reati contro il diritto d'autore sono stati calcolati i rischi riportati nella tabella seguente:

Reato presupposto	Grado di gravità	Tasso di frequenza	Valutazione impatto	Valore del rischio	Necessità protocollo
Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o parte di essa	1	2	1	2	Si
Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore e la reputazione	2	1	1	2	Si
Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; […]	3	3	1	9	Si
Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; […]	3	1	1	3	Si
Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opera dell'ingegno […]	3	3	1	9	Si
Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione	3	3	1	3	Si
Fraudolenta produzione, […] di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso […]	3	1	1	3	Si

Processi a rischio

Secondo quanto stabilito nella Parte Generale, i processi a rischio reati contro il diritto d'autore sono:

Processi principali	Processi di supporto
• Servizi per l'orientamento formativo: organizzazione ed erogazione • Servizi formativi: progettazione, organizzazione ed erogazione	• Gestione della contabilità e degli adempimenti normativi • Rendicontazione delle spese

Aree a rischio

Secondo quanto stabilito nella Parte generale, le aree a rischio reati contro il diritto d'autore sono:

- Direzione Generale
- - Formazione
- - Amministrazione
- - IT

Attività a rischio

Le attività considerate a rischio reati contro il diritto d'autore sono le seguenti:

- Utilizzo del sistema informativo, della rete interne e della posta elettronica per la preparazione e l'erogazione di servizi di orientamento e di formazione finanziati, e per le attività amministrative.

Protocolli di prevenzione e controllo

Sulla base della valutazione del rischio reato, dei processi, aree e attività sensibili vengono individuati i protocolli sotto riportati:

- Esplicita indicazione nel Codice Etico di specifiche regole di condotta
- Diffusione del Codice Etico verso tutti i dipendenti ed i collaboratori esterni
- Definizione ed applicazione di procedure organizzative per la gestione delle opere coperte da diritto d'autore

- Definizione di un sistema di auditing interno atto a monitorare la corretta applicazione dei protocolli

Nella tabella seguente è riportata la valutazione dell'efficacia dei protocolli di prevenzione e delle procedure organizzative

Analisi del rischio residuo – rischio accettabile

	Valore del rischio	Efficacia dei protocolli	Rischio residuo	Accettabilità del rischio residuo
Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o parte di essa	2	5	0,4	SI
Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore e la reputazione	2	5	0,4	Si
Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; […]	9	5	1,8	Riesame OdV
Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; […]	3	5	0,6	Si
Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opera dell'ingegno […]	9	5	1,8	Riesame OdV
Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione	3	5	0,6	Si
Fraudolenta produzione, […] di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso […]	3	5	0,6	Si

Tenendo conto che i protocolli di prevenzione e controllo previsti dal Modello sono tutti quelli implementabili senza creare intralcio nel flusso delle attività, che è prevista una adeguata formazione del personale, che sono previste attività di monitoraggio sulla reale applicazione dei protocolli, l'Organismo di Vigilanza ritiene che il rischio residuo relativo ai reati informatici e trattamento dati sia accettabile in quanto il Modello garantisce ragionevolmente di non poter essere eluso se non fraudolentemente.

Parte speciale E

Reati per violazione delle norme di sicurezza

I reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, richiamati dall'art 25-septies del Decreto ed applicabili alle attività di La Fabbrica di Lampadine sono i seguenti:

1- Omicidio colposo (art. 589 c.p.)
2- Lesioni personali colpose (art. 590 c.p.)

Grado di esposizione al rischio

In conformità alla metodologia per il calcolo del rischio descritta per i reati per la violazione delle norme di sicurezza sono stati calcolati i rischi riportati nella tabella seguente:

Reato presupposto	Grado di gravità	Tasso di frequenza	Valutazione impatto	Valore del rischio	Necessità protocollo
Omicidio colposo	3	1	1	3	Si
Lesioni personali colpose	3	1	1	3	Si

Processi a rischio

Secondo quanto stabilito nella Parte Generale, i processi a rischio reati per la violazione delle norme antinfortunistiche sono:

Processi principali	Processi di supporto
• Servizi per l'orientamento formativo: organizzazione ed erogazione • Servizi formativi: progettazione, organizzazione ed erogazione	• Gestione della documentazione: identificazione, rintracciabilità, conservazione • Valutazione della competenza del personale • Gestione amministrativa del personale

Aree a rischio

Secondo quanto stabilito nella Parte Generale, le aree a rischio reati per la violazione delle norme antinfortunistiche sono:

- Direzione Generale
- RSPP

Attività a rischio

Le attività considerate a rischio reato per violazione norme antinfortunistiche sono le seguenti:

- Gestione dei documenti richiesti dalla normativa vigente in materia di sicurezza
- Formazione del personale in materia di sicurezza

Protocolli di prevenzione e controllo

Sulla base di valutazione di rischio reato, dei processi, aree e attività sensibili vengono decisi i protocolli riportati di seguito:

- Redazione del Documento di Valutazione rischi
- Redazione Piani di Emergenza
- Effettuazione delle prove di evacuazione
- Nomina delle figure previste dal D.lgs 81/08
- Attestati di frequenza ai corsi obbligatori
- Definizione di un sistema di auditing interno atto a monitorare la corretta applicazione dei protocolli.

Analisi del rischio residuo – rischio accettabile

Nella tabella che segue è riportata la valutazione dell'efficacia dei protocolli di prevenzione e delle procedure organizzative:

	Valore del rischio	Efficacia dei protocolli	Rischio residuo	Accettabilità del rischio residuo
Omicidio colposo	3	5	0,6	SI
Lesioni personali colpose	3	5	0,6	Si