



ISTITUTO SALESIANO
SAN MARCO

1990-2015
25° ANNIVERSARIO

via dei Salesiani, 15 - 30174 Mestre-Venezia
T. 041.5498111 - F. 041.5498112
info@issm.it - www.issm.it

MODELLO ORGANIZZATIVO E DI GESTIONE

Redatto secondo
il D. Lgs. 8 giugno 2001, n. 231 e s.m.i.

INDICE SISTEMATICO

INDICE SISTEMATICO	2
SEZIONE 1 – OGGETTO DEL MODELLO ORGANIZZATIVO	6
1.1 Funzione del Modello Organizzativo.....	6
1.2 Formazione del Modello Organizzativo	7
1.3 Elementi fondamentali del Modello Organizzativo	7
1.4 Adozione del Modello Organizzativo	8
I Processi ed eventi sensibili rispetto ai reati nei rapporti con la pubblica amministrazione.....	8
II Processi ed eventi sensibili rispetto ai reati contro la personalità dell’individuo e contro la persona.....	8
III Processi ed eventi sensibili rispetto ai reati contro la vita e l’incolumità individuale	8
IV Processi ed eventi sensibili rispetto ai reati contro il patrimonio	8
V Processi ed eventi sensibili rispetto ai reati informatici.....	9
VI Processi ed eventi sensibili rispetto ai delitti di criminalità organizzata	9
VII Processi ed eventi sensibili rispetto ai delitti contro l’industria ed il commercio	9
VIII Processi ed eventi sensibili rispetto ai delitti in materia di diritto d’autore.....	9
SEZIONE 2 – ASSETTO DELL’ENTE ECCLESIASTICO	9
2.1 Natura giuridica dell’ente Istituto Salesiano San Marco.....	9
2.2. Ispettoria.....	10
2.3 Struttura interna dell’ente Istituto Salesiano San Marco.....	10
SEZIONE 3 – ORGANISMO DI VIGILANZA	11
3.1 Costituzione dell’Organismo di vigilanza	11
3.2 Funzioni e poteri dell’Organismo di vigilanza.....	12
3.3 Attività di riferimento	12
3.4 Obblighi di informazione.....	12
3.5 Verifiche sull’adeguatezza del Modello Organizzativo	13
3.6 Attività di audit.....	13
3.7 Attività di formazione	14
SEZIONE 4 – DIVULGAZIONE DEL MODELLO ORGANIZZATIVO.....	15
4.1 Informazioni generali.....	15
4.2 Informazioni ai religiosi.....	15
4.3 Informazioni ai dipendenti	15
4.4 Informazioni ai collaboratori	15
4.5 Informazioni alle figure apicali e ai preposti	16

SEZIONE 5 – SISTEMA DISCIPLINARE E SANZIONATORIO.....	16
5.1 Oggetto	16
5.2 Sanzioni relative ai dipendenti	16
5.3 Sanzioni relative ai collaboratori e ai soggetti esterni	16
5.4 Sanzioni relative ai dirigenti	17
SEZIONE 6 – NORMATIVA DI RIFERIMENTO.....	17
6.1 Reati da prevenire	17
6.2 Esonero dell’ente da responsabilità amministrativa	18
SEZIONE 7 – REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE.....	19
7.1 Nozioni relative alla pubblica amministrazione	19
7.2 Elenco dei reati	20
7.2.1 Malversazione a danno dello Stato o dell’Unione Europea (art. 316-bis cod. pen. - art. 24 d.lgs.231/01)	20
7.2.2 Indebita percezione di erogazioni in danno dello Stato o dell’Unione Europea (art. 316-ter cod. pen. - art. 24 d.lgs.231/01)	20
7.2.3 Concussione - Induzione indebita a dare o promettere utilità (art. 317 cod. pen. - art. 319 quater cod. pen. - art. 25 d.lgs.231/01)	20
7.2.4 Corruzione per un atto d’ufficio o contrario ai doveri d’ufficio (artt. 318-319-320-321 cod. pen. - art. 25 d.lgs.231/01)	21
7.2.5 Istigazione alla corruzione (art. 322 cod. pen. - art. 25 d.lgs.231/01)	21
7.2.6 Corruzione in atti giudiziari (art. 319-ter cod. pen. - art. 25 d.lgs.231/01)	21
7.2.7 Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis cod. pen. - art. 25 d.lgs.231/01)	21
7.2.8 Malversazione a danno dello Stato (art. 316 bis cod. pen. - art. 24 d. lgs. 231/01) - Indebita percezione di erogazioni a danno dello Stato (art. 316 ter cod. pen. - art. 24 d.lgs. 231/01)	22
7.2.9 Truffa in danno dello Stato, di altro ente pubblico o dell’Unione Europea (art. 640, comma 2, n. 1, cod. pen. - art. 24 d. lgs. 231/01)	22
7.2.10 Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis cod. pen. - art. 24 d. lgs. 231/01)	22
7.2.11 Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter cod. pen. - art. 24 d. lgs. 231/01)	23
7.3 Processi ed eventi sensibili.....	23
7.4 Deleghe e procure.....	23
7.5 Controlli dell’Organismo di vigilanza	24
SEZIONE 8 – REATI CONTRO LA VITA E L’INCOLUMITÀ INDIVIDUALE.....	24
8.1 Elenco dei reati	24
8.1.1 Omicidio colposo con violazione delle norma sulla prevenzione degli infortuni sul lavoro (art. 589, comma 2, cod. pen. - art. 25 septies d.lgs. 231/01)	24
8.1.2 Lesioni personali colpose aggravate dalla violazione delle norma sulla prevenzione degli infortuni sul lavoro (art. 590, comma 3, cod. pen. - - art. 25 septies d.lgs. 231/01)	25
8.2 Processi ed eventi sensibili.....	26

SEZIONE 9 – REATI CONTRO LA PERSONALITÀ DELL'INDIVIDUO	27
9.1.1 Riduzione in schiavitù (art. 600 cod. pen. - art. 25 quinquies d.lgs. 231/01)	28
9.1.2 Prostituzione minorile (art. 600-bis cod. pen. - art. 25 quinquies d.lgs. 231/01)	28
9.1.3 Pornografia minorile (art. 600-ter cod. pen. - art. 25 quinquies d.lgs. 231/01) - Pornografia virtuale (art. 600 quater.1 cod. pen.)	28
9.1.4 Detenzione di materiale pornografico (art. 600-quater cod. pen. - art. 25 quinquies d.lgs. 231/01) - Pornografia virtuale (art. 600 quater.1 cod. pen.)	29
9.1.5 Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies cod. pen. - art. 25 quinquies d.lgs. 231/01)	29
9.2 Processi ed eventi sensibili	29
SEZIONE 10 – REATI CONTRO IL PATRIMONIO MEDIANTE FRODE	30
10.1 Elenco dei reati	30
10.1.1 Ricettazione (art. 648 cod. pen. - art. 25 octies d.lgs. 231/01)	30
10.1.2 Riciclaggio (art. 648-bis cod. pen. - art. 25 octies d.lgs. 231/01)	31
10.1.3 Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter cod. pen. - art. 25 octies d.lgs. 231/01)	31
10.1.4 Autoriciclaggio (art. 648 ter.1 cod. pen. - art. 25 octies d.lgs. 231/01)	31
10.2 Processi ed eventi sensibili	32
SEZIONE 11 REATI SOCIETARI ED ALTRI REATI	32
SEZIONE 12 – REATI INFORMATICI	33
12.1 Elenco dei reati	33
12.1.1 Accesso abusivo ad un sistema informatico o telematico (art. 615-ter cod. pen. - art. 24 bis d.lgs. 201/01)	33
12.1.2 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. pen. - art. 24 bis d.lgs. 201/01)	34
12.1.3 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. pen. - art. 24 bis d.lgs. 201/01)	34
12.1.4 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. pen. - art. 24 bis d.lgs. 201/01)	34
12.1.5 Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies cod. pen. - art. 24 bis d.lgs. 201/01)	35
12.1.6 Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. pen. - art. 24 bis d.lgs. 201/01)	35
12.1.7 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter cod. pen. - art. 24 bis d.lgs. 201/01)	36
12.1.8 Danneggiamento di sistemi informatici o telematici (art. 635-quater cod. pen. - art. 24 bis d.lgs. 201/01)	36
12.1.9 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cod. pen. - art. 24 bis d.lgs. 201/01)	36
12.1.10 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies cod. pen. - art. 24 bis d.lgs. 201/01)	37
12.1.11 - Documenti informatici (art. 491 bis cod. pen. - art. 24 bis d.lgs. 231/01)	37

12.2 - Processi ed eventi sensibili	37
SEZIONE 13 – DELITTI DI CRIMINALITÀ ORGANIZZATA	38
13.1 Elenco dei reati	38
13.1.1 Associazione per delinquere per commettere i reati di cui all'art. 416 n.6 cod. pen. (- art. 24 ter d.lgs. 201/01)	38
13.1.2 Associazione di tipo mafioso (art. 416 bis cod. pen. - art. 24 ter d.lgs. 201/01)	38
13.1.3 Scambio elettorale politico – mafioso (art. 416 ter cod. pen. - art. 24 ter d.lgs. 201/01)	39
13.1.4 Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309 - art. 24 ter d.lgs. 201/01)	39
13.1.5 Associazione per delinquere commi da 1 a 5 (art. 416 cod. pen. - art. 24 ter d.lgs. 201/01)	39
SEZIONE 14 – DELITTI CONTRO L'INDUSTRIA ED IL COMMERCIO	40
SEZIONE 15 DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE	40
15.1 Elenco dei reati	40
15.1.1 Reati previsti dagli articoli 171, 171 bis, 171 ter, 171 septies e 171 octies della legge 22 aprile 1941, n. 633 (legge in materia di diritto d'autore) (art. 25 nonies d.lgs. 201/01)	40
SEZIONE 16 – ORGANIZZAZIONE COMUNE ALLE ATTIVITÀ DELL'ENTE	44
16.1 Tutela della salute e sicurezza nei luoghi di lavoro	44
16.2 Protezione dei dati personali	44
16.3 Igiene ed autocontrollo alimentare	44
16.4 Attività esternalizzate	44
16.5 Modello organizzativo e certificazione di qualità	45
SEZIONE 17 – INDIVIDUAZIONE DELLE ATTIVITÀ SENSIBILI	46
Istituto Salesiano San Marco	46
Istituto Salesiano San Marco	46

SEZIONE 1 – OGGETTO DEL MODELLO ORGANIZZATIVO

1.1 Funzione del Modello Organizzativo

Il D.Lgs. 8 giugno 2001, n. 231, reca le disposizioni normative concernenti la «Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di responsabilità giuridica».

Il provvedimento è stato emanato in base a quanto previsto dagli artt. 11 e 14 della legge 29 settembre 2000, n. 300, che delegava il Governo ad adottare un decreto legislativo avente ad oggetto la disciplina della responsabilità amministrativa delle persone giuridiche e delle società, associazioni od enti privi di personalità giuridica che non svolgessero funzioni di rilievo costituzionale.

Ai sensi dell'art. 5, comma 1, D.Lgs. n. 231/2001, l'ente ecclesiastico civilmente riconosciuto **Istituto Salesiano San Marco** può essere ritenuto responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da soggetti in posizione formale apicale, vale a dire da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente ecclesiastico civilmente riconosciuto o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale;
- da soggetti in posizione di fatto apicale, vale a dire da persone che esercitano anche di fatto, senza formale investitura, la gestione e il controllo dell'ente ecclesiastico civilmente riconosciuto;
- da soggetti direttamente sottordinati alle posizioni di vertice, vale a dire da persone sottoposte alla direzione o alla vigilanza di un soggetto in posizione apicale.

Scopo del presente Modello Organizzativo è la predisposizione di un sistema strutturato ed organico di prevenzione, di dissuasione e di controllo, finalizzato alla riduzione del rischio di commissione dei reati, mediante l'individuazione delle attività sensibili e, se necessario, la loro conseguente proceduralizzazione.

Il Modello Organizzativo è composto da:

- descrizione dei reati individuati dal D.Lgs. n. 231/2001, in relazione alla realtà lavorativa dell'ente;
- elenco dei processi e degli eventi rientranti nella casistica prevista dal D.Lgs. n. 231/2001 e considerati rilevanti per l'ente;
- indicazione delle procedure organizzative specifiche e degli elementi di controllo identificati al fine di prevenire o limitare le situazioni a rischio di reato connesse a tali eventi e processi;
- descrizione delle attività dell'Organismo di vigilanza, identificato dall'ente **Istituto Salesiano San Marco** per garantire il rispetto del sistema organizzativo adottato e la vigilanza sull'operato dei destinatari; al riguardo si evidenzia che gli istituti di vita consacrata sono soggetti al sistema di vigilanza previsto dal diritto canonico, per cui già l'attenta applicazione di tale diritto è il primo strumento di salvaguardia;
- sistema sanzionatorio adottato per la violazione delle regole e delle procedure previste dal modello;
- modalità di informazione e formazione rispetto ai contenuti del modello.

I principi contenuti nel presente Modello Organizzativo e di gestione devono condurre a determinare nel potenziale autore del reato la consapevolezza di commettere un illecito, la cui commissione è deprecata e contraria agli interessi di , anche quando apparentemente esso potrebbe trarne un vantaggio; inoltre,

grazie ad un monitoraggio costante dell'attività, devono consentire all'ente stesso di prevenire o di reagire tempestivamente per impedire la commissione del reato.

1.2 Formazione del Modello Organizzativo

A seguito dell'emanazione del D.Lgs. n. 231/2001, l'ente **Istituto Salesiano San Marco** ha avviato una serie di attività, al fine di predisporre il Modello Organizzativo previsto dal decreto legislativo.

Le attività svolte sono state le seguenti:

- mappatura dei rischi e identificazione delle attività sensibili: è stata effettuata un'indagine sulla complessiva organizzazione dell'ente ecclesiastico, analizzando la documentazione disponibile e mantenendo una serie di contatti personali con le figure-chiave nell'ambito della struttura dell'ente, per individuare le attività potenzialmente in grado di ingenerare rischi in ordine all'eventuale commissione dei reati o illeciti; per ciascuna attività sensibile individuata sono state verificate le modalità di gestione approntate dall'ente e il sistema di controllo in essere;
- individuazione degli interventi di miglioramento e predisposizione del modello: sulla base della situazione rilevata e degli scopi del D.Lgs. n. 231/2001, si sono individuate le possibili azioni di miglioramento dell'attuale sistema di controllo interno (processi e procedure esistenti) e i requisiti organizzativi essenziali per la definizione di un modello di organizzazione; si è, quindi, proceduto alla definizione di un elenco degli interventi ed alla parallela stesura del presente Modello Organizzativo.

1.3 Elementi fondamentali del Modello Organizzativo

Nella redazione del presente modello si è tenuto conto delle procedure e dei sistemi di controllo interno esistenti e già operanti, in quanto strumenti di prevenzione dei reati e di controllo sui processi coinvolti nelle attività sensibili, nonché del sistema delle deleghe e delle responsabilità in vigore.

Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni, anche in relazione ai reati da prevenire, l'ente **Istituto Salesiano San Marco** ha identificato:

1. i principi generali sull'autorità e sull'amministrazione dei beni contenuti nella Parte Quarta Capitoli X, XI, XII, XIII e XIV delle Costituzioni della *Società di San Francesco di Sales* emanate dal Capitolo generale e approvate dalla Sacra Congregazione per gli Istituti di Vita Consacrata e le Società di Vita Apostolica il 25 novembre 1984;
2. i Regolamenti generali della Società di San Francesco di Sales;
3. il Codice Etico già approvato e allegato al presente modello;
4. il direttorio economico ispettoriale;
5. il diritto canonico;
6. il diritto concordatario;
7. il sistema sanzionatorio recato dalla contrattazione collettiva di lavoro applicata nella gestione delle attività dell'ente **Istituto Salesiano San Marco**;
8. la legislazione italiana.

Sono stati inoltre tenuti presenti i requisiti indicati dal D.Lgs. n. 231/2001, quali:

- l'attribuzione ad un Organismo di vigilanza, interno alla struttura dell'ente ecclesiastico, del compito di attuare efficacemente il Modello Organizzativo, anche tramite il monitoraggio dei comportamenti dei vari addetti dell'ente e il diritto a ricevere informazioni sulle attività sensibili;
- l'attività di verifica del funzionamento del modello con eventuale successivo aggiornamento;
- la sensibilizzazione e la diffusione all'interno dell'ente ecclesiastico delle regole e delle procedure stabilite.

Il Modello Organizzativo si ispira pure ai principi generali di un adeguato sistema di controllo interno, quali:

- la verificabilità, la documentabilità, la coerenza e la congruenza di ogni operazione rilevante ai fini del D.Lgs. n. 231/2001;
- il rispetto del principio di separazione delle funzioni;
- l'assegnazione di poteri di autorizzazione coerenti con le responsabilità in essere;
- a comunicazione all'Organismo di vigilanza delle informazioni rilevanti.

1.4 Adozione del Modello Organizzativo

L'ente **Istituto Salesiano San Marco** ha deciso di dotarsi del modello di organizzazione e gestione, facendolo adottare da parte del Consiglio della Comunità e di procedere all'istituzione dell'Organismo di vigilanza.

Il Modello Organizzativo è, per legge, un «atto di emanazione dell'organo dirigente», sicché le successive modifiche di carattere sostanziale sono rimesse alla competenza del Consiglio della Comunità; intendendosi per «sostanziali» quelle modifiche che si rendessero necessarie a seguito dell'evoluzione della normativa di riferimento o che implicassero un cambiamento nelle regole e nei principi comportamentali contenuti nel presente modello, nei poteri e doveri dell'Organismo di vigilanza e nel sistema sanzionatorio. L'analisi della realtà dell'ente ecclesiastico, effettuata al fine di definire le aree di rischio rilevanti per l'ente stesso ha consentito di identificare i seguenti «processi sensibili», articolati in due sezioni omogenee per contenuti:

I Processi ed eventi sensibili rispetto ai reati nei rapporti con la pubblica amministrazione

1. rapporti contrattuali con la pubblica amministrazione;
2. gestione e liquidazione di infortuni sul lavoro e prestazioni previdenziali;
3. acquisti di beni o servizi, consulenze e sponsorizzazioni;
4. selezione e assunzione del personale;
5. ottenimento e utilizzo di contributi e finanziamenti;
6. erogazione di contributi commerciali;
7. collegamenti telematici o trasmissione di dati;
8. edilizia e gestione degli immobili.

II Processi ed eventi sensibili rispetto ai reati contro la personalità dell'individuo e contro la persona

1. selezione e assunzione del personale;
2. utilizzo di collegamenti telematici;
3. utilizzo di apparecchiature audiovisive;
4. assistenza a minorenni e portatori di handicap fisici e sociali;
5. gestione della sicurezza e dell'igiene nei luoghi di lavoro;
6. trattamento dei dati personali;

III Processi ed eventi sensibili rispetto ai reati contro la vita e l'incolumità individuale

Sicurezza sui luoghi di lavoro.

IV Processi ed eventi sensibili rispetto ai reati contro il patrimonio

1. gestione del patrimonio immobiliare e mobiliare;
2. acquisti di beni o servizi.

V Processi ed eventi sensibili rispetto ai reati informatici

Tutte le attività che implicano l'utilizzazione di sistemi informatici.

Non sono stati considerati rilevanti in quanto solo astrattamente ipotizzabili, e quindi sono stati tralasciati il reato di falso nummario, il reato di mutilazione degli organi genitali femminili, i reati con finalità di terrorismo e di eversione dell'ordine democratico, i reati relativi agli abusi di mercato.

VI Processi ed eventi sensibili rispetto ai delitti di criminalità organizzata

1. rapporti con utenti dei servizi di minor età;
2. rapporti con i fornitori;
3. comportamento del personale e degli utenti;

VII Processi ed eventi sensibili rispetto ai delitti contro l'industria ed il commercio

1. svolgimento di attività commercial e all'interno dei locali dell'ente;
2. preparazione e somministrazione di prodotti alimentari;

VIII Processi ed eventi sensibili rispetto ai delitti in materia di diritto d'autore

1. utilizzo dei dispositivi informatici;
2. riproduzione di opere audiovisive in occasione di feste, celebrazioni ed attività di carattere educativo o ricreativo;

Non sono stati considerati rilevanti in quanto solo astrattamente ipotizzabili, e quindi sono stati tralasciati il reato di falso nummario, il reato di mutilazione degli organi genitali femminili, i reati con finalità di terrorismo, di eversione dell'ordine democratico, i reati relativi agli abusi di mercato

SEZIONE 2 – ASSETTO DELL'ENTE ECCLESIASTICO

2.1 Natura giuridica dell'ente Istituto Salesiano San Marco

L'ente **Istituto Salesiano San Marco**, con sede legale in Via dei Salesiani, 15 30174 Venezia-Mestre, soggetto di diritto della Chiesa cattolica ed Ente Ecclesiastico civilmente riconosciuto in Italia ai sensi e per gli effetti della L. 20 maggio 1985, n. 222. In ragione di ciò, davanti all'ordinamento civile italiano l'Istituto è persona giuridica autonoma, mentre dal punto di vista del diritto canonico e del relativo sistema di controlli ed autorizzazioni, esso costituisce una comunità della *Società di San Francesco di Sales*, istituto religioso di vita consacrata di diritto pontificio.

La *Società di San Francesco di Sales* si configura in comunità ispettoriali che, a loro volta, sono articolate in comunità locali. Il fine costitutivo è di religione e di culto, realizzando in una specifica forma di vita religiosa il progetto apostolico del Fondatore, San Giovanni Bosco. Tale missione è realizzata principalmente attraverso attività ed opere in cui è possibile promuovere l'educazione umana e cristiana dei giovani, come l'oratorio e il centro giovanile, la scuola e i centri professionali, i convitti e le case per giovani in difficoltà.

La legale rappresentanza dell'ente **Istituto Salesiano San Marco**, spetta alla persona fisica indicata dall'Ispettore, la cui nomina è regolarmente iscritta nel Registro delle Persone Giuridiche tenuto dalla Prefettura – Ufficio Territoriale del Governo di Venezia.

2.2. Ispettorìa

Nella organizzazione gerarchica della Società di San Francesco di Sales, l'Istituto Salesiano San Marco è parte di una Ispettorìa che comprende tutti i Salesiani che vivono e operano nella Regione del Triveneto. A capo di ciascuna Ispettorìa viene posto un Ispettore.

L'Ispettore, che civilmente non fa parte dell'organigramma dell'ente **Istituto Salesiano San Marco**, esercita, rispetto all'attività dello stesso, una funzione apicale di fatto, in forza dei meccanismi di diritto proprio che collegano l'attività dei singoli enti ecclesiastici civilmente riconosciuti con l'Ispettorìa. In particolare l'Ispettore, rispetto all'attività dell'ente, è titolare dei seguenti poteri:

- nomina del legale rappresentante;
- nomina del Direttore dell'opera;
- nomina dell'Economo dell'opera;
- autorizzazione scritta per gli atti di straordinaria amministrazione, previo parere del Consiglio ispettoriale.

2.3 Struttura interna dell'ente Istituto Salesiano San Marco

L'ente **Istituto Salesiano San Marco** ha un legale rappresentante, nominato dall'Ispettore secondo il procedimento regolato dal diritto proprio.

Il legale rappresentante è titolare dei poteri relativi agli atti di ordinaria amministrazione, essendo necessario, per gli atti di straordinaria amministrazione, il consenso scritto dell'Ispettore.

Il legale rappresentante è la funzione in posizione apicale formale dell'ente **Istituto Salesiano San Marco**, nei confronti dell'ordinamento civile.

Oltre al legale rappresentante dell'ente, l'Ispettore nomina, per ciascuna opera gestita dall'ente, un Direttore dell'opera, che, oltre a tutto quanto concerne i profili spirituali e di animazione della comunità religiosa, è titolare, tra l'altro, delle prerogative connesse ai seguenti ambiti:

- coordinamento della comunità dei confratelli;
- resoconto dell'Ispettore in merito all'andamento dell'opera ed alle questioni più rilevanti connesse alla gestione dell'attività, comprese le eventuali criticità ;
- amministrazione dei beni temporali, avvalendosi a tale ultimo fine dell'attività dell'Economo dell'opera.

Le norme di diritto proprio individuano gli atti per i quali il Direttore deve avere il consenso del Consiglio della Comunità.

Il Direttore dell'opera, rispetto al livello di responsabilità individuato dal D. Lgs. 231/01, costituisce una funzione apicale di fatto.

Rispetto all'attività dell'ente **Istituto Salesiano San Marco** l'Economo dell'opera si configura quale preposto, giacché agisce in dipendenza dal Direttore.

Oltre a quanto definito relativamente all'amministrazione dei beni dell'opera, le ulteriori regole in materia di amministrazione dei beni temporali sono definite dall'ordinamento canonico per la generalità degli enti ecclesiastici e dal diritto proprio per quanto riguarda la distribuzione interna dei relativi poteri di decisione, controllo e gestione.

SEZIONE 3 – ORGANISMO DI VIGILANZA

3.1 Costituzione dell'Organismo di vigilanza

L'art. 6 D.Lgs. n. 231/2001, nel riconnettere l'esonero da responsabilità dell'ente all'adozione e all'efficace attuazione di un modello di organizzazione, gestione e controllo idoneo a prevenire la realizzazione degli illeciti penali considerati dalla normativa, ha previsto l'istituzione di un Organismo di vigilanza, cui è assegnato specificamente il compito di vigilare:

- sull'osservanza del Modello Organizzativo da parte dei religiosi, dei dipendenti, dei collaboratori esterni, degli appaltatori di opere e servizi;
- sull'efficacia e sull'adeguatezza del modello in relazione alla struttura organizzativa dell'ente ed all'effettiva capacità di prevenire la commissione dei reati;
- sull'opportunità di aggiornamento del Modello Organizzativo, quando si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni organizzative o normative, sollecitando a tal fine gli organi competenti.

I compiti assegnati all'Organismo di vigilanza richiedono che lo stesso sia dotato di autonomi poteri di iniziativa e di controllo. Da tale caratterizzazione discendono:

- l'insindacabilità delle scelte dell'Organismo di vigilanza, onde non far venire meno la sua autonomia;
- la posizione di indipendenza dei membri che compongono l'Organismo di vigilanza, posizione da riservare a soggetti di assoluta affidabilità in ragione delle capacità personali loro riconosciute;
- l'appartenenza dell'Organismo di vigilanza alla struttura dell'ente, dati la sua specificità e il cumulo dei compiti attribuitigli.

Alla luce di quanto sopra delineato, l'Organismo di vigilanza è costituito da n. 3 componenti, nominati dal Legale Rappresentante.

L'Organismo di vigilanza, in base al requisito di autonomia e indipendenza stabilito dal D.Lgs. n. 231/2001, ha l'obbligo di riferire periodicamente all'organo amministrativo che, nel caso dell'Istituto Salesiano San Marco è il legale rappresentante dello stesso.

L'Organismo di vigilanza potrà essere supportato da un professionista esterno all'ente ovvero una società specializzata avente funzioni di Compliance e all'uopo incaricata.

Il Compliance Officer, ovvero l'organizzazione professionale incaricata della funzione di Compliance, avrà il compito di assistere tutte le funzioni dell'ente nell'osservanza delle prescrizioni contenute nel presente modello e nell'allegato Codice Etico.

Al fine di garantire l'imparzialità e la competenza professionale connesse alle caratteristiche delle mansioni affidate, il Compliance Officer dovrà essere in possesso di specifiche competenze in materia di diritto penale, diritto d'impresa, sistemi gestionali ed organizzazione aziendale.

Il Compliance Officer potrà partecipare a tutti gli effetti, ma senza diritto di voto, alle attività dell'Organismo di vigilanza.

Il Compliance Officer ha il compito di coordinare gli adempimenti connessi ai diversi settori normativi, che interagiscono nell'ambito delle rispettive sfere di applicazione e che presentano, come tratto comune, l'incidenza, diretta o indiretta, sui processi sensibili individuati all'interno del presente Modello Organizzativo (a titolo non esaustivo: gestione del personale, esternalizzazione dei servizi mediante appalti o altra forma contrattuale, certificazione di qualità, sicurezza sul lavoro, privacy, accreditamento regionale, adempimenti contabili e di bilancio, igiene alimentare...).

3.2 Funzioni e poteri dell'Organismo di vigilanza

L'Organismo di vigilanza:

- relativamente ai processi a rischio di commissione di reati, accede agli archivi delle funzioni coinvolte e alle procedure informatiche di supporto al fine di controllare, a campione, il rispetto delle procedure organizzative definite;
- riceve flussi informativi dalle singole funzioni, relativamente ad alcune specifiche situazioni a rischio di commissione reato ai sensi del D.Lgs. 231/2001; ove dalle verifiche effettuate emergano delle situazioni anomale, l'Organismo di vigilanza si attiva con specifiche attività ispettive sulle funzioni interessate;
- conduce ricognizioni sulle attività dell'ente ai fini dell'aggiornamento della mappatura delle attività potenzialmente interessate dai reati;
- raccoglie, elabora e conserva le informazioni rilevanti in ordine al rispetto del Modello Organizzativo, aggiornando la lista di informazioni che devono essergli trasmesse o tenute a sua disposizione;
- verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutti i documenti interni di conferimento delle deleghe, raccomandando eventuali modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie;
- si coordina con i responsabili per la definizione dei programmi di formazione per il personale e del contenuto delle comunicazioni periodiche da inviare ai dipendenti, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. n. 231/2001.

3.3 Attività di riferimento

L'attività di riferimento (reporting) dell'Organismo di vigilanza in merito all'attuazione del Modello Organizzativo e all'emersione di eventuali criticità si sviluppa su due linee:

- la prima, su base continuativa, direttamente verso il legale rappresentante dell'Istituto;
- la seconda, annuale, verso il Consiglio della Casa, per il quale predispone una relazione scritta sull'attività svolta nel corso dell'anno, sui controlli e sulle verifiche eseguiti, nonché sull'eventuale aggiornamento della mappatura delle attività sensibili alla commissione dei reati, allegando un piano delle attività previste per l'anno successivo.

Gli incontri con il Consiglio della Casa devono essere verbalizzati e copie dei verbali devono essere custodite dal Consiglio stesso

3.4 Obblighi di informazione

L'Organismo di vigilanza deve essere informato, mediante apposite segnalazioni, da parte dei religiosi, dei dipendenti, dei consulenti, dei fornitori o di altri collaboratori in merito a fatti, azioni od omissioni che potrebbero ingenerare responsabilità ai sensi del D.Lgs. n. 231/2001.

Valgono al riguardo le seguenti prescrizioni di carattere generale:

- i religiosi e i dipendenti, hanno il dovere di trasmettere all'Organismo di vigilanza eventuali segnalazioni relative alla commissione dei reati, ovvero alle situazioni di rischio di commissione degli stessi;
- coloro che in buona fede inoltrano segnalazioni devono essere garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione; in ogni caso sarà assicurata la riservatezza

dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela delle persone accusate erroneamente o in mala fede.

I religiosi che intendono inoltrare segnalazioni all'Organismo di vigilanza si atterranno alle norme del diritto proprio.

I dipendenti che intendano segnalare una violazione (o presunta violazione) del Modello Organizzativo, devono contattare il diretto superiore. Tuttavia, qualora la segnalazione non dia esito o il dipendente abbia oggettiva ragione di non rivolgersi al suo diretto superiore per la presentazione della segnalazione, può riferire direttamente all'Organismo di vigilanza.

I consulenti, i fornitori e gli altri collaboratori, per quanto riguarda l'attività svolta nei confronti o per conto dell'ente **Istituto Salesiano San Marco**, effettuano le segnalazioni direttamente all'Organismo di vigilanza.

L'Organismo di vigilanza valuta le segnalazioni ricevute; gli eventuali provvedimenti conseguenti sono applicati in conformità a quanto previsto dal sistema disciplinare definito nel presente Modello Organizzativo.

3.5 Verifiche sull'adeguatezza del Modello Organizzativo

L'Organismo di vigilanza, oltre all'attività sull'effettività del Modello Organizzativo, vale a dire di verifica della coerenza tra i comportamenti dei destinatari ed il modello stesso, periodicamente effettua specifiche verifiche sulla reale capacità del modello di prevenire i reati, relazionandosi, ove occorra, con soggetti terzi con adeguate caratteristiche di professionalità e indipendenza, di volta in volta indicati dal legale rappresentante.

Tale attività si concretizza in una verifica a campione sia dei documenti di maggior rilevanza relativi ai processi sensibili sia nelle attività di audit sul campo successivamente descritte.

Deve essere, inoltre, svolta una revisione di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'Organismo di vigilanza, delle verifiche a campione degli eventi considerati rischiosi e della sensibilizzazione dei dipendenti e degli organi dell'ente rispetto alla problematica della responsabilità penale.

Le verifiche e il loro esito sono riportate nei report periodici al legale rappresentante.

3.6 Attività di audit

Il piano annuale di audit è organizzato dall'Organismo di vigilanza secondo il criterio del campionamento rispetto al numero ed alla tipologia delle attività verificate.

Le verifiche e il loro esito sono riportate nel report annuale.

L'attività di audit si dovrà fondare sui seguenti principi ispiratori, diretti a garantire la completezza, l'imparzialità e l'efficacia dell'audit.

a) Comportamento etico

Durante l'audit sarà tenuto un comportamento basato su: fiducia, integrità, riservatezza e discrezione.

b) Presentazione imparziale

L'auditor riporterà fedelmente e con precisione le risultanze, le conclusioni ed i rapporti di audit, riportando gli ostacoli significativi incontrati durante l'audit e le opinioni divergenti non risolte tra il gruppo di audit e l'organizzazione oggetto dell'audit.

c) Adeguata professionalità

Gli auditor baseranno il contenuto del rapporto di audit sulle conoscenze di cui dispongono a livello professionale, integrate con le informazioni registrate nel corso dell'audit.

d) Indipendenza

Gli auditor conserveranno uno stato di obiettività di pensiero durante il processo dell'audit per assicurare che le risultanze e le conclusioni dell'audit siano basate solo sulle evidenze dell'audit.

e) Approccio basato sull'evidenza

Le evidenze dell'audit saranno verificabili. Esse si baseranno su campioni di informazioni disponibili ed indicati nel rapporto di audit.

3.7 Attività di formazione

L'Organismo di Vigilanza promuove e supervisiona l'attività di comunicazione, divulgazione del modello e formazione di competenza del legale rappresentante.

Il programma di formazione deve essere modulato in funzione dei destinatari, siano essi interni o esterni all'ente.

La partecipazione ai corsi costituisce obbligo per dipendenti.

L'OdV è tenuto a promuovere iniziative per la formazione, supervisionandone il processo e coordinandosi eventualmente con il responsabile del personale.

In particolare l'OdV dovrà:

1. richiedere il programma oggetto di formazione e il materiale oggetto dell'attività
2. verificare il contenuto, l'aggiornamento e la qualità del programma di formazione
3. verificare la completezza dei destinatari del programma di formazione
4. verificare il contenuto, l'aggiornamento e la qualità dei corsi di formazione svolti
5. verificare l'effettiva partecipazione del personale
6. verificare i risultati dell'attività di formazione.

SEZIONE 4 – DIVULGAZIONE DEL MODELLO ORGANIZZATIVO

4.1 Informazioni generali

L'ente **Istituto Salesiano San Marco**:

- garantisce una corretta conoscenza e divulgazione delle regole di condotta contenute nel presente Modello Organizzativo, sia verso i dipendenti che verso i collaboratori;
- provvede a portare a conoscenza di tutti i dipendenti e di chiunque collabori o interagisca con esso il Codice Etico allegato al presente documento.

L'adozione del Modello Organizzativo è comunicata a tutti i soggetti portatori di interesse, con avviso sul sito Internet dell'ente **Istituto Salesiano San Marco**, nel quale lo stesso si dichiara disponibile a consentirne la visione integrale a questi soggetti.

4.2 Informazioni ai religiosi

I religiosi che operano nelle attività dell'ente **Istituto Salesiano San Marco** e che gestiscono attività sensibili devono entrare in possesso di una copia del Codice Etico e del presente Modello Organizzativo. Le ricevute devono essere trasmesse all'Organismo di vigilanza, che le conserverà.

4.3 Informazioni ai dipendenti

Il livello di formazione e informazione è attuato con le modalità più opportune in relazione ai soggetti destinatari e con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento degli stessi nei processi sensibili.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'Organismo di vigilanza in collaborazione con tutti i responsabili delle altre funzioni di volta in volta coinvolte nell'applicazione del modello.

Ai dipendenti in servizio o di futuro inserimento viene consegnata una copia del Codice Etico allegato al presente Modello Organizzativo e viene loro richiesto di rilasciare una dichiarazione che ne attesti l'effettiva conoscenza. Il Codice Etico deve essere altresì affisso nei luoghi di lavoro, in spazi accessibili a tutti i dipendenti, a formare parte integrante della normativa disciplinare ai sensi dell'art. 7 della legge 20 maggio 1970, n. 300.

L'Organismo di vigilanza si impegna anche a definire programmi informativi specifici quando vengano apportate modifiche rilevanti al Modello Organizzativo e di gestione.

4.4 Informazioni ai collaboratori

Devono essere previste specifiche clausole, da inserire nei rapporti contrattuali, con le quali i soggetti che collaborano a vario titolo con l'ente **Istituto Salesiano San Marco** dichiarino di conoscere ed accettare i principi etici o il Modello Organizzativo, a seconda dei casi.

4.5 Informazioni alle figure apicali e ai preposti

Le figure in posizione formale apicale, le figure in posizione di fatto apicale e le figure in posizione di preposizione individuate nel presente documento devono entrare in possesso di una copia del Modello Organizzativo e del Codice Etico allegato.

SEZIONE 5 – SISTEMA DISCIPLINARE E SANZIONATORIO

5.1 Oggetto

Il sistema disciplinare identifica le sanzioni previste per le infrazioni ai principi, ai comportamenti e agli elementi specifici di controllo contenuti nel Modello Organizzativo.

L'applicazione del sistema sanzionatorio presuppone la sola violazione delle disposizioni del Modello Organizzativo; pertanto essa verrà attivata indipendentemente dallo svolgimento e dall'esito del procedimento penale, eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato.

Resta salva la facoltà per l'ente **Istituto Salesiano San Marco** di rivalersi per ogni danno o responsabilità che allo stesso possa derivare da comportamenti di dipendenti e collaboratori in violazione del Modello Organizzativo.

Il sistema disciplinare è vincolante per tutti i dipendenti e, pertanto, va affisso in luogo accessibile a tutti i lavoratori, come previsto dall'art. 7 della legge 20 maggio 1970, n. 300.

5.2 Sanzioni relative ai dipendenti

La violazione da parte dei dipendenti delle singole regole comportamentali di cui al presente Modello costituisce infrazione disciplinare.

I provvedimenti disciplinari irrogabili al personale, nel rispetto delle procedure previste dalla legge, sono quelli previsti dalla contrattazione collettiva applicata ai singoli rapporti di lavoro, in proporzione alla gravità dell'infrazione. Potrà essere applicata anche la sanzione del licenziamento per giusta causa, ricorrendo i presupposti di cui all'art. 2119 cod. civ.

Per quanto riguarda l'accertamento delle violazioni e l'irrogazione della sanzione, la competenza è estesa all'Organismo di vigilanza, così come ad esso è estesa la competenza per il monitoraggio del comportamento dei dipendenti nella specifica prospettiva dell'osservanza del Modello Organizzativo.

5.3 Sanzioni relative ai collaboratori e ai soggetti esterni

Ogni violazione delle regole del Modello Organizzativo applicabili a collaboratori esterni è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti, clausole che potranno prevedere la risoluzione del rapporto contrattuale ovvero il diritto di recesso dal medesimo.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti all'ente, come nel caso di applicazione alla stessa da parte dell'autorità giudiziaria delle misure sanzionatorie previste dal D.Lgs. n. 231/2001.

L'OdV verifica che nella modulistica contrattuale sia inserita una clausola di conoscenza del MOG e del relativo Codice Etico, come da fac simile di seguito indicato:

"Il contraente (fornitore, collaboratore o altro...) dichiara di essere a conoscenza della normativa vigente in materia di responsabilità amministrativa della persona giuridica e, in particolare, del disposto di cui al d. lgs. n. 231/01 e s.m.i., nonché dei contenuti del MOG e del relativo Codice Etico adottato dall'Istituto Salesiano San Marco. A tale riguardo dichiara che la propria attività e quella di eventuali propri dipendenti e collaboratori è improntata al rispetto della normativa vigente e dell'insieme di valori di etica dell'ente, e alla astensione da qualsiasi comportamento idoneo a configurare le ipotesi di reato di cui al menzionato decreto legislativo. L'inosservanza di tale impegno è considerata dalle Parti un inadempimento grave e motivo di risoluzione del contratto, che legittimerà l'ente a risolvere lo stesso con effetto immediato, fatto salvo, in ogni caso, il risarcimento dei danni subiti".

5.4 Sanzioni relative ai dirigenti

Quando la violazione delle regole previste dal presente MOG o l'adozione, nell'espletamento di attività sensibili, di un comportamento non conforme alle prescrizioni del MOG stesso è compiuta da dirigenti, si provvederà ad applicare nei confronti dei responsabili la misura ritenuta più idonea in conformità a quanto previsto dal Codice Civile, allo Statuto dei Lavoratori e al relativo contratto nazionale.

Quale sanzione specifica potrà essere disposta anche la sospensione delle procure eventualmente conferite al dirigente stesso.

SEZIONE 6 – NORMATIVA DI RIFERIMENTO

6.1 Reati da prevenire

I reati cui si applica la disciplina dettata dal D.Lgs. 8 giugno 2001, n. 231 e s.m.i., e che sono specificamente indicati dal presente Modello Organizzativo per quanto attiene ai fatti che più verosimilmente potrebbero riguardare l'ente **Istituto Salesiano San Marco**, sono:

- art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico;
- art. 24 bis - Delitti informatici e trattamento illecito dei dati;
- art. 24 ter - Delitti di criminalità organizzata;
- art. 25 - Concussione, induzione indebita a dare o a promettere utilità e corruzione;
- art. 25 quinquies - Delitti contro la personalità individuale;
- art. 25 septies - Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- art. 25 octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;
- art. 25 nonies - Delitti in materia di violazione del diritto d'autore;
- art. 25 decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

Attesa la natura giuridica dell'ente e altresì le sue attività tipiche, è da ritenersi che i reati di cui agli artt. 25 bis (falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento), 25 bis.1. (delitti contro l'industria e il commercio) 25 ter (reati societari), 25 quater.1

(Pratiche di mutilazione degli organi genitali femminili), 25 quater (delitti con finalità di terrorismo o di eversione dell'ordine democratico), 25 sexies (abusi di mercato), 25 undecies (reati ambientali), 25 duodecies (impiego di cittadini di paesi terzi in cui soggiorno è irregolare), art. 24 ter (illegale fabbricazione, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di comuni armi da sparo), art. 24 quater (sequestro di persona a scopo di rapina o di estorsione;), siano a rischio di commissione molto basso o inesistente.

6.2 Esonero dell'ente da responsabilità amministrativa

Nel caso in cui venga commesso uno dei reati suindicati, alla responsabilità penale della persona fisica che ha realizzato materialmente il fatto si aggiunge, se ed in quanto siano integrati tutti gli altri presupposti normativi, anche la responsabilità amministrativa dell'ente.

Gli artt. 6 e 7 D.Lgs. n. 231/2001 prevedono, tuttavia, l'esonero dalla responsabilità, qualora l'ente dimostri di avere adottato ed efficacemente attuato modelli di organizzazione e gestione idonei a prevenire la realizzazione degli illeciti penali.

L'ente nelle prime due ipotesi prima indicate, quelle che riguardano le posizioni di vertice, non risponde se dà la prova liberatoria che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- è stato affidato ad un Organismo dell'ente, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'osservanza dei modelli organizzativi e di curare il loro aggiornamento;
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo autonomo di vigilanza interna.

Nella terza ipotesi, che riguarda i soggetti direttamente sottoposti alle figure di vertice, è stata esclusa la presunzione di responsabilità, sicché l'ente è responsabile solo se viene dimostrato che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione (culpa in eligendo) o vigilanza (culpa in vigilando).

Il presente Modello Organizzativo è l'insieme delle regole interne di cui l'ente **Istituto Salesiano San Marco** si è dotato in funzione delle specifiche attività svolte e dei relativi rischi connessi.

Il Modello Organizzativo, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, è stato formato in modo da rispondere alle seguenti esigenze:

1. individuare le attività nel cui ambito possono essere commessi reati;
2. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
3. individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
4. prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza del modello stesso.

L'osservanza degli obblighi di direzione e vigilanza, invece, è incontestabile quando vi sia l'adozione e l'efficace attuazione di un modello di organizzazione, gestione e controllo idoneo a prevenire i reati, attuato attraverso sue verifiche periodiche e la sua eventuale modifica, quando siano scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività.

Il legislatore ha, poi, introdotto un elemento comune sia all'adozione di corretti modelli organizzativi che all'adempimento degli obblighi di direzione e vigilanza: l'introduzione di un sistema disciplinare idoneo a

sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo ovvero nell'esercizio dei poteri direttivi.

Il sistema congegnato dal Modello Organizzativo adottato dall'ente risponde, infine, alle ulteriori seguenti esigenze individuate dal D.Lgs. n. 231/2001:

- istituzione di un Organismo di controllo, con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello Organizzativo, nonché di curarne l'aggiornamento;
- assenza di colpa da parte dell'Organismo di controllo per omessa o insufficiente vigilanza in merito all'attuazione e all'osservanza del Modello Organizzativo;
- predisposizione di un sistema di verifica periodica e di eventuale aggiornamento del Modello Organizzativo;
- commissione del reato con elusione fraudolenta delle disposizioni del Modello Organizzativo.

SEZIONE 7 – REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Nell'individuare i reati realizzabili nell'ambito dei rapporti tra l'ente **Istituto Salesiano San Marco** e la pubblica amministrazione si persegue l'obiettivo di indurre gli organi dell'ente stesso, i dipendenti e, in generale, tutti i collaboratori ad adottare regole di condotta conformi a quanto prescritto dal Modello Organizzativo, al fine di prevenire il verificarsi di questi reati.

7.1 Nozioni relative alla pubblica amministrazione

Per «pubblica amministrazione» si intendono tutti gli enti pubblici, territoriali e non, i membri e gli organi interni degli enti, compresi i pubblici funzionari e gli incaricati di pubblici servizi.

Agli effetti della legge penale viene comunemente considerato come «ente della pubblica amministrazione» qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

Ai sensi dell'art. 357, primo comma, cod. pen., è considerato pubblico ufficiale agli effetti della legge penale colui il quale esercita una pubblica funzione legislativa, giudiziaria o amministrativa. Il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale, «è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo volgersi per mezzo di poteri autoritativi o certificativi».

Ai sensi dell'art. 358 cod. pen. sono considerati soggetti incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per «pubblico servizio» deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni d'ordine e della prestazione di opera meramente materiale.

7.2 Elenco dei reati

7.2.1 Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis cod. pen. - art. 24 d.lgs.231/01)

Il reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, a prescindere dal fatto che l'attività programmata si sia effettivamente svolta).

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	gestione rendicontazione di contributi per attività scolastiche e formative	- consulenza esterna - coordinamento delle attività ispettoriali - controllo in itinere e finale della gestione documentale da parte dell'economista dell'ente - lavoro in equipe

7.2.2 Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter cod. pen. - art. 24 d.lgs.231/01)

Il reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute - si ottengono, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	richieste di contributi finanziamenti per attività e opere	- comunicazioni ufficiali tramite documenti cartacei - utilizzo della posta elettronica certificata - nessuna delega - firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - controllo da parte dell'economista dell'ente

7.2.3 Concussione - Induzione indebita a dare o promettere utilità (art. 317 cod. pen. - art. 319 quater cod. pen. - art. 25 d.lgs.231/01)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovute. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal D.Lgs. n. 231/2001.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	richieste di contributi finanziamenti per attività e opere	- comunicazioni ufficiali tramite documenti cartacei - utilizzo della posta elettronica certificata - nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - denuncia tempestiva all'autorità giudiziaria qualora in possesso di elementi probatori

7.2.4 Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319-320-321 cod. pen. - art. 25 d.lgs.231/01)

Il reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente). L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare l'evasione di una pratica), sia in un atto contrario ai suoi doveri (ad esempio: garantire l'aggiudicazione di una gara). Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	rapporti con la pubblica amministrazione	- comunicazioni ufficiali tramite documenti cartacei - utilizzo della posta elettronica certificata - nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - denuncia tempestiva all'autorità giudiziaria qualora in possesso di elementi probatori

7.2.5 Istigazione alla corruzione (art. 322 cod. pen. - art. 25 d.lgs.231/01)

Il reato si configura tutte le volte in cui, in presenza di un comportamento finalizzato alla commissione di un reato di corruzione, questa non si perfezioni in quanto il pubblico ufficiale rifiuta l'offerta o la promessa non dovuta e illecitamente avanzatagli per indurlo a compiere ovvero a omettere o ritardare un atto del suo ufficio. Sostanzialmente si tratta della fattispecie descritta nel capoverso precedente, nella quale però l'offerta non venga accettata dal pubblico funzionario.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	rapporti con la pubblica amministrazione	- comunicazioni ufficiali tramite documenti cartacei - utilizzo della posta elettronica certificata - nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - denuncia tempestiva all'autorità giudiziaria qualora in possesso di elementi probatori

7.2.6 Corruzione in atti giudiziari (art. 319-ter cod. pen. - art. 25 d.lgs.231/01)

Il reato si configura nel caso in cui l'Ente sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	pendenza di un procedimento giudiziario	comunicazioni ufficiali e costante scambio informativo con professionista incaricato di assistenza e patrocinio

7.2.7 Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis cod. pen. - art. 25 d.lgs.231/01)

Questa norma estende ai membri delle Comunità europee i reati di istigazione alla corruzione e quelli di peculato, concussione e corruzione.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
--------------------	--------------------	--------------

BASSO	domande di accesso a fondi europei diretti domande contributi per attività scolastiche e formative	- nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - comunicazioni ufficiali tramite le procedure standardizzate richieste - utilizzo della posta elettronica certificata e portali ufficiali dedicati
-------	---	---

7.2.8 Malversazione a danno dello Stato (art. 316 bis cod. pen. - art. 24 d. lgs. 231/01) - Indebita percezione di erogazioni a danno dello Stato (art. 316 ter cod. pen. - art. 24 d.lgs. 231/01)

Il reato si configura nel caso in cui, avendo ottenuto dallo Stato o da altro ente pubblico o dall'Unione europea contributi sovvenzioni o finanziamenti per realizzare opere o svolgere attività di pubblico interesse, questi non vengano destinati alle predette finalità, ovvero tali contributi vengano ottenuti mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere o mediante l'omissione di informazioni dovute,

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	richieste di contributi finanziamenti per attività e opere	- nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - comunicazioni ufficiali tramite le procedure standardizzate richieste - utilizzo della posta elettronica certificata e portali ufficiali dedicati - sistemi di contabilità separata e tracciabilità di finanziamenti - predisposizione di sistemi di rendicontazione

7.2.9 Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2, n. 1, cod. pen. - art. 24 d. lgs. 231/01)

Il reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro ente pubblico o all'Unione Europea).

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	richieste di contributi finanziamenti per attività e opere	- nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - comunicazioni ufficiali tramite le procedure standardizzate richieste - utilizzo della posta elettronica certificata e portali ufficiali dedicati - sistemi di contabilità separata e tracciabilità di finanziamenti - predisposizione di sistemi di rendicontazione

7.2.10 Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis cod. pen. - art. 24 d. lgs. 231/01)

Il reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche. Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad

esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	richieste di contributi finanziamenti per attività e opere	- nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - comunicazioni ufficiali tramite le procedure standardizzate richieste - utilizzo della posta elettronica certificata e portali ufficiali dedicati

7.2.11 Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter cod. pen. - art. 24 d. lgs. 231/01)

Il reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico, o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	richieste di contributi finanziamenti per attività e opere partecipazione a gare pubbliche	- nessuna delega e firma esclusiva di chi è in funzione formale apicale (direttore o legale rappresentante) - comunicazioni ufficiali tramite le procedure standardizzate richieste - utilizzo della posta elettronica certificata e portali ufficiali dedicati

7.3 Processi ed eventi sensibili

I principali processi sensibili su identificati pretendono che tutte le attività sensibili siano svolte conformandosi alle leggi vigenti, al Codice Etico ed alle regole contenute nel presente Modello Organizzativo.

7.4 Deleghe e procure

Il sistema di deleghe e di procure è caratterizzato da elementi di sicurezza che garantiscono la rintracciabilità e l'evidenza delle operazioni svolte a fronte di delega, consentendo comunque la gestione efficiente delle opere istituzionali, nel rispetto delle norme dettate dal libro I titolo VIII del codice di diritto canonico in materia di potestà di governo.

Ai soli fini di cui al presente Modello Organizzativo la «delega» è un atto interno di attribuzione di compiti e la «procura» un atto unilaterale con il quale viene conferito ad un soggetto il potere di rappresentanza.

Ai responsabili di unità organizzativa cui, per lo svolgimento dei loro incarichi, si vogliono attribuire poteri di rappresentanza viene rilasciata apposita procura con poteri adeguati e coerenti con i compiti e le funzioni assegnati per delega.

In generale il sistema delle deleghe prevede che:

- le deleghe siano coerenti con la posizione organizzativa ed aggiornate in conseguenza a variazioni organizzative;
- in ogni delega siano specificati i poteri del delegato ed il soggetto cui il delegato riporta;
- i poteri specificati nella delega siano allineati e coerenti con le necessità dell'opera;

- il delegato possieda autonomia decisionale e di spesa adeguati alla funzione e ai compiti conferiti, nei limiti segnati dalle norme che disciplinano l'ente ecclesiastico e dalle norme del diritto canonico e di quello proprio.

In generale il sistema delle procure prevede che:

- le procure siano assegnate a soggetti provvisti di delega;
- le procure individuino e delimitino i poteri conferiti;
- le procure siano assegnate a religiosi appartenenti all'ente, ovvero a professionisti per l'espletamento di incarichi professionali per l'esecuzione dei quali sia indispensabile il rilascio di specifica procura.

7.5 Controlli dell'Organismo di vigilanza

L'Organismo di vigilanza accede, in qualunque momento, agli archivi delle funzioni che intervengono nei processi potenzialmente interessati dai reati e verifica:

- il procedimento seguito;
- la presenza della documentazione a supporto delle singole fasi dei processi;
- il rispetto delle responsabilità definite.

SEZIONE 8 – REATI CONTRO LA VITA E L'INCOLUMITÀ INDIVIDUALE

Nel descrivere i reati realizzabili contro la vita e l'incolumità individuale si persegue l'obiettivo di indurre gli organi dell'ente, i dipendenti e, in generale, tutti i collaboratori ad adottare regole di condotta conformi a quanto prescritto, non soltanto dal Modello Organizzativo, ma pure dal piano di sicurezza adottato ai sensi del D.Lgs. 9 aprile 2008, n. 81, al fine di prevenire il verificarsi di questi reati.

8.1 Elenco dei reati

8.1.1 Omicidio colposo con violazione delle norme sulla prevenzione degli infortuni sul lavoro (art. 589, comma 2, cod. pen. - art. 25 septies d.lgs. 231/01)

Il reato si configura quando si cagiona per colpa, consistente nella violazione delle norme per la prevenzione degli infortuni sul lavoro, la morte di una persona.

Tra i reati che offendono i beni essenziali l'omicidio è senz'altro il più rilevante, consistendo nell'uccisione di una persona provocata da altra persona mediante un comportamento doloso o colposo ed in assenza di cause di giustificazione.

L'oggetto della tutela penale è, così, direttamente la vita umana, che viene perseguito, perfino contro la volontà dello stesso soggetto interessato, quale interesse della collettività (tanto che l'art. 579 cod. pen. punisce pure l'omicidio del consenziente).

Se l'oggetto materiale dell'azione criminosa è sempre un essere umano, il fatto materiale dell'omicidio concreta un reato a forma libera, poiché è indifferente il modo attraverso il quale la morte viene data e può consistere sia in un'azione positiva che in un'azione omissiva; sia nell'uso di mezzi fisici che psichici, diretti o indiretti.

L'omicidio è colposo quando l'agente determina la morte della persona per colpa.

Per l'individuabilità della circostanza aggravante del fatto commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro nell'omicidio colposo, è sufficiente che sussista legame causale tra

la violazione e l'evento dannoso; legame che ricorre tutte le volte che il fatto sia ricollegabile all'inosservanza delle norme stesse, secondo i principi dettati dagli artt. 40 e 41 cod. pen. Occorre, inoltre, che sia stata posta in essere una condotta antiggiuridica contemplata, anche in forma generica, da qualsiasi norma comunque preordinata alla prevenzione degli infortuni sul lavoro.

La terminologia adoperata dal codificatore («norme per la prevenzione degli infortuni sul lavoro»), è riferibile, peraltro, non solo alle norme inserite nelle leggi specificamente antinfortunistiche, ma anche a tutte quelle che, direttamente o indirettamente, perseguono il fine di evitare incidenti sul lavoro o malattie professionali e che, in genere, tendono a garantire la sicurezza del lavoro in relazione all'ambiente in cui esso deve svolgersi.

Prima tra tali norme è, allora, quella posta dall'art. 2087 cod. civ., che istituisce il generalissimo principio dell'obbligo del datore di lavoro di tutelare le condizioni di lavoro, per tali intendendosi sia l'integrità fisica che la personalità morale dei prestatori di lavoro; tale norma, infatti, ha carattere sussidiario, di integrazione della specifica normativa antinfortunistica, con riferimento all'interesse primario della garanzia della sicurezza del lavoro ed importa l'inadempimento del dovere di sicurezza, non soltanto quando si inattuino le misure specifiche imposte tassativamente dalla legge, ma pure quando non si adottino, in mancanza di queste o nell'ipotesi della loro inadeguatezza rispetto all'evoluzione della tecnica ed al progresso scientifico, i mezzi comunque idonei a prevenire ed evitare i sinistri, assunti con i sussidi dei dati di comune esperienza, prudenza, diligenza, prevedibilità, in relazione all'attività svolta.

Oltre all'attuazione dell'art. 2087 cod. civ., ai fini della prevenzione degli infortuni sul lavoro sono da rispettare non soltanto le norme specifiche contenute nelle speciali leggi antinfortunistiche ma anche quelle che, seppure stabilite da leggi generali, sono ugualmente dirette a prevenire gli infortuni.

L'omicidio colposo aggravato dalla violazione di norme antinfortunistiche può concorrere con altri reati. L'omissione di impianti o di segnali destinati alla prevenzione degli infortuni (art. 437 cod. pen.), anche se ascritta come reato autonomo, opera pure come circostanza aggravante del concorrente reato di omicidio colposo, essendo distinti e giuridicamente autonomi gli interessi offesi, rispettivamente la pubblica incolumità e la vita della persona; il che giustifica l'applicabilità al reato di omicidio colposo della circostanza aggravante della violazione delle norme per la prevenzione degli infortuni sul lavoro, che pure costituisce la condotta tipica descritta dall'art. 437 cod. pen. Il danno alla persona, infatti, non è compreso nell'ipotesi complessa di cui al capoverso dell'art. 437, costituendo la morte effetto soltanto eventuale e non essenziale del disastro o dell'infortunio causato dall'omissione delle cautele: la punizione dell'uno e dell'altro reato, pertanto, non comporta duplice condanna per lo stesso fatto in quanto, essendo diverse le condotte e le rispettive oggettività giuridiche, non si può verificare assorbimento per diversità dell'elemento soggettivo, rispettivamente dolo e colpa.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	ambienti e luoghi di lavoro	• documento di valutazione dei rischi (DVR) • formazione e informazione dei dipendenti • coordinamento e verifiche periodiche con RSPP

8.1.2 Lesioni personali colpose aggravate dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro (art. 590, comma 3, cod. pen. - - art. 25 septies d.lgs. 231/01)

Il delitto di lesioni personali colpose è quello che più di frequente si accompagna alle condotte represses dal diritto penale del lavoro, anche perché rappresenta il risvolto penalistico del danno biologico.

L'evento, costituito dalle lesioni subite in assenza di dolo dell'autore dalla parte offesa, ricorre spesso nelle ipotesi di violazione delle norme lavoristiche: basta porre mente non solo alle evidenti conseguenze degli inadempimenti ai precetti antinfortunistici ed igienici, ma pure al danno alla salute, inteso come alterazione dell'equilibrio psico-fisico del soggetto, che quasi sempre si accompagna a comportamenti anche solo civilisticamente illeciti del datore di lavoro, quali ad esempio il licenziamento

invalido, il demansionamento e la dequalificazione professionale, o l'uso illegittimo del potere disciplinare.

La circostanza aggravante della violazione di specifiche norme per la prevenzione degli infortuni sul lavoro sussiste anche per l'omessa adozione di ogni idonea misura a protezione dell'integrità fisica dei lavoratori, in violazione dell'art. 2087 cod. civ.

La terminologia «norme per la prevenzione degli infortuni sul lavoro» è, infatti, riferibile non soltanto alle norme inserite nelle leggi specificamente antinfortunistiche, ma anche a tutte quelle che, direttamente o indirettamente, perseguono il fine di evitare incidenti sul lavoro o malattie professionali, le quali tendono in genere a garantire la sicurezza del lavoro in relazione all'ambiente in cui deve svolgersi.

E in tema di prevenzione degli infortuni sul lavoro il disposto dell'art. 2087 ha carattere generale e non meramente contrattuale, come si desume dallo stessa rubrica («tutela delle condizioni di lavoro») nonché dal suo particolare contenuto normativo.

Ne consegue, pertanto, che, quantunque la norma sia inserita nel codice civile, anziché in una legge speciale, pone specifici doveri di comportamento, la cui effettiva inosservanza integra conseguentemente il delitto aggravato di cui al terzo comma dell'art. 590 cod. pen., allorché sia stata causa del relativo evento lesivo ai sensi dell'art. 40 cod. pen.

L'ultimo comma dell'art. 590 cod. pen., ai fini della perseguibilità d'ufficio del reato di lesioni personali colpose, annovera le lesioni commesse con violazione delle norme antinfortunistiche, delle norme relative all'igiene sul lavoro o determinanti malattie professionali; il terzo comma contempla invece come aggravante solo la violazione delle norme per la prevenzione degli infortuni sul lavoro: dal rapporto tra tali commi deve dedursi che non è consentito ricomprendere estensivamente la violazione delle norme sull'igiene del lavoro tra le ipotesi aggravate.

Il reato di lesioni personali colpose è istantaneo, consumandosi al momento dell'insorgere della malattia prodotta dalle lesioni.

Durata e permanenza della malattia sono irrilevanti ai fini dell'individuazione del momento consumativo; se la condotta colposa causatrice della malattia non cessa, però, con l'insorgenza di questa, ma persistendo ne provochi un successivo aggravamento, il reato si consuma nel momento in cui si verifica l'ulteriore debilitazione.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	ambienti e luoghi di lavoro	- DVR - formazione e informazione dei dipendenti - coordinamento e verifiche periodiche con RSPP

8.2 Processi ed eventi sensibili

In relazione ai principali processi sensibili suindividuati, al fine di prevenire la potenziale commissione dei reati sopra elencati è stato adottato il piano di sicurezza di cui all'art. 100 D.Lgs. 9 aprile 2008, n. 81, e varate le misure generali e specifiche di tutela del lavoro.

Il riesame e l'eventuale modifica del Modello Organizzativo saranno adottati quando fossero scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

In particolare si è proceduto alla valutazione dei rischi per la salute e la sicurezza, tendendo all'eliminazione dei rischi e, nell'impossibilità, alla loro riduzione al minimo nonché alla riduzione dei rischi alla fonte; alla programmazione della prevenzione; alla sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso; all'utilizzo limitato degli agenti chimici, fisici e biologici sui luoghi di

lavoro; all'adozione delle misure igieniche e delle misure di protezione collettiva ed individuale imposte dalle leggi in materia e suggerite dal progresso tecnologico e scientifico; all'uso di segnali di avvertimento e di sicurezza.

Sono state inoltre predisposte le misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave ed immediato; è prevista la regolare manutenzione di ambienti, attrezzature, macchine ed impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti.

L'ente ritiene imprescindibile assicurare l'adempimento di tutti gli obblighi giuridici relativi:

- al rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Al fine di verificare l'adempimento degli obblighi giuridici di cui sopra in relazione alla prevenzione dei reati di omicidio colposo con violazione delle norme sulla prevenzione degli infortuni sul lavoro e di lesioni personali colpose aggravate dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro, il responsabile del servizio di prevenzione e di protezione di cui all'art. 2, comma 1, lett. f), D.Lgs. 9 aprile 2008, n. 81, rimetterà periodicamente all'Organismo di vigilanza una relazione in cui sia dato conto sia dei dati rilevati attraverso l'adozione di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività anzidette, sia dell'osservanza di tutte le regole di condotta che garantiscano la conformità del Modello Organizzativo alle linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 ovvero al British Standard OHSAS 18001:2007. L'Organismo di vigilanza segnalerà alla direzione eventuali deficienze organizzative e gestionali che impediscano od ostacolino il soddisfacimento dell'esigenza di far sì che, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, l'ente adotti un'articolazione di funzioni che assicuri le competenze tecniche ed i poteri necessari per la verifica, la valutazione, la gestione ed il controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo al fine di prevenire i reati contro la vita e l'incolumità individuale.

L'ente ritiene essenziale, comunque, l'informazione, la formazione, la consultazione e la partecipazione dei lavoratori, ovvero dei loro rappresentanti, sulle questioni riguardanti la sicurezza e la salute sui luoghi di lavoro.

SEZIONE 9 – REATI CONTRO LA PERSONALITÀ DELL'INDIVIDUO

Nel descrivere i reati realizzabili contro la personalità dell'individuo si persegue l'obiettivo di indurre gli organi dell'ente, i dipendenti e, in generale, tutti i collaboratori ad adottare regole di condotta conformi a quanto prescritto dal Modello Organizzativo al fine di prevenire il verificarsi di questi reati.

9.1 Elenco dei reati

9.1.1 Riduzione in schiavitù (art. 600 cod. pen. - art. 25 quinquies d.lgs. 231/01)

Il reato si configura quando una persona viene ridotta in schiavitù o in una condizione analoga alla schiavitù, consistente nello stato di un individuo sul quale si esercitano gli attributi del diritto di proprietà o alcuni di essi o di mantenimento in uno stato di soggezione continuativa, mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività educative	- regolamento di Istituto - assistenza e vigilanza diretta dei religiosi appartenenti alla comunità - selezione del personale - formazione del personale - coordinamento con il personale docente

9.1.2 Prostituzione minorile (art. 600-bis cod. pen. - art. 25 quinquies d.lgs. 231/01)

Il reato si realizza qualora qualcuno induca alla prostituzione una persona minore di anni 18, ovvero ne favorisca o sfrutti la prostituzione.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività educative	- regolamento di Istituto - assistenza e vigilanza diretta dei religiosi appartenenti alla comunità - selezione del personale - formazione del personale - coordinamento con il personale docente

9.1.3 Pornografia minorile (art. 600-ter cod. pen. - art. 25 quinquies d.lgs. 231/01) - Pornografia virtuale (art. 600 quater.1 cod. pen.)

Il reato consiste nello sfruttamento di minori al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico ovvero nel fare commercio o nel distribuire, divulgare o pubblicizzare materiale pornografico o, ancora, nel distribuire e divulgare notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori o, infine, nel cedere ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento di minori. Il reato si configura anche nell'ipotesi in cui il materiale pornografico rappresenti immagini virtuali realizzate utilizzando immagini di minori. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

La configurazione in capo all'ente di questo reato attiene alle misure adottate dall'ente stesso per limitare l'uso degli accessi a siti Internet e l'installazione di programmi non autorizzati sui computer in dotazione all'Istituto.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività educative	- adozione di filtri informatici - identificazione degli accessi con username e password

		• regolamento di Istituto • assistenza e vigilanza diretta dei religiosi • firma del progetto educativo • selezione del personale • formazione del personale • coordinamento con il personale docente • colloqui personali di ingresso
--	--	--

9.1.4 Detenzione di materiale pornografico (art. 600-quater cod. pen. - art. 25 quinquies d.lgs. 231/01) - Pornografia virtuale (art. 600 quater.1 cod. pen.)

Il reato si perfeziona nel momento in cui un soggetto consapevolmente si procura o disponga di materiale pornografico prodotto mediante lo sfruttamento sessuale di minori. Il reato si configura anche nell'ipotesi in cui il materiale pornografico rappresenti immagini virtuali realizzate utilizzando immagini di minori. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Anche per questo reato la sua configurazione in capo all'ente attiene alle misure adottate per limitare l'uso degli accessi a siti Internet e l'installazione di programmi non autorizzati sui computer in dotazione all'Istituto.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività educative	• adozione di filtri informatici • identificazione degli accessi con username e password • regolamento di Istituto • assistenza e vigilanza diretta dei religiosi • firma del progetto educativo • selezione del personale • formazione del personale • coordinamento con il personale docente • colloqui personali di ingresso

9.1.5 Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies cod. pen. - art. 25 quinquies d.lgs. 231/01)

Il reato consiste nell'organizzazione e propaganda di viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività educative e ricreative	selezione di idonei vettori e agenzie

9.2 Processi ed eventi sensibili

In relazione ai principali processi sensibili suindividuati, al fine di prevenire la potenziale commissione di alcuni dei reati sopra elencati tramite l'utilizzo degli strumenti informatici messi a disposizione dall'ente:

- è stato adottato il documento programmatico sulla sicurezza di cui al D.Lgs. 30 giugno 2003, n. 196;
- sono state adottate misure preventive sui sistemi informatici volte a limitare l'accesso a siti Internet potenzialmente a rischio;

- è vietata l'installazione di software sui personal computer utilizzati da ciascun dipendente senza la preventiva autorizzazione del superiore gerarchico.

Viene, inoltre, espressamente fatto rilevare a tutti i dipendenti che gli strumenti informatici a loro disposizione devono essere utilizzati per i soli fini strettamente inerenti all'attività lavorativa.

La dottrina sociale della Chiesa cattolica impone il rispetto della dignità dell'uomo dal concepimento alla morte e l'adempimento dei diritti naturali della persona nel lavoro, sicché non è tollerata alcuna forma di lavoro irregolare o non conforme alla normativa vigente.

SEZIONE 10 – REATI CONTRO IL PATRIMONIO MEDIANTE FRODE

Tra i delitti contro il patrimonio commessi mediante frode rientrano i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita. La repressione e la prevenzione di questi reati assumono particolare rilevanza nel contrasto del riciclaggio e del finanziamento del terrorismo:

Nell'individuare i reati di cui si tratta si deve perseguire l'obiettivo di indurre gli organi, i membri, i dirigenti, i dipendenti e, in generale, tutti i collaboratori dell'ente ad adottare regole di condotta conformi a quanto prescritto dal Modello Organizzativo al fine di evitare, nell'agire dell'ente o nell'occasione del suo agire, l'utilizzo del sistema finanziario e di quello economico per finalità di riciclaggio o di finanziamento del terrorismo, con l'intento di prevenire il verificarsi dei seguenti reati, il cui comune presupposto è quello della provenienza da delitto del denaro e dell'altra utilità di cui l'agente sia venuto a disporre.

10.1 Elenco dei reati

10.1.1 Ricettazione (art. 648 cod. pen. - art. 25 octies d.lgs. 231/01)

Il delitto è commesso da chi, fuori dei casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare. La ricettazione si distingue dal riciclaggio in senso stretto perché quest'ultimo riguarda le attività che si esplicano sul bene di provenienza delittuosa trasformandolo o modificandolo parzialmente, nonché quelle che, senza incidere sulla cosa ovvero senza alterarne i dati esteriori, sono comunque di ostacolo per la ricerca della sua provenienza delittuosa. Essa, poi, si distingue sia dal riciclaggio che dall'impiego di denaro, beni o utilità di provenienza illecita per essere presente nella ricettazione solo una generica finalità di profitto, mentre le altre due fattispecie reitali richiedono la specifica finalità di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità, quanto all'ultima delle due, che detta finalità deve essere perseguita mediante l'impiego delle risorse in attività economiche o finanziarie. La ricettazione è ravvisabile tutte le volte in cui la condotta delittuosa cada, oltre che sul denaro, su una cosa che abbia un certo valore, anche se non puramente economico, qualunque sia la sua misura; perciò anche la ricettazione di oggetti provenienti da un delitto che non sia contro il patrimonio si configura ugualmente come reato attinente al patrimonio, in dipendenza dell'illecito incremento patrimoniale derivante dall'acquisizione di beni di illegittima provenienza. Ulteriore presupposto della ricettazione è dunque l'esistenza di un delitto anteriore, seppure non è ancora giudizialmente accertato.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	acquisto e	• adozione di protocolli e procedure nelle attività di

	approvvigionamento di lavori servizi e forniture attività di gestione pagamenti e incassi	dichiarazione dei redditi e nel ciclo di fatturazione attiva e passiva • individuazione di modalità di qualificazione delle imprese fornitrici • selezione e verifica delle controparti contrattuali
--	--	---

10.1.2 Riciclaggio (art. 648-bis cod. pen. - art. 25 octies d.lgs. 231/01)

Commette il delitto chiunque, fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa: la pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. Il reato si commette attraverso il compimento delle specifiche operazioni di sostituzione e di trasferimento, nonché a quelle che ostacolano l'identificazione della provenienza delittuosa delle cose o delle altre utilità; non è richiesta, invece, la finalizzazione della condotta al rientro del bene «ripulito» nella disponibilità dell'autore del reato presupposto.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	• acquisto e approvvigionamento di lavori servizi e forniture • attività di gestione pagamenti e incassi	• adozione di protocolli e procedure nelle attività di dichiarazione dei redditi e nel ciclo di fatturazione attiva e passiva • individuazione di modalità di qualificazione delle imprese fornitrici • selezione e verifica delle controparti contrattuali

10.1.3 Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter cod. pen. - art. 25 octies d.lgs. 231/01)

Commette il delitto chiunque, fuori dei casi di concorso nel reato e dei casi di ricettazione o riciclaggio, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto; anche per tale reato la pena è aumentata quando il fatto sia commesso nell'esercizio di un'attività professionale.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	• acquisto e approvvigionamento di lavori servizi e forniture • attività di gestione pagamenti e incassi	• adozione di protocolli e procedure nelle attività di dichiarazione dei redditi e nel ciclo di fatturazione attiva e passiva • individuazione di modalità di qualificazione delle imprese fornitrici • selezione e verifica delle controparti contrattuali

10.1.4 Autoriciclaggio (art. 648 ter.1 cod. pen. - art. 25 octies d.lgs. 231/01)

Tale ipotesi di reato si configura nel caso in cui chiunque avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce trasferisce in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	• acquisto e approvvigionamento di lavori servizi e	• adozione di protocolli e procedure nelle attività di dichiarazione dei redditi e nel ciclo di fatturazione attiva e passiva

	forniture • attività di gestione pagamenti e incassi	• individuazione di modalità di qualificazione delle imprese fornitrici • selezione e verifica delle controparti contrattuali
--	--	---

10.2 Processi ed eventi sensibili

In tutti i principali processi sensibili suindividuati può presentarsi l'occasione della commissione dei reati contemplati dalla normativa antiriciclaggio e antiterrorismo, ma soprattutto in quelli attinenti alla gestione del patrimonio dell'ente, con particolare riguardo all'alienazione o alla concessione di diritti reali od obbligatori sui beni immobili che ne fanno parte, sol che si consideri che per «riciclaggio» devono intendersi quelle azioni intenzionali dirette a: a) conversione o trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; b) occultamento o dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; c) acquisto, detenzione o utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; d) partecipazione ad uno degli atti su indicati, associazione per commettere tale atto, tentativo di perpetrarlo, nonché il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione.

Per «finanziamento del terrorismo» si deve intendere, invece, qualsiasi attività diretta, con qualunque mezzo, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, comunque realizzati, destinati ad essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo previsti dal codice penale, e ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti.

In relazione ai principali processi sensibili su individuati, al fine di prevenire la potenziale commissione di alcuni dei reati sopra elencati tramite l'utilizzo degli strumenti informatici messi a disposizione dall'ente:

- è stato adottato il documento programmatico sulla sicurezza di cui al D.Lgs. 30 giugno 2003, n. 196;
- sono state adottate misure preventive sui sistemi informatici volte a limitare l'accesso a siti Internet potenzialmente a rischio;

SEZIONE 11 REATI SOCIETARI ED ALTRI REATI

La qualità di ente non commerciale rende impossibile, anche in considerazione del tipo di attività che esso gestisce - di natura religiosa, di culto, educativa e socio-assistenziale - riferire ad essa altre categorie di reati, pure previste dal D.Lgs. n. 231/2001.

SEZIONE 12 – REATI INFORMATICI

12.1 Elenco dei reati

12.1.1 Accesso abusivo ad un sistema informatico o telematico (art. 615-ter cod. pen. - art. 24 bis d.lgs. 201/01)

Commette il delitto chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Il legislatore vuole assicurare la protezione del «domicilio informatico», quale spazio ideale, ma anche fisico in cui sono contenuti i dati informatici, di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. La norma, peraltro, non si limita a tutelare i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nel diritto di escludere gli altri da questo domicilio, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente. La conseguenza è che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati tanto se il titolare del diritto di esclusiva è persona fisica, quanto se sia persona giuridica o altro ente.

Il delitto, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa.

Per «sistema informatico» deve intendersi un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche parziale, di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di codificazione e decodificazione - dalla registrazione o memorizzazione, attraverso impulsi elettronici, su supporti adeguati, di «dati». Per «dati», poi, si intendono rappresentazioni elementari di un fatto, effettuata attraverso simboli («bit»), in combinazione diverse; dall'elaborazione automatica dei dati si generano «informazioni», costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.

Ben possono concorrere i reati di accesso abusivo ad un sistema informatico e di frode informatica, in quanto si tratta di reati totalmente diversi, il secondo dei quali postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del primo: la differenza fra le due ipotesi criminose si ricava, inoltre, dalla diversità dei beni giuridici tutelati, dall'elemento soggettivo e dalla previsione della possibilità di commettere il reato di accesso abusivo solo nei riguardi di sistemi protetti, caratteristica che non ricorre nel reato di frode informatica.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	• identificazione degli accessi con username e password • adozione di filtri informatici • regolamento di Istituto • gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.2 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. pen. - art. 24 bis d.lgs. 201/01)

Commette il delitto chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Una delle condotte più ricorrenti che integrano questo reato è la detenzione di schede contraffatte per la decrittazione di trasmissioni televisive a pagamento. Altra condotta criminosa consiste nell'appropriarsi del numero seriale di un telefono cellulare appartenente ad altri, per realizzare un'illecita connessione alla rete di telefonia mobile attraverso la modifica del codice di un ulteriore apparecchio (la «clonazione»).

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	- identificazione degli accessi con username e password - adozione di filtri informatici - adozione del DPS con le misure minime previste - regolamento di Istituto - gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.3 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. pen. - art. 24 bis d.lgs. 201/01)

Commette il delitto chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	- identificazione degli accessi con username e password - adozione di filtri informatici - adozione del DPSS con le misure minime previste - regolamento di Istituto - gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.4 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. pen. - art. 24 bis d.lgs. 201/01)

Commette il delitto chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. La stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di siffatte comunicazioni.

Integra, ad esempio, questo reato anche la semplice utilizzazione da parte di chi esercita un'attività commerciale, mediante un terminale in suo possesso, di una carta di credito contraffatta, poiché costui è legittimato ad usare il terminale di lettura della carta e l'accesso abusivo genera un flusso di informazioni ai danni del titolare della carta contraffatta diretto all'addebito sul suo conto della spesa fittiziamente effettuata.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	• identificazione degli accessi con username e password • adozione di filtri informatici • adozione del DPS con le misure minime previste • regolamento di Istituto • gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.5 Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinques cod. pen. - art. 24 bis d.lgs. 201/01)

Commette il delitto chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività informatiche svolte da allievi, corsisti e personale amministrativo	• identificazione degli accessi con username e password • adozione di filtri informatici • adozione del DPS con le misure minime previste • regolamento di Istituto • gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.6 Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. pen. - art. 24 bis d.lgs. 201/01)

Commette il delitto, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

La pena edittale è più grave se il fatto è commesso con abuso della qualità di operatore del sistema.

Antecedentemente all'entrata in vigore della legge 23 dicembre 1993, n. 547, in tema di criminalità informatica, che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione di dati dalla memoria di un computer, in modo tale da renderne necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento, reato punito dall'art. 635 cod. pen., in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore. L'elemento psicologico del reato sta nella coscienza e volontà di danneggiare; a nulla rilevano il movente o le finalità per le quali il fatto sia commesso. Il reato sussiste anche quando l'azione sia posta in essere non al diretto scopo di nuocere, bensì quale mezzo per conseguire uno scopo diverso.

Per escludere la sussistenza del delitto di danneggiamento non basta che il danno causato sia di modesta entità, ma è necessario che esso sia talmente esiguo da non poter integrare una modificazione strutturale o funzionale della cosa, ovvero un deterioramento di una certa consistenza ed evidenza.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	• identificazione degli accessi con username e password • adozione di filtri informatici • adozione del DPS con le misure minime previste • regolamento di Istituto • gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.7 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter cod. pen. - art. 24 bis d.lgs. 201/01)

Il delitto, salvo che il fatto costituisca più grave reato, consiste nella commissione di un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. La pena è più elevata se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici; è aumentata se il fatto è commesso con violenza o minaccia alla persona oppure con abuso della qualità di operatore del sistema.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	- identificazione degli accessi con username e password - adozione di filtri informatici - adozione del DPS con le misure minime previste - regolamento di Istituto - gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.8 Danneggiamento di sistemi informatici o telematici (art. 635-quater cod. pen. - art. 24 bis d.lgs. 201/01)

Commette il delitto, salvo che il fatto costituisca più grave reato, chiunque distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. La norma richiede che il danneggiamento si attui o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi oppure con distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici. La pena è aumentata se il fatto è commesso con violenza o minaccia alla persona oppure con abuso della qualità di operatore del sistema.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	- identificazione degli accessi con username e password - adozione di filtri informatici - adozione del DPS con le misure minime previste - regolamento di Istituto - gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.1.9 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cod. pen. - art. 24 bis d.lgs. 201/01)

Il reato ricorre se il danneggiamento di sistemi informatici o telematici è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. La pena è più grave se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. La pena è aumentata se il fatto è commesso con violenza o minaccia alla persona oppure con abuso della qualità di operatore del sistema.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
--------------------	--------------------	--------------

MEDIO	attività informatiche svolte da allievi, corsisti e personale amministrativo	• identificazione degli accessi con username e password • adozione di filtri informatici • adozione del DPS con le misure minime previste • regolamento di Istituto • gestione informatica tramite presidio da parte dell'ufficio informatico interno
--------------	--	---

12.1.10 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies cod. pen. - art. 24 bis d.lgs. 201/01)

È reato proprio che commette il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Il sistema per la creazione e la verifica di firme elettroniche sfrutta le caratteristiche dei sistemi crittografici a due chiavi. Un sistema crittografico garantisce la riservatezza del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso di una chiave per interpretarli. Nei sistemi crittografici a due chiavi, detti anche a chiave pubblica o a chiave asimmetrica, ogni utente ha una coppia di chiavi: una chiave privata, da non svelare a nessuno, con cui può decodificare i messaggi che gli vengono inviati e firmare i messaggi che invia, e una chiave pubblica, che altri utenti utilizzano per codificare i messaggi da inviargli e per decodificare la sua firma e stabilirne quindi l'autenticità. Per ogni utente, le due chiavi vengono generate da un apposito algoritmo, con la garanzia che la chiave privata sia la sola in grado di poter decodificare correttamente i messaggi codificati con la chiave pubblica associata e viceversa. Grazie alla proprietà delle due chiavi, inversa rispetto a quella appena descritta, un sistema di questo tipo è adatto anche per ottenere dei documenti firmati. Infatti, la chiave pubblica di un utente è la sola in grado di poter decodificare correttamente i documenti codificati con la chiave privata di quell'utente.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività informatiche svolte da personale amministrativo	• conferimento al personale incaricato delle credenziali di accesso nei limiti in cui l'accesso sia funzionale allo svolgimento dell'incarico • - controllo accessi

12.1.11 - Documenti informatici (art. 491 bis cod. pen. - art. 24 bis d.lgs. 231/01)

L'art. 491 bis del codice penale punisce le falsità previste dal capo III del codice penale riguardanti un documento informatico pubblico o privato avente efficacia probatoria.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività informatiche svolte da allievi, corsisti e personale amministrativo	• identificazione degli accessi con username e password • adozione di filtri informatici • adozione del DPS con le misure minime previste • regolamento di Istituto • gestione informatica tramite presidio da parte dell'ufficio informatico interno

12.2 - Processi ed eventi sensibili

I processi sensibili sono tutti quelli che presuppongono o impongono l'utilizzazione di un sistema informatico.

SEZIONE 13 – DELITTI DI CRIMINALITÀ ORGANIZZATA

13.1 Elenco dei reati

13.1.1 Associazione per delinquere per commettere i reati di cui all'art. 416 n.6 cod. pen. (- art. 24 ter d.lgs. 201/01)

In base alla prima parte dell'art. 416 cod. pen. L'associazione per delinquere si ha quando tre o più persone si associano allo scopo di commettere più delitti. La pena si applica anche solo per la promozione o costituzione dell'associazione.

Sanzioni particolarmente pesanti, oltre che responsabilità amministrativa dell'ente ex decreto 231, si ha quando l'associazione per delinquere è finalizzata alla commissione dei seguenti reati:

- riduzione o mantenimento in schiavitù;
- prostituzione minorile;
- pornografia minorile;
- detenzione di materiale pornografico;
- pornografia virtuale;
- iniziative turistiche volte allo sfruttamento della prostituzione minorile;
- tratta di persone;
- acquisto e alienazione di schiavi;
- promozione, direzione, organizzazione, finanziamento o esecuzione del trasporto di stranieri nel territorio dello Stato;
- compimento di altri atti diretti a procurare illegalmente l'ingresso dello straniero nel territorio dello stato.

La responsabilità amministrativa dell'ente per gli ultimi due reati indicati sussiste solo se il reato è commesso in presenza di almeno due delle seguenti cinque circostanze aggravanti:

- il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;
- la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;
- la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;
- il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;
- gli autori del fatto hanno la disponibilità di armi o materie esplosive.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività educative	• regolamento di Istituto • assistenza e vigilanza diretta dei religiosi • firma del progetto educativo • selezione del personale • formazione del personale • coordinamento con il personale docente • colloqui personali di ingresso

13.1.2 Associazione di tipo mafioso (art. 416 bis cod. pen. - art. 24 ter d.lgs. 201/01)

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva

per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività gestionale	adozione di procedure nell'acquisto di lavori beni e servizi

13.1.3 Scambio elettorale politico – mafioso (art. 416 ter cod. pen. - art. 24 ter d.lgs. 201/01)

Il vigente codice penale, frutto della consistente legislazione antimafia prodotta a partire dagli anni novanta, prevede che la pena stabilita per l'associazione mafiosa si applichi anche a chi ottiene la promessa di voti in cambio dell'erogazione di denaro.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività educative e culturali	adozione Codice etico

13.1.4 Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309 - art. 24 ter d.lgs. 201/01)

In questo caso lo scopo dell'associazione è la commissione dei seguenti delitti: produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope.

La punibilità, quindi, riguarda anche la semplice detenzione illecita di una quantità di stupefacenti superiore ai limiti massimi stabiliti con decreto ministeriale.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività educative	- regolamento di Istituto - assistenza e vigilanza diretta dei religiosi - firma del progetto educativo - selezione del personale - formazione del personale - coordinamento con il personale docente - colloqui personali di ingresso

13.1.5 Associazione per delinquere commi da 1 a 5 (art. 416 cod. pen. - art. 24 ter d.lgs. 201/01)

L'associazione per delinquere si ha quando tre o più persone si associano allo scopo di commettere più delitti. La pena si applica anche solo per la promozione o costituzione dell'associazione.

Nelle analisi sopra elencate la responsabilità amministrativa dell'ente si riferiva all'associazione finalizzata alla commissione di specifici reati. In questo caso, si colpisce, seppure con sanzioni amministrative di minor entità, l'associazione per delinquere diretta alla generalità dei reati.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività educative	- regolamento di Istituto - assistenza e vigilanza diretta dei religiosi - firma del progetto educativo - selezione del personale - formazione del personale - coordinamento con il personale docente

- colloqui personali di ingresso

SEZIONE 14 – DELITTI CONTRO L'INDUSTRIA ED IL COMMERCIO

SEZIONE 15 DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

15.1 Elenco dei reati

15.1.1 Reati previsti dagli articoli 171, 171 bis, 171 ter, 171 septies e 171 octies della legge 22 aprile 1941, n. 633 (legge in materia di diritto d'autore) (art. 25 nonies d.lgs. 201/01).

Compie i reati previsti dalla legge sul diritto d'autore:

1) chi mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta o parte di essa;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	sito internet	• controlli periodici

2) chi compie una qualunque delle violazioni previste dall'art. 171 della legge sul diritto d'autore su un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore ed alla reputazione dell'autore;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	pubblicazioni attività didattiche	• controlli periodici • formazione e informazione degli operatori

3) chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società Italiana degli Autori ed Editori (SIAE);

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIODPS	• attività didattiche formative • attività amministrative	• controlli periodici da parte dell'ufficio informatico • formazione e informazione degli operatori • archivio delle licenze

4) chi, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge 633/41, ovvero esegue l'estrazione o il reimpiego della banca dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della stessa legge, ovvero distribuisce, vende o concede in locazione una banca dati;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	- attività didattiche formative - attività amministrative	adozione del DPS con le misure minime previste

5) chi abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento,

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

6) chi abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite a banche dati;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

7) chi, pur non avendo concorso alla duplicazione o alla riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta al pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

8) chi, detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione del contrassegno da parte della Società

Italiana degli Autori ed Editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

9) chi, in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
MEDIO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

10) chi introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

11) chi fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

12) chi abusivamente rimuove o altera le informazioni elettroniche di cui all'art. 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
--------------------	--------------------	--------------

BASSO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione
-------	----------------------------------	---

13) chi riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate da diritto d'autore e da diritti connessi;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
/		

14) chi, a fini di lucro, commercia al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
BASSO	attività legate agli audiovisivi	- regolamento di Istituto - formazione e informazione degli operatori - verifica periodica da parte della direzione

15) chi, esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da altri diritti connessi, si rende colpevole dei fatti previsti al comma 1;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
/		

16) i produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
/		

17) chi dichiara falsamente l'avvenuto assolvimento degli obblighi in materia di diritto d'autore;

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
/		

18) chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

Analisi del rischio

Livello di rischio	Processi sensibili	Contromisure
/		

SEZIONE 16 – ORGANIZZAZIONE COMUNE ALLE ATTIVITÀ DELL'ENTE

16.1 Tutela della salute e sicurezza nei luoghi di lavoro

In ottemperanza al D. Lgs. n. 81 del 9 aprile 2008 e successive modifiche, l'ente ha individuato la figura del RSPP (Responsabile del Servizio di Prevenzione e Protezione) in possesso dei requisiti previsti dalla normativa cogente.

Nella sua attività, RSPP è supportato da una società esterna di consulenza, che è un fornitore strategico dell'ente ed al quale viene inviata una copia controllata del Codice Etico allegato al presente Modello Organizzativo.

Ove gli stessi lavoratori, nelle singole case dell'ente, provvedano a nominare un RLS (Rappresentante dei Lavoratori per la Sicurezza), l'ente gli riconosce le prerogative, i diritti ed i poteri attribuiti dalla normativa cogente.

16.2 Protezione dei dati personali

In ottemperanza a quanto previsto dal D. Lgs. n. 196 del 30 giugno 2003 e successive modifiche, il Titolare del trattamento dei dati, per tutte le attività dell'ente, è il direttore della casa.

Gli addetti delle varie case che trattano, in qualunque forma, dati sensibili, giudiziari o personali, come individuati nel Documento Programmatico sulla Sicurezza dei dati (DPS), ricevono e sottoscrivono apposita lettera d'incarico.

16.3 Igiene ed autocontrollo alimentare

Il servizio di ristorazione può essere effettuato tramite esternalizzazione (contratti di appalto o di fornitura dei pasti) o direttamente dal personale dell'ente. In tal caso, è in vigore presso ogni centro cottura dell'ente un Manuale HACCP, predisposto secondo la normativa vigente. Le case che acquistano pasti preparati presso centri di cottura esterni dovranno eseguire, almeno una volta l'anno, un audit di seconda parte sul posto, al fine di verificare il rispetto delle norme in materia di igiene alimentare.

16.4 Attività esternalizzate

Per le attività dell'ente affidate a fornitori esterni mediante contratto di appalto di servizi, vengono rispettati i seguenti criteri:

- stipulazione di un contratto di appalto di servizi conforme alla normativa vigente;
- obbligo per l'appaltatore di trasmettere all'ente la documentazione comprovante l'assolvimento degli obblighi nei confronti del personale dipendente dell'appaltatore stesso, secondo il regime di solidarietà previsto dal D. Lgs. n. 276 del 10 settembre 2003 e successive modifiche;
- predisposizione del Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI), previsto dal D. Lgs. n. 81 del 9 aprile 2008.

16.5 Modello organizzativo e certificazione di qualità

L'ente **Istituto Salesiano San Marco** adotta un sistema di gestione per la qualità conforme allo standard internazionale Iso 9001:2008, certificato da organismi di parte terza, accreditati Sincert/Accredia. Come effetto dell'adozione dello standard ISO sono già in essere le seguenti contromisure, rilevanti anche ai fini dei controlli previsti dal presente Modello Organizzativo e dal Codice Etico:

1. redazione di un Manuale della Qualità;
2. redazione di procedure documentate;
3. individuazione delle attività affidate in outsourcing;
4. definizione di una Politica per la Qualità;
5. nomina di un Rappresentante della Direzione;
6. stesura del mansionario e dell'organigramma;
7. definizione periodica di obiettivi misurabili di qualità;
8. svolgimento, a scadenze periodiche prestabilite, di verbali di riesame della direzione;
9. pianificazione delle attività di formazione, addestramento ed aggiornamento del personale, religioso e laico, interno ed esterno;
10. individuazione dei requisiti obbligatori ed ulteriori richiesti ai fini dell'assunzione del personale;
11. definizione di criteri e metodi per la selezione del personale;
12. definizione di criteri e procedure per l'autovalutazione e la valutazione del personale;
13. definizione di procedure dirette a tenere sotto controllo la manutenzione ordinaria e straordinaria degli impianti e degli immobili;
14. pianificazione, progettazione ed erogazione in forma controllata dei servizi
15. definizione dei requisiti contrattuali dell'utenza
16. predisposizione di modalità controllate di gestione dei reclami dell'utenza e di raccolta delle segnalazioni del personale interno;
17. definizione di procedure per la gestione delle non conformità e delle conseguenti azioni correttive, preventive e di miglioramento;
18. somministrazione, raccolta ed analisi di questionari di customer satisfaction,
19. svolgimento periodico di verifiche ispettive interne, sia sull'applicazione dei requisiti obbligatori che sull'efficienza del sistema gestionale;
20. analisi sistematica dei dati relativi alle varie attività svolte;
21. elaborazione di piani della qualità e di miglioramento continuo.

SEZIONE 17 – INDIVIDUAZIONE DELLE ATTIVITÀ SENSIBILI

Istituto Salesiano San Marco

Sede: Via dei salesiani, 15 – 30174 VENEZIA MESTRE

Certificazione di qualità Iso 9001: ☒ sì ☐ no

Attività:

- Istituto tecnico industriale per le arti grafiche e la comunicazione;
- Erogazione di corsi di formazione superiore e continua;
- Attività di mensa scolastica e corsisti;
- Convitto scolastico per allievi dell'istituto tecnico e del CFP CNOS-FAP San Marco;
- Casa per ferie.

Servizi in outsourcing: /

Funzioni apicali formali: Legale rappresentante dell'ente, Direttore- Procuratore speciale.

Funzioni apicali di fatto: Ispettore, Direttore dell'opera.

Preposti: Economo dell'opera, preside-coordinatore didattico,
incaricato dell'oratorio, incaricato del convitto.

Istituto Salesiano San Marco

Sede: Calle don Bosco, 361 - 30015 CHIOGGIA - VE

Certificazione di qualità Iso 9001: ☐ sì ☒ no

Attività:

- Oratorio e centro giovanile;
- Cinema teatro;
- Bar interno.

Funzioni apicali formali: Legale rappresentante dell'ente, Direttore- Procuratore speciale.

Funzioni apicali di fatto: Ispettore, Direttore dell'opera.

Preposti: Economo dell'opera, incaricato dell'oratorio.