RESEARCH FOUNDATION

# MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. N. 231/2001

## PARTE SPECIALE N. 11

## GESTIONE SALA OPERATIVA

**INDICE**

# CONSIDERAZIONI PRELIMINARI SUL PROCESSO

Il presente documento sintetizza l'insieme dei protocolli diretti a programmare la gestione delle attività  e delle decisioni della Fondazione Cima nel processo "*Gestione sala operativa*".

Il protocollo attiene pertanto all'attività prestata all'interno della sala operativa e dei relativi servizi, attiva 24/24 - 7/7.

# REATI ASSOCIABILI

Nel paragrafo in questione si individuano le differenti figure di reato che, a seguito dell'attività di *risk assessment* svolta, si ritengono configurabili.

In particolare il processo in oggetto si ritiene a rischio di commissione delle seguenti fattispecie previste dagli **artt. 24-*bis*** del Decreto:

**Art. 24-bis: Reati informatici**

Art. 615-ter c.p. Accesso abusivo ad un sistema informatico o telematico;

Art. 615-quater c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

Art. 615-quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;

Art. 617-quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;

Art. 617-quinquies c.p.Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;

Art. 629 co. 3 c.p. Estorsione;

Art. 635-bis c.p. Danneggiamento di informazioni, dati e programmi informatici;

Art. 635-ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;

Art. 635-quater c.p. Danneggiamento dei sistemi informatici o telematici;

Art. 635 quater1 Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Art. 635-quinquies c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità;

Art. 640-quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica;

Art. 491-*bis* c.p. Falsità in documento informatico o avente efficacia probatoria;

Art. 482 c.p. Falsità materiale commessa dal privato;

Art.484 c.p. Falsità in registri e notificazioni;

Art. 485 c.p. Falsità in scrittura privata;

Art. 486 c.p. Falsità in foglio firmato in bianco. Atto privato;

Art. 487 c.p. Falsità in foglio firmato in bianco. Atto pubblico;

Art. 488 c.p. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali;

Art.489 c.p. Uso di atto falso;

Art. 490 c.p. Soppressione, distruzione e occultamento di atti veri;

Art. 491 c.p. Documenti equiparati agli atti pubblici agli effetti della pena;

Art. 492 c.p. Copie autentiche che tengono luogo degli originali mancanti;

Art. 493 c.p. Falsità commesse da pubblici impiegati incaricati di un servizio pubblico.

**Art. 25-*novies*: Reati in violazione del diritto d'autore**

Art. 171 L. 633/1941 co. 1 lett. a) bis Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa;

Art. 171 L. 633/1941 co. 3 Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione;

Art. 171-bis, co. 1 Duplicazione,importazione, distribuzione, vendita o detenzione di programmi contenuti in supporti non contrassegnati dalla SIAE;

Art. 171 ter L. 633/1941 a fini di lucro abusivamente duplica, mette in vendita opere altrui

Sono stati, altresì, individuati i seguenti reati che indirettamente potrebbero interessare il processo. In particolare, si ritiene a rischio di commissione delle seguenti fattispecie previste dagli artt. 24-bis del Decreto:

**Art. 24-bis: Delitti informatici e trattamento illecito di dati**

Art. 482 c.p. Falsità materiale commessa dal privato;

Art. 489 c.p. Uso di atto falso.

## POSSIBILI OCCASIONI DI ILLECITO

L'area di rischio, insita in ciascun processo, nel caso di specie può essere rintracciata nelle seguenti fasi:

- accesso al sistema telematico di pertinenza di soggetti terzi;
- manomissione del sistema telematico di pertinenza di soggetti terzi.

# SISTEMA DI CONTROLLO

L'attività nel processo dovrà svolgersi nel rispetto delle leggi e regolamenti vigenti, delle norme del Codice di Comportamento, dei valori e delle politiche della Fondazione Cima, delle regole contenute nel Modello e nei protocolli attuativi dello stesso.

Il sistema dei controlli, adottato dall'Organizzazione con riferimento al processo in questione prevede per le attività suindicate:

- principi di controllo "generali", presenti in tutte le attività sensibili;

- principi di controllo "specifici", applicati alle singole attività sensibili.

## PRINCIPI DI CONTROLLO GENERALI

I principi di controllo sono stati adottati sulla base delle indicazioni contenute nelle Linee Guida di Confindustria per la costruzione dei Modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001.

Essi sono stati applicati nell'ambito della realtà organizzativa ed operativa della Organizzazione.

Tali principi sono di seguito indicati:

**Esistenza di procedure/linee guida formalizzate**: esistenza di specifici documenti volti a disciplinare principi di comportamento e modalità operative per lo svolgimento dell'attività, caratterizzati da una chiara ed esaustiva definizione di ruoli e responsabilità e da un'appropriatezza delle modalità previste per l'archiviazione della documentazione rilevante.

**Tracciabilità e verificabilità ex-post delle transazioni tramite adeguati supporti documentali/informatici**: verificabilità, documentabilità, coerenza e congruenza di operazioni, transazioni e azioni, al fine di garantire un adeguato supporto documentale che consenta di poter effettuare specifici controlli.

**Separazione dei compiti**: l'esistenza di una preventiva ed equilibrata distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi anche all'interno di una stessa Unità Organizzativa, idonei ad evitare commistione di ruoli potenzialmente incompatibili o eccessive concentrazioni di responsabilità e poteri in capo a singoli soggetti.

**Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate**: l'attribuzione di poteri esecutivi, autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate nell'ambito dell'attività descritta, oltre che chiaramente definiti e conosciuti all'interno della Organizzazione.

# PRINCIPI DI CONTROLLO SPECIFICI

Ogni attività svolta con l'ausilio del mezzo informatico deve avvenire nel rispetto della normativa vigente, della normativa in materia di diritto d'autore, *copyright* e trattamento dei dati personali, nonché nel rispetto di tutta la normativa nazionale ed internazionale concernente l'utilizzo dei mezzi informatici.

## GUIDA PRATICA PER L'OPERATORE DI SALA SITUAZIONI

Per la gestione delle attività della sala operativa, attiva 7/7 - h 24/24, Fondazione Cima ha redatto e diffuso il documento "Guida pratica per l'operatore di sala situazioni", da intendersi integralmente richiamata in tale sede.

La citata documentazione deve essere conosciuta e rispettata da tutte le risorse impegnate in tale ambito.

## GESTIONE DEI SISTEMI INFORMATICI

Tutte le risorse impiegate nelle attività afferenti la gestione della sala operativa dovranno, inoltre, osservare quanto disposto all'intento del protocollo n. 7 "Gestione dei sistemi informativi".

# RAPPORTI CON L'ORGANISMO DI VIGILANZA

Tutti i soggetti coinvolti nel processo dovranno dare tempestiva comunicazione al Responsabile Aziendale dell'Organismo di Vigilanza, di eventuali significativi scostamenti dai flussi procedurali o di eventuali criticità significative e rilevanti ai fini dei modello organizzativo previsto dal D.Lgs. 231.

Il Responsabile Aziendale del flusso valuterà il successivo inoltro all'Organismo di Vigilanza tempestivamente o nell'ambito delle comunicazioni periodiche.

Il canale informativo è l'indirizzo di posta elettronica 231@cimafoundation.org.

Il Referente dell'OdV invierà secondo le tempistiche indicate nel documento "Flusso verso OdV" le seguenti informazioni:

- criticità emerse;
- contenziosi.

Fermo restando il potere discrezionale di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza attua le procedure di controllo previste dal Modello di Organizzazione e Gestione ed effettua periodicamente controlli a campione sulle attività potenzialmente a rischio di reato, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole del Modello e, in particolare, alle procedure interne in essere. Il medesimo Organismo provvederà ad esaminare e verificare tutte le segnalazioni ricevute, analizzare i report provenienti dai responsabili di funzione, nonché predisporre un piano di verifiche periodico da integrare in relazione a specifiche esigenze.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale.