RESEARCH FOUNDATION

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

PARTE SPECIALE N. 7

GESTIONE DEI SISTEMI INFORMATICI

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 dei sistemi informatici*".

Il protocollo attiene pertanto all'attività inerente la materia di sicurezza del sistema informatico e telematico (cfr. n. 7 della mappatura dei processi).

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* e 25-*novies*** 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

POSSIBILI OCCASIONI DI ILLECITO

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

- definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico;
- gestione degli accessi al sistema informatico degli utenti, dei profili utente e del processo di autenticazione;
- gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni;
- gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni ecc.) e delle attività di inventariazione dei beni;
- acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione);
- monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica;
- gestione degli aspetti infrastrutturali delle transazioni *on-line*.

Le condotte umane tali da concretizzare le fattispecie di reato sopra richiamate sono certamente molteplici e variegate e dunque, a mero titolo esemplificativo e certamente non esaustivo, si riportano taluni casi:

- alterazione del funzionamento di un sistema informatico al fine di procurarsi un ingiusto profitto con l'altrui danno;
- violazione degli obblighi previsti dalla legge per il rilascio del certificato di firma elettronica;
- duplicazione, al fine di trarne profitto, di opere tutelate dal marchio SIAE;
- alterazione documenti informatici;
- accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza.

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, documentabilit, 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.

REGISTRO DEI SERVIZI INFORMATICI E REGISTRO DEGLI UTENTI

Fondazione CIMA manterrà un **Registro dei sistemi e dei servizi informatici (Registro n. 1),** che conterrà:

a) L'elenco di tutto il materiale *hardware* "sensibile" acquistato da Fondazione CIMA e non trasferito nella disponibilità di terzi per la sua gestione e controllo (da intendersi oggetti sensibili ai fini dei controlli 231 tutti i dispositivi *hardware* si cui possono essere installati programmi di calcolo o applicazioni software, e che sono in grado di collegarsi alla rete internet.).

Item	Fornitore	N. Fattura	Data	Oggetto	N. Seriale	Responsabile
#1						
#2						

b)

Tabella 1 ***Registro dei sistemi e dei servizi informatici (Registro n. 1) - Colonne minime***

b) Per ogni prodotto *software* acquistato, l'elenco degli utenti a cui viene intestata una licenza personale.

c) L'elenco dei servizi informatici erogati a favore di tutti i dipendenti e collaboratori per lo svolgimento delle attività di lavoro, sia attraverso la propria infrastruttura, sia attraverso piattaforme digitali di terze parti (programmi, server, banche dati, sistemi *software* integrati, posta elettronica, piattaforme di collaborazione, servizi *cloud*, etc.).

GESTIONE DEGLI ACCESSI AI SERVIZI INFORMATICI E REGISTRO DELLE DOTAZIONI INFORMATICHE AD USO PERSONALE

A seguito dell'entrata in vigore, in data 5.04.2008, della Legge 18 marzo 2008 n. 48, attuativa della Convenzione del Consiglio d'Europa in tema di criminalità informatica, ai fini della prevenzione dei reati così introdotti ai sensi del D.Lgs. n. 231/2001, Fondazione CIMA assocerà

ad ogni dipendente o collaboratore un “nome utente” (tipicamente composta da “*nome.cognome*”) necessario per accedere a tutti i servizi informatici erogati dalla Fondazione.

A tal proposito Fondazione CIMA manterrà anche un **Registro degli utenti (Registro n. 2),** che riporterà il nome degli utenti autorizzati all’uso di ogni programma registrato, ovvero che avranno il suddetto software installato nei dispositivi loro assegnati.

Ad ogni dipendente o collaboratore della Fondazione, con la limitazione dell’uso personale e l’obiettivo di svolgere al meglio i compiti loro assegnati, possono essere forniti *personal computer* fissi o portatili, *monitor*, *tablet* e apparati *smartphone*.

Nel caso di *pc* e *laptop* ad ogni utente sarà consegnata una prima *password* personalizzata abbinata al suo “*nome utente*” a cui saranno associati i privilegi di Amministrazione, con prescrizione di modificare la password al primo accesso utile.

Il dipendente riceverà ogni anno delle “Indicazioni” o “Linee-guida”, concordate con il DPO ed il Titolare del Trattamento dei dati personali, per l’utilizzo degli strumenti di lavoro ricevuti ed il trattamento dei relativi dati personali. Il rispetto delle suddette indicazioni e del buon utilizzo della strumentazione di lavoro fornita potrà essere oggetto di controlli casuali tra il personale.

Per gestire le dotazioni informatiche, Fondazione Cima dovrà catalogare tutti gli strumenti forniti ad uso personale, evidenziando il *software* caricato al momento della consegna e l’eventuale data di scadenza delle singole licenze.

L’obbligo del 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 è trasferito al dipendente/collaboratore che riceve la dotazione.

Fondazione CIMA dovrà compilare e far accettare formalmente a tutti gli assegnatari delle dotazioni informatiche una “scheda di presa in carico” dove viene descritta la strumentazione e le licenze software fornite.

La traccia di tutte le schede sarà mantenuta nel registro degli utenti associate al nominativo di ciascun assegnatario.

Le condizioni d’uso di ogni dotazione fornita sono riportate nel regolamento aziendale inviato periodicamente ad ogni utente.

A riconsegna avvenuta Fondazione CIMA rilascerà una scheda di restituzione in cui, con riferimento alla scheda di presa in carico sarà elencato il materiale restituito con numero di matricola ed evidenza dello stato in cui si trova.

PREDISPOSIZIONE O UTILIZZO DI DOCUMENTI INFORMATICI PUBBLICI AVENTI EFFICACIA PROBATORIA

Nel caso di predisposizione o uso di documenti informatici integranti atto pubblico, copia autentica e/o attestato, occorre:

- verificare la provenienza e la veridicità del documento e del suo contenuto;
- conservare il documento cartaceo e la relativa documentazione cartacea probante la veridicità del suo contenuto e la sua provenienza nel fascicolo di competenza (da costituirsi necessariamente all'atto della predisposizione o dell'utilizzo di un documento informatico di cui sopra qualora esso non faccia parte di un fascicolo già esistente – ad esempio archivio fatture);
- interrompere la trasmissione allorquando la provenienza e/o la veridicità del documento o del suo contenuto siano dubbi, nonché informarne senza indugio le competenti autorità aziendali e l'OdV, a mezzo di apposito *report*.E' fatto divieto di proseguire nell'operazione in assenza di verifiche che consentano di procedere.

DATA BREACH

Il c.d. *data breach* è una violazione dei sistemi informatici che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati da Fondazione Cima. La violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi di *data breach* sono:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, *virus*, *malware*, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Il Titolare del trattamento, senza ingiustificato ritardo e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se, invece, la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Nel caso in cui una delle risorse di Fondazione Cima e/o anche un collaboratore, consulente, *partner*, fornitore venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati.

La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:

1. rilevazione della violazione dei dati personali da parte del personale, dei collaboratori, dei fornitori e segnalazione immediata all'Amministrazione di sistema o suo delegato, che effettua un immediato *screening* della situazione;
2. segnalazione della violazione dei dati personali da parte dell'Amministrazione di sistema o suo delegato al Titolare del trattamento e al DPO;
3. raccolta delle informazioni sulla violazione e comunicazione nell'immediato della violazione da parte dell'Amministratone di sistema o suo delegato al Titolare del trattamento e al DPO;
4. valutazione del rischio da parte dell'Amministratone di sistema o suo delegato, in confronto col DPO, da indirizzare al Titolare del trattamento;
5. individuazione delle azioni correttive da parte dell'Amministratone di sistema o suo delegato, in confronto col Titolare del trattamento e il DPO;
6. comunicazione delle valutazioni effettuate e delle azioni da intraprendere al personale di Fondazione CIMA, se reputato necessario dall'Amministratone di sistema, dal Titolare del trattamento e dal DPO.

Attività	Chi	A chi	Quando	Come
Rilevazione e segnalazione eventuale data breach	- tutto il personale - collaboratori - fornitori - Amministratore di sistema o suo delegato	- Amministratore di sistema o suo delegato	Appena se ne viene a conoscenza	Via mail o telefono
Segnalazione eventuale data breach	- Amministratore di sistema o suo delegato	- al Titolare del trattamento - al DPO	Appena ne viene a conoscenza, comunque dopo aver prestato la prima necessaria assistenza	Via mail

Raccolta delle informazioni sulla violazione e comunicazione del data breach	- Amministratore di sistema o suo delegato	- al Titolare del trattamento - al DPO	Entro 24 ore dalla rilevazione	Via mail
Valutazione del rischio	- Amministratore di sistema o suo delegato - DPO	- Titolare del trattamento	Entro 24 ore dalla rilevazione	Via mail
Individuazione delle azioni correttive	- Amministratore di sistema o suo delegato - Titolare del trattamento - DPO		Appena terminata la valutazione	Via telefono/mail, comunque da inserire nella Relazione del DPO
Comunicazione dell'accaduto e delle azioni da intraprendere	- Amministratore di sistema o suo delegato - Titolare del trattamento - DPO	Al personale	Entro 72 ore dalla rilevazione	Via telefono/mail, comunque da inserire nella Relazione del DPO
Notifica della violazione (se necessaria)	Titolare del Trattamento	Al Garante	Entro 72 ore dalla rilevazione	Modulistica predisposta dal Garante
Documentazione delle violazioni	- DPO	- Titolare del trattamento	Una volta all'anno	Relazione annuale del DPO

RAPPORTI CON L'ORGANISMO DI VIGILANZA

Tutti i soggetti coinvolti nel processo, per il tramite del proprio superiore gerarchico, dovranno dare tempestiva comunicazione, al corrispondente Responsabile Aziendale del flusso verso l'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.

L'OdV ha facoltà di:

- prendere visione di tutti i documenti concernenti la Gestione dei Sistemi Informatici;
- prendere visione dei Registri;
- accedere ai documenti telematici inviati, al fine di verificare la loro coincidenza con gli eventuali atti originali cartacei ovvero con i dati sulla base dei quali è stato predisposto il documento telematico;
- verificare l'assenza di software contraffatto sui dispositivi assegnati come dotazione aziendale;
- verificare le licenze dei programmi installati sui PC.

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

- numero di amministratori di sistema abilitati/disabilitati;
- numero di incidenti di intrusione ed eventuali criticità rilevate;
- numero di spam/virus rilevati nell'infrastruttura della Fondazione
- nuove licenze *software* acquistate/scadute/rinnovate;
- operazioni effettuate in deroga alle procedure e/o promanate direttamente da apicali;
- elenco delle autorizzazioni all'accesso ai servizi informatici attive, rilasciate o modificate;
- contenziosi e/o criticità emerse.

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.