SOGESID S.P.A

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE – "B"

DELITTI INFORMATICI

DOCUMENTO APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE IN DATA 18/02/2021

INDICE

- PARTE SPECIALE "B"-

1. REATI APPLICABILI ALLA SOCIETÀ

Per quanto concerne la presente Parte Speciale "B", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 24-bis del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili dalla Società, in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Direzione/Funzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

Documenti informatici (art. 491-bis c.p.)

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo, bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, comma 1, lett. p), D.Lgs. 82/2005).

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)

Tale reato si realizza quando un soggetto 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 diritto ad escluderlo.

L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema stesso.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Tale reato si realizza quando un soggetto, 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 di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, policy Internet).

L'art. 615-quater, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.)

Tale reato si realizza qualora qualcuno, 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.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

Tale ipotesi di reato si realizza qualora un soggetto fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Tale ipotesi di reato si realizza quando qualcuno, 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.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

Tale fattispecie di reato si realizza quando un soggetto "distrugge, deteriora, cancella,

altera o sopprime informazioni, dati o programmi informatici altrui". Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

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

Tale reato si realizza quando un soggetto commette 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. Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.
Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)

Questo reato di realizza quando un soggetto mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.
Si tenga conto che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis.
Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus informatico).

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

Questo reato si configura quando il fatto di cui all'art. 635-quater (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.
Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di

pubblica utilità (art. 635-ter), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblica utilità indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Il reato si può configurare nel caso in cui un Dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero nel caso in cui l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

2. ATTIVITÀ SENSIBILI

Le attività che la Società ha individuato come sensibili, nell'ambito dei reati informatici, sono indicate in dettaglio nella "Matrice delle Attività a Rischio-Reato", conservata a cura della Società.
Le aree di attività ritenute più specificamente a rischio ai fini della presente Parte speciale "B", sono di seguito riepilogate sulla base della numerazione indicata all'interno della "Matrice delle aree a rischio-reato ex D.Lgs. 231/2001".

Si evidenzia che le possibili modalità e finalità di realizzazione delle principali fattispecie di reato connesse alle Aree e alle Attività sensibili sono indicate, a titolo esemplificativo e non esaustivo, nella "Matrice delle aree a rischio-reato ex D.Lgs. 231/2001" allegata al Modello 231.

A. GESTIONE DEI RAPPORTI CON SOGGETTI APPARTENENTI ALLA PUBBLICA AMMINISTRAZIONE

A.3) Gestione dei rapporti con i funzionari pubblici nell'ambito dello svolgimento delle attività aziendali di natura operativa, anche in occasione di verifiche, ispezioni e accertamenti quali, a titolo esemplificativo e non esaustivo:
- Guardia di Finanza ed Enti competenti in materia fiscale e tributaria;

- Corte dei Conti, Agenzia delle Entrate e Riscossione e, in linea di principio, Amministrazione finanziaria per l'invio di dichiarazioni ed altri adempimenti obbligatori;

- INPS, INAIL, Ispettorato del Lavoro per gli adempimenti in materia di gestione del personale.

Principali fattispecie di reato connesse

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis c.p.)

Principali Ruoli/Aree coinvolti

- ✓ PAD
- ✓ Direzione Amministrazione, Personale e Legale

N. GESTIONE DEGLI ADEMPIMENTI SOCIETARI

Principali fattispecie di reato connesse

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis c.p.)

Principali Ruoli/Aree coinvolti

- ✓ Affari Societari e Giuridici
- ✓ Segretario CDA

O. GESTIONE INFRASTRUTTURE INFORMATICHE

O.1) Gestione delle infrastrutture informatiche a supporto delle attività aziendali. Nello specifico:

- Gestione e manutenzione sistemi informatici e reti;

- Cura rapporti tecnici con società affidatarie di servizi IT in outsourcing;

- Aggiornamento e pubblicazione web dei dati e informazioni aziendali;

- Supporto utenti e assistenza tecnica e sicurezza informatica.

Principali fattispecie di reato connesse

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici anche di pubblica utilità (art. 635-quater e quinquies c.p.)

Principali Ruoli/Aree coinvolti

- ✓ DAPL Information Technologies

3. PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001 e del Codice Etico e di Condotta adottato dalla Società, nello svolgimento delle attività sensibili sopra citate, tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi generali di comportamento.

In particolare, è fatto divieto ai soggetti destinatari della presente parte speciale di:

- Porre in essere comportamenti tali da integrare le fattispecie di reato, previste dall'art. 24-bis del D.Lgs. n. 231/2001, riguardanti i delitti informatici presentati nel capitolo 1 "Reati applicabili alla società" ed identificati nella Matrice delle attività rischio-reato;
- Connettere ai sistemi informatici della Società personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del soggetto responsabile individuato;
- Modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- Acquisire, possedere o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi della Società – che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici;
- Divulgare, cedere o condividere con il personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale o di terze parti;
- Accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri dipendenti/collaboratori o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- Sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- Comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

- Mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti *virus* o altri programmi in grado di danneggiare o intercettare dati;
- Inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi;
- Divulgare informazioni riservate a soggetti interni o esterni alla Società;
- Diffondere e/o utilizzare dati sensibili relativi a dipendenti e fornitori senza idonea autorizzazione.

In via generale, ai destinatari della presente parte speciale è richiesto di:

- Proteggere la rete di trasmissione dei dati aziendali mediante adeguati strumenti di limitazione degli accessi (firewall e proxy).
- Prevedere un piano di Business Continuity ed un piano di Disaster Recovery a fronte di eventi disastrosi, al fine di garantire la continuità dei sistemi informativi e dei processi ritenuti critici; le soluzioni individuate devono esser periodicamente aggiornate e testate.
- Monitorare la limitazione degli accessi alle aree ed ai siti Internet potenzialmente sensibili al fine di evitare la distribuzione e diffusione di programmi infetti (c.d. "virus").
- Protezione del server e dei dispositivi aziendali con adeguati programmi antivirus, aggiornati in modo automatico, contro il rischio di intrusione.
- Nell'ambito della gestione dei sistemi informatici coordinarsi con il responsabile della protezione dei dati nominato dalla Società.
- Implementare, su indicazione del responsabile della protezione dei dati, le misure minime di sicurezza identificate dalla normativa, oltre a misure idonee e preventive da identificare in base ad un'accurata analisi dei rischi.

4. PRINCIPI DI CONTROLLO SPECIFICI

Al fine di evitare la commissione dei reati di cui alla presente Parte Speciale, la Società ha previsto, con riferimento alle aree a rischio

- Gestione dei rapporti con soggetti appartenenti alla Pubblica Amministrazione
- Gestione infrastrutture informatiche

i principi di controllo specifici di seguito elencati.

<u>Gestione dei rapporti con soggetti appartenenti alla Pubblica Amministrazione</u>

- Gestione dei rapporti con i Rappresentanti della Pubblica Amministrazione e con altri Enti pubblici esclusivamente da parte di soggetti aziendali muniti degli occorrenti poteri in conformità al sistema di deleghe e procure, ovvero di coloro che siano da questi formalmente delegati.
- Inserimento della clausola di rispetto dei principi contenuti nel Modello di Organizzazione, Gestione e Controllo *ex* D.Lgs. 231/01 e del Codice Etico e di Condotta adottati dalla Società nel contratto/lettera di incarico, qualora i rapporti della Società con la Pubblica Amministrazione siano gestiti anche attraverso professionisti esterni.
- Effettuazione degli adempimenti nei confronti della Pubblica Amministrazione e predisposizione della relativa documentazione nel rispetto delle normative vigenti (comunitarie, nazionali, regionali, provinciali e comunali) e con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse.
- Applicazione dei principi di trasparenza, onestà e correttezza da parte del personale delegato a intrattenere rapporti con rappresentanti della Pubblica Amministrazione, al fine di non compromettere l'integrità e la reputazione della Società.
- Formalizzazione dell'obbligo di intrattenere, nell'ambito delle proprie mansioni, rapporti di leale collaborazione con le Autorità e di cooperare con esse, salvaguardando la loro e la propria autonomia. In particolare, è fatto obbligo di produrre e fornire tutti i documenti richiesti dalle Autorità e fornire risposte complete, attinenti ed esaustive ai quesiti posti dalle medesime Autorità. È comunque formalizzato il divieto di dare e/o richiedere a terzi notizie o informazioni che riguardino fatti oggetto di procedimenti disciplinari in corso.
- Individuazione del collega o del superiore dotato di idonee procure, da parte del personale coinvolto nella gestione dei rapporti con i rappresentanti della Pubblica

Amministrazione, qualora sia chiamato a sottoscrivere la documentazione correlata (ad es. verbali o comunicazioni ufficiali).

- Verifica e sottoscrizione di tutta la documentazione da parte del personale dotato di idonei poteri, conformemente a quanto previsto dal sistema vigente di procure e deleghe.
- Corretta archiviazione della documentazione rilasciata dai rappresentanti della Pubblica Amministrazione incaricati di svolgere gli accertamenti e le verifiche ispettive (es. verbali di accertamento, reportistica prodotta, risultanze, ecc.) e di qualsiasi altro elemento idoneo a definire chiaramente, anche a posteriori, la tipologia del rapporto intercorso.
- Formalizzazione delle attività svolte, compresi pagamenti effettuati a favore della PA ed eventuali verifiche/controlli da parte della stessa, mediante apposito verbale/report, invio del medesimo al Responsabile di livello superiore e successiva archiviazione.

<u>Gestione infrastrutture informatiche</u>

- Pianificazione di attività di routine e straordinarie da parte della funzione aziendale preposta mediante la predisposizione del "Piano di attività sistemi informatici".
- Previsione di credenziali di autenticazione e di accessi sugli applicativi aziendali adeguatamente tracciati su log, nel rispetto della normativa vigente.
- Previsione di applicazioni che tengono traccia delle modifiche, compiute dagli utenti, ai dati ed ai sistemi aziendali.
- Definizione di criteri e modalità per l'assegnazione, la modifica e la cancellazione dei profili utente.
- Definizione di meccanismi di monitoraggio del traffico e di tracciabilità degli eventi di sicurezza sulle reti (ad esempio: accessi anomali per frequenza, modalità, temporalità).
- Definizione di una policy formale che regoli le modalità operative per la messa a disposizione e la corretta gestione delle risorse informatiche.
- Formalizzazione, a cura della funzione aziendale preposta, di appositi report al fine di condividere con il Vertice societario la presenza di eventuali anomalie riscontrate e di attività straordinarie svolte.
- Esecuzione quotidiana e automatica di backup dei dati sui server aziendali.

- Verifica del corretto funzionamento dei server aziendali al fine di individuare operazioni anomale o malfunzionamenti e di prevenire accessi non autorizzati sugli apparati informatici aziendali.
- Verifica periodica avente ad oggetto lo stato di aggiornamento delle componenti software di base.
- Verifica periodica avente ad oggetto l'applicazione delle misure minime di sicurezza (ad es. accessi fisici alla sala CED, correttezza delle procedure di archiviazione dei dati trattati, ecc.).
- Aggiornamento e pubblicazione dei dati/informazioni aziendali e manutenzione del sito web aziendale da parte della funzione aziendale preposta previa autorizzazione del Vertice aziendale.
- Gestione del servizio di posta elettronica aziendale, compresa la PEC, secondo le modalità definite nelle apposite procedure interne.
- Divieto d'uso della casella di posta aziendale per finalità estranee alle esigenze di servizio.
- Esecuzione dei backup di file di progetto mediante supporto idoneo, identificabile e rintracciabile, archiviato a cura della funzione aziendale preposta.
- Verifica del materiale informatico acquistato e tempestiva segnalazione di eventuali incongruenze riscontrate.
- Installazione e configurazione di nuovi apparati a cura del personale tecnico specializzato.
- Assegnazione e utilizzo degli strumenti informatici sulla base delle procedure/regolamenti interni.
- Archiviazione della documentazione e delle registrazioni all'interno del Sistema documentale aziendale depositato sui Server.
- Gestione dell'elenco dei dispositivi HW e i SW aziendali da parte delle funzioni aziendali preposte e formalizzazione dello stesso mediante apposita modulistica.
- Esecuzione delle attività di verifica, validazione ed eventuale manutenzione/aggiornamento di SW e formalizzazione delle stesse mediante apposita modulistica.
- Protezione della rete di trasmissione dati aziendale da adeguati strumenti di limitazione degli accessi (firewall e proxy).

- Protezione dei sistemi informativi aziendali mediante programmi antivirus, aggiornati in modo automatico, al fine di evitare il rischio di intrusione.
- Definizione di procedure al fine di rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.
- Predisposizione di un piano di emergenza in caso di malfunzionamento o di fermo del sistema.
- Garanzia della corretta esecuzione delle operazioni di avvio e chiusura del sistema.
- Valutazioni periodiche al fine di verificare l'adattabilità e l'integrità delle misure di sicurezza.
- Definizione di regole per la navigazione in Internet che includono, in particolare:
    - l'utilizzo della rete al solo fine lavorativo;
    - il divieto di scaricare software nelle strutture informative aziendali;
    - il divieto di connessione a siti segnalati.

Principali procedure operative (PO), istruzioni operative (IST), regolamenti (Reg.) di riferimento:

- PO 01 – Redazione, modifica e tenuta sotto controllo della documentazione e delle registrazioni
- PO 04 – Gestione delle infrastrutture
- PO 13 – Amministrazione trasparente
- PO 14 - Omaggi, regalie ed altre forme di utilità
- IST 01 – Archiviazione documentale e protocollo
- IST 7a – Sistemi informativi ed informatici
- IST 7B – Regolamento utilizzo strumenti informatici
- Procedure amministrative contabili del Dirigente Preposto compliance con il D.Lgs. 262 del 2005 – Sistemi informativi