Società di Gestione Servizi Industriali S.r.l.



MODELLO DI ORGANIZZAZIONE,

GESTIONE E CONTROLLO

EX D. LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE B

Reati informatici
 (art. 24 bis)

Approvato dal Consiglio di Amministrazione il 13 settembre 2018

**Società di Gestione Servizi Industriali S.r.l. (SO.GE.S.I.)**

**Sede Legale in Ancona (AN), Via Roberto Bianchi, 60131**

**Codice Fiscale n. 00421720426**

**INDICE**

[LE FATTISPECIE DI REATO 3](#_Toc523387017)

[ Falsità riguardanti un documento informatico (art. 491 bis c.p.) 3](#_Toc523387018)

[ Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.) 3](#_Toc523387019)

[ Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.) 3](#_Toc523387020)

[ Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) 3](#_Toc523387021)

[ Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.) 3](#_Toc523387022)

[IDENTIFICAZIONE DELLE ATTIVITA’ A RISCHIO REATO 4](#_Toc523387023)

[PRINCIPI GENERALI DI COMPORTAMENTO 4](#_Toc523387024)

[PROCEDURE DI CONTROLLO 5](#_Toc523387025)

# **LE FATTISPECIE DI REATO**

La presente Parte Speciale si riferisce ai reati informatici, richiamati dall’art. 24 bis del D.Lgs.231/2001, ed in particolare riporta le singole fattispecie di reato considerate rilevanti per la responsabilità amministrativa di Sogesi S.r.l.. Individua inoltre le cosiddette attività “sensibili” (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell’ambito dell’attività di risk assessment) specificando i principi comportamentali ed i presidi di controllo operativi per l’organizzazione, lo svolgimento e la gestione delle operazioni svolte nell’ambito delle sopracitate attività “sensibili”.

In considerazione dell’analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di Sogesi seguenti reati:

* Falsità riguardanti un documento informatico (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 il comportamento riguardi non un documento cartaceo, bensì un documento informatico.

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

* 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.

* 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.

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.

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

Tale fattispecie reato si realizza quando un soggetto distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

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

Questo reato di realizza quando un soggetto attraverso il danneggiamento di dati, informazioni e programmi informatici, oppure attraverso l'introduzione o la trasmissione di dati, informazioni e programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

# **IDENTIFICAZIONE DELLE ATTIVITA’ A RISCHIO REATO**

Le attività che la Società ha individuato come sensibili, nell’ambito dei delitti informatici, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Tali attività sono di seguito riepilogate:

* Falsificazione di documenti informatici relativi ad esempio a rendicontazione in formato elettronico di attività e/o a attestazioni elettroniche di qualifiche o requisiti della Società.
* Utilizzo improprio del dispositivo di firma digitale, da parte sia di soggetti terzi non preventivamente delegati sia di soggetti abilitati all’uso del dispositivo di firma, per inviare documentazione e modulistica relativa a servizi di finanza agevolata al Comune, Provincia, Regione ecc.
* Accesso ai sistemi informatici aziendali o di terze parti, che contengono:

- dati di vendita e fatturazione;

- dati sensibili e personali;

- informazioni bancarie;

- dati relativi a pagamenti.

* Acquisizione, detenzione e gestione abusiva di credenziali di accesso (user e password) a piattaforme on-line aziendali o di terze parti.
* Gestione di strumenti e dispositivi e programmi, da parte di soggetti aziendali e amministratori di sistema, mediante i quali possono:

- essere intercettate informazioni rilevanti di terze parti o impedite comunicazioni, anche alla Pubblica Amministrazione;

- essere danneggiati sistemi informatici o telematici, nell'ambito delle strutture di un concorrente.

# **PRINCIPI GENERALI DI COMPORTAMENTO**

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001, del Codice Etico adottato dalla Società, tutti i Destinatari del Modello che, a qualunque titolo, siano stati designati o incaricati alla gestione e manutenzione dei *server*, delle banche dati, delle applicazioni, dei *client* e delle reti di telecomunicazione, nonché a tutti coloro che abbiano avuto assegnate *password* e chiavi di accesso al sistema informativo aziendale sono tenuti ad osservare i seguenti principi di comportamento e controllo:

* il personale si deve astenere da qualsiasi condotta che possa compromettere la riservatezza e l’integrità delle informazioni e dei dati aziendali e dei terzi, ed in particolare si premura di non lasciare incustoditi i propri sistemi informatici e bloccarli, qualora si allontani dalla postazione di lavoro, con i propri codici di accesso ovvero di spegnere il computer e tutte le periferiche al termine dell’orario di lavoro;
* il personale si astiene da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale o altrui;
* il personale si impegna a sottoscrivere lo specifico documento relativo al corretto utilizzo delle risorse informatiche aziendali in dotazione e a cui ha accesso;
* il personale conserva i codici identificativi assegnati, astenendosi dal comunicarli a terzi, che in tal modo potrebbero accedere abusivamente a dati aziendali riservati;
* il personale non può installare programmi senza aver preventivamente informato l’Amministratore di sistema preposta alla gestione della sicurezza informatica;

# **PROCEDURE DI CONTROLLO**

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati informatici, con particolare riferimento al processo strumentale alla commissione dei reati quale gestione dell’infrastruttura tecnologica.

Di seguito è individuato il processo sensibile nell’ambito del quale potrebbero potenzialmente essere perpetrati, i reati sopra elencati, nonché i rispettivi presidi di controllo.

Gestione dei sistemi informativi

* + il personale accede al sistema informativo aziendale unicamente attraverso il profilo identificativo assegnato, attraverso *user ID* e *password* strutturate sulle base di un adeguato livello di complessità;
	+ la Funzione Editing/Grafica/Web-Informatica definisce i meccanismi di monitoraggio del traffico e di tracciatura degli eventi di sicurezza sulle reti, da parte degli utenti e degli Amministratori di sistema, nel rispetto della segregazione dei compiti (ad esempio: accessi anomali per frequenza, modalità, temporalità);
	+ la Funzione Editing/Grafica/Web-Informatica ha definito una policy formale che regola l’utilizzo della strumentazione tecnologica (e.g. laptop, telefoni) concessa in dotazione al personale della Società;
	+ l’accesso ai sistemi informativi è consentito sulla base di credenziali di accesso univoche per il personale dipendente e nel rispetto di una corretta profilazione degli utenti rispetto alla mansione svolta, nonché bloccato per i dipendenti non più in organico;
	+ sono definiti formalmente i requisiti di autenticazione ai sistemi per l’accesso ai dati per l’assegnazione dell’accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
	+ gli amministratori di sistema sono muniti di proprie credenziali di autenticazione e gli accessi sugli applicativi aziendali;
	+ l’accesso alle sale server è consentito a soggetti autorizzati;
	+ l’accesso alle informazioni che risiedono sui server e sulle banche dati aziendali, ivi inclusi i client, è limitato da strumenti di autenticazione;
	+ il server e i laptop aziendali sono protetti da programmi antivirus, aggiornati in modo automatico, contro il rischio di intrusione;
	+ sono previste procedure di controllo dell’installazione di software sui sistemi operativi da parte dei dipendenti;
	+ la Funzione Editing/Grafica/Web-Informatica deve implementare regole di utilizzo della posta elettronica, che si riassumono nel divieto d’uso della casella di posta personale per finalità estranee alle esigenze di servizio;
	+ la Funzione Editing/Grafica/Web-Informatica definisce le regole per la navigazione in Internet che includono tra le altre l’utilizzo della rete al solo fine lavorativo, il divieto di download di software nelle strutture informative aziendali (pdl, share, etc.) e di connessione a siti segnalati anche da specifica messaggistica di *alert.*