

Reati	Rischio	Attività sensibili	Aree sensibili	Rischio ex ante	Controlli esistenti	Controlli a presidio	Rischio ex post
Art. 24bis D.Lgs. 231/01 - Accesso abusivo. Diffusione abusiva di codici di accesso a sistemi informatici i telematici	<b>Detenzione e diffusione abusiva, riproduzione e/o comunicazione, consegna di codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornire indicazioni o istruzioni idonee allo scopo, al fine di procurare a se o ad altri un profitto e/o recare danno.</b>	Accesso da parte di Soggetti non abilitati e/o autorizzati, ai portali della P.A. per la trasmissione periodica di dati: ad es. adempimenti gestione personale, adempimenti societari, gestione dei tributi da riscuotere e rendiconto degli incassi ricevuti, etc.	Servizio Front office; Servizio Riscossioni; Area AMM/FIN/CTR; Servizio Back Office; Servizio Protocollo; DO (Direttore Operativo);	MEDIO	DPS ex D.Lgs. 196/2003; Gestione delle PSW;	a) Codice Etico: linee di condotta; b) Codice Disciplinare; c) Regolamento interno su utilizzo strumenti informatici; d) <b>Gestione del trattamento e della sicurezza dati in ottica ISO 27001<sup>1</sup>.</b>	BASSO
Art. 24bis D.Lgs. 231/01 -Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni	<b>Installare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi</b>	Utilizzo di hardware e sw non autorizzati dall'Azienda, allo scopo di intercettazione. Ad es. atti a procurarsi credenziali di autenticazione, allo scopo di: accedere ai portali degli Enti Pubblici per effettuare le trasmissioni informatiche e/o telematiche: differimento di informative o dichiarazioni rispetto alla	Varie aree e funzioni aziendali	MEDIO	DPS ex D.Lgs. 196/2003; Gestione delle PSW; Presenza di filtri per accesso siti web non autorizzati. DPS ADS.	a) Codice Etico: linee di condotta; b) Codice Disciplinare; c) Regolamento interno su utilizzo strumenti informatici; d) <b>Gestione del trattamento e della sicurezza dati in ottica ISO 27001<sup>2</sup>.</b>	BASSO

<sup>1</sup> Presidio suggerito a seguito dell'aggiornamento del MOG. L'Alta Direzione dell'Azienda deve valutare se applicarlo ai fini di una mitigazione del rischio rilevato ex ante.

<sup>2</sup> V. commento nota 1.

Rev. 02	1	PARTE SPECIALE – Sez. Mappatura. Allegato n. 2 "Reati connessi con la criminalità informatica".
---------	---	---

SO.RI SPA	<b>MODELLO DI ORGANIZZAZIONE, GESTIONE, CONTROLLO</b> <i>ex D.Lgs. 231/2001</i>
-----------	--

		scadenza stabilita.					
Art. 24bis D.Lgs. 231/01 -Danneggiamento di sistemi informatici o telematici di pubblica utilità	<b>distruzione, danneggiamento, di sistemi informatici o telematici dello Stato o altri Soggetti Pubblici, resa inservibile o ostacolo grave al loro funzionamento</b>	Manomissione di apparati informatici attraverso la diffusione di malware o programmi nocivi, al fine di recare a SO.RI SpA un ingiusto vantaggio (ad es. differimento di informative o dichiarazioni rispetto alla scadenza stabilita...	Varie aree e funzioni aziendali	MEDIO	DPS ex D.Lgs. 196/2003; Gestione delle PSW; Presenza di filtri per accesso siti web non autorizzati. DPS ADS.	a) Codice Etico: linee di condotta; b) Codice Disciplinare; c) Regolamento interno su utilizzo strumenti informatici; d) <b>Gestione del trattamento e della sicurezza dati in ottica ISO 27001<sup>3</sup>.</b>	<b>BASSO</b>
Art. 24bis D.Lgs. 231/01 -Danneggiamento di informazioni, dati e programmi informatici utilizzati da un ente pubblico.	<b>distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici di pubblica utilità o del socio Ente Pubblico.</b>	Cancellazione o alterazione di informazioni aziendali, tramite utilizzo di credenziali di accesso comuni fra vari pc o generiche.	Servizio Front office; Servizio Riscossioni; Area AMM/FIN/CTR; Servizio Back Office; Servizio Protocollo; DO (Direttore Operativo);	MEDIO	DPS ex D.Lgs. 196/2003; Gestione delle PSW; DPS ADS.	a) Codice Etico: linee di condotta; b) Codice Disciplinare; c) Regolamento interno su utilizzo strumenti informatici; d) <b>Gestione del trattamento e della sicurezza dati in ottica ISO 27001<sup>4</sup>.</b>	<b>BASSO</b>

<sup>3</sup> V. commento nota 1.

<sup>4</sup> V. commento nota 1.

Rev. 02	2	PARTE SPECIALE – Sez. Mappatura. Allegato n. 2 "Reati connessi con la criminalità informatica".
---------	---	---