Art.24 bis d.lgs 231/2001 - Delitti informatici e trattamento illecito di dati PAROS SRL					
Reato presupposto	**Processi/attività aziendali sensibili**	**Funzioni aziendali coinvolte**	**Potenziali attività volte a compiere il reato**	**Protocolli macro di prevenzione implementati (attività di sistema impattanti sul sistema dei poteri, sul codice di comportamento, sull'attività formativa..)**	**Protocolli micro di prevenzione implementati (attività specifiche previste dalle procedure gestionali/operative e altri documenti del sistema documentale aziendale)**
Accesso abusivo ad un sistema informatico o telematico (art.615 ter- codice penale)	Sviluppo del sofware, Supporto all'utenza, Gestione dei sistemi	Tutti i collaboratori	Cancellazione/modifica dei dati, utilizzo improrio, diffusione di dati personali e/o sensibili	Sistema di policy per il personale interno ed esterno con la sottoscrizione del regolamento e il richiamo alla normativa di legge. Sono in corso le attività pèer l'implementazione della certificazione ISO 27000.	Utilizzo di password personali con registrazione degli accessi e tracciatura, ove possibile/necessario, delle modifiche apportate. Sono in corso le attività pèer l'implementazione della certificazione ISO 27000.
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art.617 quater c.p.)	Sviluppo del sofware, Supporto all'utenza, Gestione dei sistemi	Tutti i collaboratori	Modifca dei dati dei beneficiari dei mandati di pagamento, Divulgazione di dati personale e/o sensibili.	Sistema di policy per il personale interno ed esterno con la sottoscrizione del regolamento e il richiamo alla normativa di legge. Inclusione nel regolamento sottoscritto dai collaboratori esterni ed interni delle clausole di non divulgazione delle informazioni.	Le procedure interne prevedono la rimozione dei diritti di accesso al termine del rapporto di lavoro. I documenti di pagamento sono firmati digitalmente e le specifiche di firma dei firmatari autorizzati sono depositati in tesoreria.
Installazione di apparecchiature attead intercettare, impedire od interrompere comunciazioni informatiche o telematiche (art. 617 - quinquies c.p.)	Nessun processo				
Danneggiamento di informazioni, dati e programmi informatici (art.635 bis c.p.)	Nessun processo				
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.)	Sviluppo del sofware, Supporto all'utenza, Gestione dei sistemi	Tutti i collaboratori	Modifca dei dati dei beneficiari dei mandati di pagamento, Divulgazione di dati personale e/o sensibili.	Sistema di policy per il personale interno ed esterno con la sottoscrizione del regolamento e il richiamo alla normativa di legge. Inclusione nel regolamento sottoscritto dai collaboratori esterni ed interni delle clausole di non divulgazione delle informazioni.	Le procedure interne prevedono la rimozione dei diritti di accesso al termine del rapporto di lavoro. I documenti di pagamento sono firmati digitalmente e le specifiche di firma dei firmatari autorizzati sono depositati in tesoreria.
Danenggiamento di sistemi informatici o telematici (art.635 quater c.p.)	Nessun processo				
Danneggiamento di sistemi informatici o telematici di pubblica utilità (art.635 quinquies, co.3 c.p.)	Nessun processo				
Detenzione e diffusone abusiva di codici di accesso a sistemi informatici o telematici (art.615 quater c.p.)	Sviluppo del sofware, Supporto all'utenza, Gestione dei sistemi	Tutti i collaboratori	Cancellazione/modifica dei dati, utilizzo improrio, diffusione di dati personali e/o sensibili	Sistema di policy per il personale interno ed esterno con la sottoscrizione del regolamento e il richiamo alla normativa di legge. In particolare sulle modalità di gestione delle credenziali. Sono in corso le attività per l'implementazione della certificazione ISO 27000.	Utilizzo di password personali con registrazione degli accessi e tracciatura, ove possibile/necessario, delle modifiche apportate. Sono in corso le attività pèer l'implementazione della certificazione ISO 27000.
Diffusione di apparecchiature dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)	Sviluppo del sofware, Supporto all'utenza, Gestione dei sistemi	Tutti i collaboratori	Inserimento sui sistemi di software malevolo (virus o malware)	Sistema di policy per il personale interno ed esterno con la sottoscrizione del regolamento e il richiamo alla normativa di legge. Nel regolamento interno è previsto un apposito paragrafo (2.2.4) riguardante la gestione del software antivirus.	Sui server e sulle singole postazioni è installato un software antivirus. Le definizioni dei virus vengono aggiontate in automatico sul server e distribuite su tutti i client. Sul server di posta elettronica è istallato un apposito antivirus che controlla tutte la posta in entrata.
Falsità nei documenti informatici (art.491 bis c.p.)	Nessun processo				
Frode informaticadel soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)	Servizio di Registration Authority	Gruppo Servizi Applicativi (abilitati come Registration Authority Officer)	Emissione di certificato di firma digitale con identità diversa dalla propria	Sistema di policy per il personale interno ed esterno con la sottoscrizione del regolamento e il richiamo alla normativa di legge. Le procedure di sicurezza sono legate al processo identificato e garantito dalla Certification Authority (R.A.).	La R.A. invia settimanalmante il resoconto dei certificati emessi per la rendicontazione e per il controllo. E' comunque possibile verificare in tempo reale gli stessi dati sul sito del certificatore.