Attività sensibile: **GESTIONE COLLEGAMENTI TELEMATICI (IN ENTRATA E IN USCITA) O TRASMISSIONE DI DATI SU SUPPORTI INFORMATICI A PUBBLICHE AMMINISTRAZIONI, ENTI PUBBLICI O AD AUTORITÀ**

Nota sul contenuto: Gestione di collegamenti telematici e trasmissioni di dati ad P.A., Autorità di Vigilanza, Amministrazione finanziaria e altri soggetti pubblici

Reati associabili: Corruzione (art. 318 c.p.) concussione (art. 317 c.p.) corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), .induzione indebita a dare o promettere utilità (art. 319-quater cod. pen.) corruzione tra privati (art. 2635, comma3, cod. civ.) corruzione di persona incaricata di pubblico servizio (art. 320 c.p.) istigazione alla corruzione (art. 322 c.p.), peculato, concussione, corruzione ed istigazione alla corruzione di membri e di funzionari degli organi della Comunità europea (art. 322 bis c.p.), truffa (art. 640 c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (640 bis c.p.), frode informatica (art. 640 ter)falsità in documenti informatici (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 apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (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 od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.) indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter c.p.), detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contatti (art. 493 quater c.p.)

U.O. interessate: Direttore (DIR)

Consiglio di Amministrazione

Responsabile IT (IT)

Amministrazione e Personale (AMM)

Altre entità: Tecnici esterni

		UNITA' ORGANIZZATIVE	DESCRIZIONE DEL PROCESSO	GAP	POSSIBILI IMPLEMENTAZIONI
CONTROLLI GENERALI	**Segregazione responsabilità**	IT IT	**Gestione dei sistemi informatici e della sicurezza** I dipendenti accedono ai propri computer ed al sistema di rete tramite una password loro assegnata al momento dell'entrata in azienda. L'utente riceve il sollecito a cambiarla non appena riceve la dotazione aziendale. L'accesso ai dati identificativi dell'utente è consentito al solo Amministratore di rete, ed al personale di ditte terze, preposto alla manutenzione del sistema informatico. La posta elettronica viene gestita direttamente sui singoli pc. Al server di rete, si accede, a seconda delle autorizzazioni ricevute, tramite apposite PW di rete personali. **Sicurezza informatica** Sono applicate misure di sicurezza standard con l'accesso alla rete aziendale tramite user-id personale e password. Le password sono custodite a cura di ciascuna risorsa interessata. Ciascun utente è infatti responsabile in prima persona della gestione e della protezione della password assegnata che non deve esser comunicata a terzi per nessun motivo e deve esser periodicamente modificata, come da promemoria degli stessi programmi. La Seram è dotata di un archivio informatico per la conservazione dei documenti. L'accesso alle cartelle condivise, contenenti questi documenti, è regolato da appositi diritti di acceso, rilasciate da IT. Le password di accesso al sistema informatico ed i profili degli utenti danno accesso ai moduli del programma relativo alle responsabilità e alle mansioni dei singoli operatori. Tutti gli accessi possono essere tracciati e monitorati. L'attivazione e l'aggiornamento dei profili utente avviene ad opera dell'IT. La rete ed eventuali esigenze collegate ai profili utenti, oltre che ai filtri antivirus, antispam e di sicurezza in genere, sono responsabilità dell'IT. Le password attribuite da Enti pubblici ai responsabili aziendali competenti, per l'invio telematico dei dati richiesti da specifiche disposizioni di legge, sono tenute e conservate a cura degli stessi responsabili che ne garantiscono la necessaria riservatezza.		

		UNITA' ORGANIZZATIVE	DESCRIZIONE DEL PROCESSO	GAP	POSSIBILI IMPLEMENTAZIONI
		DIR APP CdA DIR AMM	**Collegamenti telematici alla Pubblica Amministrazione** DIR e APP possiedono la password di accesso all'Agenzia delle Dogane. **Pagamenti in via telematica** I contributi, le imposte ed i compensi per i fornitori, in base a quanto previsto dalle deleghe aziendali, sono pagati in via telematica a firma congiunta DIR e AMM: - i contributi sono pagati tramite invio F24 on line predisposti da AMM: - le imposte sono pagate tramite invio F24 on line predisposti da AMM.		

		UNITA' ORGANIZZATIVE	DESCRIZIONE DEL PROCESSO	GAP	POSSIBILI IMPLEMENTAZIONI
	Documentazione di supporto		Archivio informatico delle utenze "Procedura per l'utilizzo dei sistemi informatici di proprietà della Seram SpA" "Procedura per l'archiviazione dei documenti Autocad"		

		UNITA' ORGANIZZATIVE	DESCRIZIONE DEL PROCESSO	GAP	POSSIBILI IMPLEMENTAZIONI
	Tracciabilita'		La tracciabilità delle responsabilità è garantita dal sistema informatico aziendale, che permette di monitorare e registrare gli accessi e le attività svolte da ciascun utente. Il sistema chiede all'utente con cadenza periodica di modificare la propria password. Ogni accesso esterno può avvenire unicamente a seguito della volontaria comunicazione della password da parte dell'utente che ha necessità di supporto informatico, o attraverso controllo e comunicazione del proprio codice di accesso (variabile) verificabile al momento.		
CONTROLLI SPECIFICI	**Obbligo di segnalazione**		I responsabili delle unità organizzative che hanno contatti con Enti Pubblici, attraverso l'utilizzo di strumenti informatici o banche dati, devono comunicare all'Organismo di vigilanza eventuali problematiche o anomalie che possano verificarsi nell'ambito dell'attività in esame.		