AREA RISCHIO: PROCESSI ICT

MAPPATURA DEI PROCESSI

PROCESSO	prog	FINALITA'/FASE/ATTIVITA'	INPUT	OUTPUT	MACRO PROCESSI COINVOLTI
Gestione della Riservatezza delle informazioni nell'ambito dei trattamenti effettuati	**1**				**Pianificazione e sviluppo delle applicazioni software, delle banche dati e delle infrastrutture di elaborazione delle informazioni nell'ottica della tutela della riservatezza**
			Acquisizione di assett	Gestione in sicurezza e dismissione di Asset	
	1.1	Validazione in fase di acquisizione			
	1.2	Presa in carico e gestione			
	1.3	Dismissione sicura degli assett al termine del ciclo di vita			
Gestione dell'integrità delle informazioni gestite nell'ambito dei trattamenti effettuati	**2**				**Pianificazione e sviluppo delle applicazioni software** **Gestione dei sistemi informatici, delle banche dati e delle reti di comunicazione al fine di tutelare l'integrità del dato**
			Acquisizione di applicativi ed assett volti alla elaborazione dei dati	Gestione in sicurezza e dismissione di Asset	
	2.1	Validazione			
	2.2	Presa in carico			
	2.3	Configurazione secondo le specifiche del titolare/respomnsabile			
Gestione della continuità di servizio dei trattamenti effettuati (sia per guasti che per eventi di cybersicurezza)	**3**				**Gestione degli asset informatici e dei Dispositivi medici e delle reti di comunicazione al fine di tutelare la continuità di servizio**
			Richiesta di intervento	Rapporto d'intervento	
	3.1	Validazione (in paticolare discrimine fra guasto ed evento di Cybersicurezza)			
	3.2	Presa in carico			
	3.3	Effettuazione dell'intervento volto a ripristinare la continuità di servizio			
Implementazione, manutenzione e gestione del sistema di gestione della sicurezza	**4**				**Responsabilità e gestione della sicurezza informatica**
			Asset, processi aziendali e analisi dei rischi	Sistema di gestione della sicurezza informatica formalizzato	
	5.1	Analisi dei rischi			
	5.2	Implementazione delle misure di protezione			
	5.3	Implementazione dei sistemi di monitoraggio			
	5.4	Implementazione delle misure di contenimento e ripristino e gestione delle "Lesson Learned"			

AREA RISCHIO: PROCESSI ICT

Nota bene: nel presente documento sono riportati in forma sintetica rischi e misure collegate alla prevenzione della corruzione. Sono in corso con scadenze 2025-2026 la redazione di documenti specifici previsti per ottemperare allaDirettiva (UE) 2022/2555 (c.d. Direttiva NIS 2) recepita in italia 16 ottobre 2024 è entrato in vigore il Decreto Legislativo 4 settembre 2024, n. 138, volta a garantire a livello europeo un livello comune elevato di cibersicurezza

REGISTRO DEI RISCHI

prog	PROCESSO/FASE	EVENTO RISCHIOSO	INDICATORI DI RISCHIO		FATTORI ABILITANTI		MOTIVAZIONE VALUTAZIONE RISCHIO	VALUTAZIONE RISCHIO	TIPOLOGIA MISURE	MISURE DI PREVENZIONE	MONITORAGGIO E INDICATORI	UNITA' ORGANIZZATIVA RESPONSABILE	Tempi di attuazione della misura	Indicatori di MONITORAGGIO	Target	Tempi di monitoraggio	Note
1.0	**Gestione della Riservatezza delle informazioni nell'ambito dei trattamenti effettuati**	Accesso indebito di personale autorizzato / abuso delle credenziali / accesso indebito da parte di personale non autorizzato: a) Comunicazione di informazioni a soggetti terzi non autorizzati che ne possono trarre vantaggio;	altro		inadeguata diffusione della cultura della legalità		* Mancanza di proceduralizzazione delle attività legate al processo; * Difficoltà di delimitazione del campo di azione e di monitoraggio delle attività degli amministratori di sistema. Questi fattori in realtà sono mitigati da attribuzione di responsabilità a personale in possesso dei requisiti di professionalità e competenza adeguati per il ruolo.	BASSO	definizione e promozione dell'etica e di std di comportamento	**Prevenzione del rischio di comunicazione fraudolenta di informazioni** : * mirata attribuzione di responsabilità a personale adeguatamente formato; * registrazione di ogni accesso ai dati nei log di sistema; * implementazione di strumenti di reportistica ed analisi avanzata dei log di sistema (in progettazione).	Verifica periodica a campione dell'attività degli amministratori di sistema	ICT	misura da programmare nel triennio del PTPCT	N° di accessi anomali	→ 0	annuale	
2.0	**Gestione dell'integrità delle informazioni gestite nell'ambito dei trattamenti effettuati**	Alterazione o cancellazione di dati ed informazioni a seguito di accesso indebito o anche legittimo: a) Alterazione o cancellazione di dati ed informazioni a favore di soggetti terzi non autorizzati	livello di interesse esterno	altro	altro	scarsa responsabilizzazione interna	* Mancanza di proceduralizzazione delle attività legate al processo; * Difficoltà di delimitazione del campo di azione e di monitoraggio delle attività degli amministratori di sistema. Questi fattori in realtà sono mitigati da attribuzione di responsabilità a personale in possesso dei requisiti di professionalità e competenza adeguati per il ruolo.	BASSO	formazione	* Prevenzione del rischio di alterazione/cancellazione fraudolenta delle informazioni:	Verifica periodica a campione dell'attività degli amministratori di sistema	ICT	misura da programmare nel triennio del PTPCT	N° di accessi anomali	→ 0	annuale	
3.0	**Gestione della continuità di servizio dei trattamenti effettuati (sia per guasti che per eventi di cybersicurezza)**	Ritardo od omissione fraudolenta di risoluzione del guasto o di risoluzione di evento di Cybersecurity	grado di attuazione delle misure di trattamento		inadeguatezza o scarsa competenza del personale addetto ai processi		* Non sempre gli interventi sono svolti in modo tempestivo ed efficace a causa di sottovalutazione o analisi parziale del problema. In altri casi il ritardo nella risoluzioen del problema può essere causato da una scarsa proceduralizzazioen delle attività di ripristino. Questi fattori possono produrre conseguenze sulla continuità operativa anche di strutture critiche, ma in genere non è frutto di una volontà fraudolenta bensì di procedure non sempre ben definite o scarsa consapevolezza.	BASSO	controllo	*Implementazione di procedure di ripristino e formazione del personale * Implemetazione della procedura prevista entro fine 2025 della direttiva NIS2	monitoraggio tempi di ripristino e indicatori di mancata funzionalità delle infrastrutture chiave	ICT	misura da programmare nel triennio del PTPCT	N° di non conformità rilevate rispetto aglin indicatori temporali	→ 0	annuale	
4.0	**Implementazione, manutenzione e gestione del sistema di gestione della sicurezza**	Bypass o abbassamento delle misure di sicurezza, allo scopo di facilitare un accesso fraudolento all'infrastruttura ICT Mascheramento o ritardata segnalazione di una intrusione o violazione di sicurezza	grado di attuazione delle misure di trattamento	livello di interesse esterno	esercizio prolungato ed esclusivo della responsabilità di un processo da parte di pochi		* Proceduralizzazione e pianificazione delle attività legate al processo da migliorare; * Difficoltà di dedicare all'attività, possibilmente a tempo pieno, personale con specifica professionalità. Questi fattori in realtà sono mitigati da attribuzione di responsabilità a personale in possesso dei requisiti di professionalità e competenza adeguati per il ruolo, nonché da numerose misure di sicurezza in atto e in corso di sviluppo relativamente al tema generale della cybersecurity, e che comunque incidono positivamente anche sui rischi corruttivi.	BASSO		* backup dei dati Periodici (giornalieri per i sistemi più critici) * registrazione di log di attività di Bypass o abbassamento delle misure di sicurezza	Verifica a campione della effettuazione dei Back Up Verifica a campione di eventuali anomali dei sicurezza	ICT	misura da programmare nel triennio del PTPCT	N.rp di BackUp non eseguiti secondo la tempistica prevista n. anomalie	→ 0	annuale	