

**AREA AMMINISTRATIVA**



**ELENCO DEI PROCESSI**

**REGISTRO E VALUTAZIONE DEI RISCHI**

**PROGRAMMA DELLE MISURE**

**(in applicazione dell'allegato n. 1 al PNA 2019)**

MAPPATURA DI TUTTI PROCESSI DELLA STRUTTURA

AREA DI RISCHIO	PROCESSO	DESCRIZIONE DEL PROCESSO	FASE/ATTIVITA'	UNITA' ORGANIZZATIVA COMPETENTE									
Acquisizione e gestione del personale	Gestione del ciclo delle performance	<p><b>Descrizione del processo:</b> il Decreto Legislativo 27 ottobre 2009, n. 150 e s.m.l. "Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni" che, all'art. 10, con lo scopo di assicurare qualità, comprensibilità ed attendibilità dei documenti di rappresentazione della performance aziendale, stabilisce l'adozione, in coerenza con i contenuti e il ciclo della programmazione finanziaria e di bilancio, di un documento programmatico, denominato Piano della Performance. L'art. 15, comma 2, lettera b) del predetto Decreto prevede che l'organo di indirizzo politico-amministrativo delle PP.AA. definisce in collaborazione con i vertici dell'organizzazione aziendale. L'Istituto si dota di un proprio ciclo di gestione delle performance, che prevede l'adozione di un piano triennale in relazione alle performance attese, con propri indicatori e con gli strumenti di valutazione del livello di raggiungimento delle stesse, da approvarsi con deliberazione del consiglio di amministrazione, su proposta del direttore generale. Nell'ambito del Piano Performance sono individuati gli Obiettivi Strategici triennali. Il Piano della Performance è lo strumento che dà avvio al ciclo di gestione della Performance in quanto attraverso tale documento programmatico di durata triennale, l'Istituto individua obiettivi, indicatori, risultati attesi per la gestione aziendale. Gli obiettivi strategici vengono declinati nel c.d. "Albero delle Performance" in obiettivi operativi, accompagnati dai relativi indicatori e target, come negoziati dalla Direzione con i dirigenti responsabili delle strutture. Nell'ambito degli stessi indicatori vanno poi identificati quelli che costituiscono i c.d. "Indicatori pesati", collegati al sistema premiante definito dalla contrattazione integrativa decentrata, da assegnarsi alle strutture affinché, al fine del riconoscimento della retribuzione di risultato per la Dirigenza e la produttività per il personale del Comparto. Ciascuna struttura deve rendicontare il raggiungimento degli obiettivi, rispetto ad indicatori e target. Il Direttore Generale elabora la Relazione sulla Performance (un documento che evidenzia, a consuntivo, con riferimento all'anno precedente, i risultati organizzativi e individuali raggiunti rispetto ai singoli obiettivi programmati ed alle risorse, con rilevazione degli eventuali spostamenti) che, una volta validata dal Nucleo di Valutazione, trasmette al Consiglio di Amministrazione per l'approvazione. Il processo si conclude con l'erogazione del trattamento economico al personale dipendente.</p> <p><b>Input:</b> individuazione degli obiettivi di Performance  <b>Output:</b> adozione del Piano integrato di performance, relazione sulla performance</p> <p><b>PERSONALE DELLA UO IMPEGNATO NEL PROCESSO:</b> DIRIGENTE U.O. PROGRAMMAZIONE SERVIZI TECNICI E CONTROLLO DI GESTIONE E 1 COLLABORATORE (Ufficio controllo di gestione e performance)  <b>RESPONSABILITA':</b> DIRIGENTE DELLA U.O. PROGRAMMAZIONE SERVIZI TECNICI E CONTROLLO DI GESTIONE (REGOLARITA' TECNICA), DIRIGENTI DELLE STRUTTURE (ANALISI DEL CONTESTO, NEGOZIAZIONE DEGLI OBIETTIVI) DIRETTORE GENERALE (NEGOZIAZIONE DEGLI CON I DIRIGENTI DELLE STRUTTURE DEGLI OBIETTIVI OPERATIVI, INDIVIDUAZIONE DEGLI OBIETTIVI OPERATIVI)</p>	adozione del Piano Performance individuazione degli obiettivi operativi, indicatori e target adozione dell'Albero delle Performance acquisizione dei report sul raggiungimento degli obiettivi rispetto ai target ed agli indicatori approvazione Relazione sulla Performance pubblicazione nella sezione Amministrazione Trasparente del sito web della Relazione sulla Performance acquisizione delle rendicontazioni di ciascuna struttura sul raggiungimento degli obiettivi verifica requisiti per erogazione trattamento economico al personale dipendente determinazione del trattamento economico erogazione del trattamento economico al personale dell'IZSLER	Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance									
			Gestione delle entrate, delle spese e del patrimonio	Valorizzazione delle prove di laboratorio	<p><b>Descrizione del processo:</b> Il Processo è finalizzato alla valorizzazione e validazione delle prestazioni di laboratorio erogate dall'Istituto. La valorizzazione delle prove di laboratorio e dei prodotti precede ogni aggiornamento, modifica ed integrazione del tariffario dell'Istituto, così come previsto all'articolo 11, lett.e) dello Statuto dell'Ente. I criteri di valorizzazione sono indicati nella deliberazione del Consiglio di Amministrazione n.9/2018.</p> <p><b>IMPEGNATO NEL PROCESSO:</b> Dirigenti incaricati per la gestione del nomenclatore delle prove di laboratorio, Dirigenti valorizzatori e dirigenti validatori delle prove di laboratorio, Personale U.O. PROGRAMMAZIONE SERVIZI TECNICI E CONTROLLO DI GESTIONE (Ufficio controllo di gestione e performance)</p>	Invio da parte del Dirigente responsabile del piano di monitoraggio alla Direzione Generale di una richiesta di attivazione del piano di monitoraggio Valorizzazione della prova e invio per la validazione al Dirigente validatore preposto Verifica della valorizzazione, validazione e comunicazione all'ufficio Controllo di Gestione e performance Determinazione della tariffa della prova di laboratorio da parte dell'ufficio Controllo di gestione e performance sulla base della valorizzazione validata e predisposizione del relativo provvedimento di aggiornamento del tariffario Aggiornamento del tariffario da parte dell'ufficio Controllo di gestione e performance dopo l'approvazione da parte del Direttore Generale, pubblicato sul sito istituzionale	Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance						
						Gestione delle entrate, delle spese e del patrimonio	Valorizzazione dei prodotti / prezzo di vendita dei prodotti (tariffazione)	<p><b>Descrizione del processo:</b> Il processo è finalizzato alla valorizzazione e validazione dei prodotti forniti dall'Istituto per la definizione dei prezzi di vendita da inserire nel catalogo dei prodotti dell'Istituto.</p> <p><b>PERSONALE IMPEGNATO NEL PROCESSO:</b> Dirigenti gestori dei magazzini dei prodotti, Dirigenti valorizzatori e validatori dei prodotti, Direzione Sanitaria, Personale U.O. ProvvEDITORATO Economato e Vendite, personale U.O. PROGRAMMAZIONE SERVIZI TECNICI E CONTROLLO DI GESTIONE (Ufficio controllo di gestione e performance)</p>	Assegnazione del la valorizzazione del prodotto al Dirigente valorizzatore proposto da parte del Dirigente gestore del magazzino prodotti Valorizzazione del prodotto e invio per la validazione al Dirigente validatore preposto Verifica la valorizzazione, validazione e comunicazione all'ufficio Controllo di gestione e performance Proposta del prezzo di vendita da parte del Dirigente valorizzatore Verifica di Congruità del prezzo proposto rispetto alla valorizzazione del prodotto da parte del Direttore Sanitario con l'ufficio Controllo di Gestione e performance Conferma del prezzo di vendita proposto da parte del Direttore Sanitario Aggiornamento del catalogo dei prodotti venduti da parte dell'U.O. ProvvEDITORATO Economato e Vendite	Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance			
									Gestione delle entrate, delle spese e del patrimonio	Controllo richieste di nota di variazione di fatture emesse	<p><b>Descrizione del processo:</b> Il processo è finalizzato al controllo della corrispondenza fra i dati presenti nel software sanitario e quanto indicato nelle richieste di nota di variazione da emettere relativamente a fatture già contabilizzate</p> <p><b>PERSONALE IMPEGNATO NEL PROCESSO:</b> Personale U.O. PROGRAMMAZIONE SERVIZI TECNICI E CONTROLLO DI GESTIONE (Ufficio controllo di gestione e performance) e Personale U.O. Gestione Servizi Contabili</p>	Ricezione da parte dell'ufficio Controllo di Gestione e performance dall'U.O. Gestione Servizi Contabili delle richieste di emissione di note di variazione L'ufficio Controllo di Gestione e performance effettua un controllo di corrispondenza fra i dati presenti nel software sanitario e quanto indicato nelle richieste di nota di variazione da emettere. Se il controllo è positivo l'ufficio Controllo di Gestione e performance comunica l'esito al U.O. Gestione Servizi Contabili che procederà ed emettere la nota di variazione, in caso negativo l'ufficio Controllo di Gestione e performance comunica al reparto che ha emesso la richiesta di procedere con le opportune modifiche nel software sanitario	Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance

Gestione delle attività di ricerca	Attivazione piani di monitoraggio	<p><b>Descrizione del processo:</b> Il processo è mirato all'attivazione di piani di monitoraggio finalizzati allo sviluppo delle conoscenze in materia di sicurezza alimentare e sanità veterinaria. Il processo è finalizzato all'approvazione del decreto di attivazione di piani di monitoraggio e, dopo approvazione da parte del Direttore Generale, prevede la codifica nei software gestionali aziendali al fine di permettere la rendicontazione completa dei costi dell'attività svolta.</p> <p><b>PERSONALE IMPEGNATO NEL PROCESSO:</b> Dirigente responsabile del piano di monitoraggio, Direzione Generale, Personale U.O. PROGRAMMAZIONE SERVIZI TECNICI E CONTROLLO DI GESTIONE (Ufficio controllo di gestione e performance)</p>	<p>Invio da parte del Dirigente responsabile del piano di monitoraggio alla Direzione Generale di una richiesta di attivazione del piano di monitoraggio</p> <p>Autorizzazione da parte del Direttore Generale dell'attivazione del piano e comunicazione all'ufficio Controllo di Gestione e performance</p> <p>Predisposizione del provvedimento di attivazione del piano e codifica il piano dei software aziendali da parte dell'ufficio Controllo di Gestione e performance</p> <p>Rendicontazione dell'attività svolta al Direttore Generale</p>	<p>Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance</p>
B) Contratti pubblici - Affidamento di lavori, servizi e forniture	Definizione degli standard metodologici, documentali e architetture per la realizzazione e l'erogazione dei servizi IT	<p>Questo processo riguarda la realizzazione dell'architettura teorica con la quale i Sistemi Informativi intendono soddisfare le esigenze sia infrastrutturali che applicative dell'Istituto.</p> <p>Si tratta di analizzare come recepire ed elaborare i fabbisogni di servizi IT, definire e gestire il Portafoglio dei servizi ICT, definire e pianificare le misure logiche e fisiche di sicurezza e gli altri adempimenti necessari a garantire la sicurezza delle informazioni e la tutela della privacy, definire gli standard metodologici e documentali per le attività di progettazione e sviluppo dei servizi IT, curare la progettazione e lo sviluppo dei servizi per l'accesso ai dati disponibili presso le banche dati gestite anche in modalità Open data, svolgere le funzioni di Program e Project Management ICT, coadiuvare la progettazione, lo sviluppo e la gestione tecnica dei siti web.</p> <p>Responsabilità complessiva: Responsabile dei Sistemi Informativi</p> <p>1) Ricognizione Ricognizione standard metodologici e best practice di riferimento ATTIVITA': Raccolta ed analisi della documentazione disponibile su Standard e Best Practice di riferimento. Ricerca su web, partecipazione a convegni e seminari RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>2) Adozione Recepimento e adozione degli standard di riferimento nel contesto IZSLER ATTIVITA': Predisposizione ed aggiornamento degli standard IZSLER per lo sviluppo dei servizi e predisposizione della relativa documentazione RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>3) Analisi esigenze architetture dell' IT di IZSLER Raccolta ATTIVITA': Raccolta requisiti architetture necessari a supportare lo sviluppo dell'IT IZSLER. Verifica architettura esistente, stima del dimensionamento sulla base delle richieste e progetti noti e delle indicazioni di legge RESPONSABILITA': Dirigente Sistemi Informativi Formalizzazione ATTIVITA': Formalizzazione documento di analisi dei requisiti architetture necessari a supportare lo sviluppo dell'IT IZSLER</p>	<p>1.1) Ricognizione: Raccolta ed analisi della documentazione disponibile su Standard e Best Practice di riferimento</p> <p>1.2) Adozione: Predisposizione ed aggiornamento degli standard IZSLER per lo sviluppo dei servizi e predisposizione della relativa documentazione</p> <p>1.3) Analisi esigenze architetture dell' IT di IZSLER Raccolta ATTIVITA': Raccolta requisiti architetture necessari a supportare lo sviluppo dell'IT IZSLER. Verifica architettura esistente, stima del dimensionamento sulla base delle richieste e progetti noti e delle indicazioni di legge Formalizzazione ATTIVITA': Formalizzazione documento di analisi dei requisiti architetture necessari a supportare lo sviluppo dell'IT IZSLER</p>	<p>Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi</p> <p>Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi</p> <p>Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi</p>
B) Contratti pubblici - Affidamento di lavori, servizi e forniture	Gestione della Capacità dei sistemi/servizi IT Comprendere i requisiti aziendali correnti e futuri, le operazioni dell'organizzazione, l'infrastruttura informatica e garantire che tutti gli aspetti relativi alle prestazioni e alle capacità siano forniti ottimizzando costi, risorse e qualità	<p>Gestione della Capacità dei sistemi/servizi IT di comprendere i requisiti aziendali correnti e futuri, le operazioni dell'organizzazione, l'infrastruttura informatica e garantire che tutti gli aspetti relativi alle prestazioni e alle capacità siano forniti ottimizzando costi, risorse e qualità</p> <p>Responsabilità Complessiva: Dirigente Sistemi Informativi</p> <p>1) Analisi previsionale della capacità dei sistemi Analisi ATTIVITA': Analisi dei dati provenienti dalle attività di monitoraggio relative all'occupazione di spazio storage, memoria, processori, etc. Vengono raccolti dalle console di monitoraggio dell'infrastruttura i principali key indicator sul consumo di memoria, spazio RESPONSABILITA': Dirigenti Sistemi Informativi ATTIVITA': Analisi dei trend di crescita della capacità occupata e stima delle ulteriori esigenze di acquisizione di hardware/software, risorse e servizi RESPONSABILITA': Dirigenti Sistemi Informativi Valutazione impatto ATTIVITA': In caso di partenza di nuovi progetti, modifiche normative che abbiano impatto su numero utenti dei servizi e/o quantità di dati acquisiti, stima della capacità aggiuntiva necessaria e analisi delle ulteriori esigenze di acquisizione di hardware/software RESPONSABILITA': Dirigenti Sistemi Informativi Formalizzazione fabbisogni ATTIVITA': Formalizzazione dei fabbisogni di approvvigionamento di hardware/software, risorse e servizi. Se l'analisi dell'impatto evidenzia la necessità di un upgrade dell'infrastruttura, la stessa viene segnalata e da avvio al processo : "Gestione domanda e pianificazione servizi IT" RESPONSABILITA': Dirigenti Sistemi Informativi</p>	<p>2.1) Analisi previsionale della capacità dei sistemi Analisi ATTIVITA': Analisi dei dati provenienti dalle attività di monitoraggio relative all'occupazione di spazio storage, memoria, processori, etc. Vengono raccolti dalle console di monitoraggio dell'infrastruttura i principali key indicator sul consumo di memoria, spazio ATTIVITA': Analisi dei trend di crescita della capacità occupata e stima delle ulteriori esigenze di acquisizione di hardware/software, risorse e servizi Valutazione impatto ATTIVITA': In caso di partenza di nuovi progetti, modifiche normative che abbiano impatto su numero utenti dei servizi e/o quantità di dati acquisiti, stima della capacità aggiuntiva necessaria e analisi delle ulteriori esigenze di acquisizione di hardware/software Formalizzazione fabbisogni ATTIVITA': Formalizzazione dei fabbisogni di approvvigionamento di hardware/software, risorse e servizi. Se l'analisi dell'impatto evidenzia la necessità di un upgrade dell'infrastruttura, la stessa viene segnalata e da avvio al processo : "Gestione domanda e pianificazione servizi IT"</p>	<p>Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi</p>
B) Contratti pubblici - Affidamento di lavori, servizi e forniture	Gestione della domanda e Pianificazione servizi IT	<p>Questo processo gestisce il ricevimento delle richieste di servizi IT (sia infrastrutturali che applicativi) da parte dei reparti ed uffici IZSLER, la loro quantificazione e pianificazione, l'approvazione da parte delle Direzioni, e l'elaborazione del piano dettagliato di realizzazione</p> <p>Responsabilità complessiva: Dirigente Sistemi Informativi</p> <p>1) Rilevazione e consolidamento dei fabbisogni di servizi/applicazioni IT Acquisizione ATTIVITA': Acquisizione, dagli uffici/strutture IZSLER, dei fabbisogni di servizi e applicazioni IT. Ricezione delle richieste da parte del reparto con la vidimazione del responsabile di struttura complessa o semplice se trattasi di struttura in staff RESPONSABILITA': Dirigenti Sistemi Informativi ATTIVITA': Incontri di approfondimento con le strutture al fine di dettagliare le esigenze funzionali, i vincoli di progetto, ... RESPONSABILITA': Dirigenti Sistemi Informativi Elaborazione ATTIVITA': Elaborazione della documentazione relativa alle specifiche tecniche/applicative di sviluppo dei servizi/applicazioni IT. Le specifiche funzionali devono essere approvate dal dirigente di struttura complessa o semplice (se struttura in staff) da cui è partita la richiesta RESPONSABILITA': Dirigenti Sistemi Informativi Consolidamento ATTIVITA': Analisi e consolidamento dei fabbisogni di servizi e applicazioni IT per arrivare ad una proposta di pianificazione progetti. RESPONSABILITA': Dirigenti Sistemi Informativi</p> <p>2) Definizione delle esigenze di sviluppo di servizi/applicazioni IT e quantificazione degli interventi Formalizzazione bisogni ATTIVITA': Formalizzazione delle esigenze di sviluppo di servizi/applicazioni e relativa quantificazione ai fini di soddisfare la domanda interna RESPONSABILITA': Dirigenti Sistemi Informativi ATTIVITA': Richiesta di approvazione priorità ed interventi di sviluppo da parte della Direzione RESPONSABILITA': Direzioni</p> <p>3) Elaborazione piano degli interventi IT Definizione ATTIVITA': Definizione interventi IT da realizzare nel corso dell'anno. Dalla proposta approvata stesura del calendario attività RESPONSABILITA': Dirigenti Sistemi Informativi ATTIVITA': Stesura del piano di esecuzione con dettaglio dei tempi e delle modalità richieste al fornitore Monitoraggio ATTIVITA': Monitoraggio e controllo dell'attuazione delle attività a piano RESPONSABILITA': Dirigenti Sistemi Informativi</p>	<p>3.1) Rilevazione e consolidamento dei fabbisogni di servizi/applicazioni IT: Acquisizione, dagli uffici IZSLER, dei fabbisogni di servizi e applicazioni IT Incontri di approfondimento con le strutture al fine di dettagliare le esigenze Elaborazione della documentazione relativa alle specifiche tecniche/applicative di sviluppo dei servizi/applicazioni IT</p> <p>3.2) Definizione delle esigenze di sviluppo di servizi/applicazioni IT e quantificazione degli interventi: Formalizzazione delle esigenze di sviluppo di servizi/applicazioni e relativa quantificazione ai fini di soddisfare la domanda interna Richiesta di approvazione priorità ed interventi di sviluppo da parte della Direzione</p> <p>3.3) Elaborazione piano degli interventi IT: Definizione interventi IT da realizzare nel corso dell'anno Definizione del piano di realizzazione Monitoraggio e controllo dell'attuazione delle attività a piano</p>	<p>Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi</p> <p>Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi</p> <p>Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi</p>

Controlli verifiche, ispezioni e sanzioni	<p>Erogazione dei Servizi</p> <p>Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT.</p> <p>Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi</p> <p>Responsabilità complessiva: Dirigente Sistemi Informativi</p> <p>1) Definizione dei requisiti di disponibilità</p> <p>Disponibilità</p> <p>ATTIVITA': Definizione dei requisiti di disponibilità; definizione, per ciascun servizio, delle finestre di disponibilità verso l'esterno o derivarli da vincoli normativi/regolamentari/tecnici o da requisiti provenienti dagli uffici</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>2) Monitoraggio della disponibilità dei servizi</p> <p>Monitoraggio</p> <p>ATTIVITA': Definizione degli oggetti da sottoporre a monitoraggio; vengono individuati in collaborazione con Direzione e reparti coinvolti</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Configurazione</p> <p>ATTIVITA': Configurazione del monitoraggio; si configura il sistema di monitoraggio per inserire i nuovi oggetti</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Reportistica disponibilità</p> <p>ATTIVITA': Produzione della reportistica di disponibilità dei servizi e dell'infrastruttura; acquisizione delle reportistiche prodotte dai sistemi di monitoraggio</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>RISCHIO: possibile alterazione dei report di diponibilità da parte del personale dell'ufficio in modo da coprire inadempienze contrattuali dei fornitori del servizio di conduzione</p> <p>Verifica</p> <p>ATTIVITA': Verifica degli allarmi generati dalle sonde di monitoraggio o delle segnalazioni presenti nelle reportistiche</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Contromisure</p> <p>ATTIVITA': Individuazione ed applicazione delle contromisure in caso di livelli di disponibilità inaccettabili</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>3) Gestione degli incidenti</p> <p>Rilevazione</p> <p>ATTIVITA': Rilevazione dell'incidente: rilevazione incidente o dall'analisi dei file di log, o da segnalazioni automatiche degli applicativi o da segnalazioni degli utenti</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Informativa e contromisure temporanee</p> <p>ATTIVITA': Attivazione contromisure temporanee o attivazione del Disaster Recovery; comunicazione agli stakeholder: A fronte dell'evento si eseguono le attività necessarie per almeno una sua risoluzione temporanea. Si da avviso agli utenti interni ed eventualmente esterni del problema</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Risoluzione</p> <p>ATTIVITA': Risoluzione dell'incidente: viene realizzata l'eventuale soluzione definitiva di risoluzione del problema</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>4) Gestione dei Problemi</p> <p>Rilevazione</p> <p>ATTIVITA': Individuazione problemi a sistemi e/o servizi IT: Rilevazione del problema o dall'analisi dei file di log, o da segnalazioni automatiche degli applicativi o da segnalazioni degli utenti</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Analisi cause</p> <p>ATTIVITA': Analisi delle cause tramite ispezione dei log, analisi dei dati, verifiche di raggiungibilità dei servizi, etc.</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Proposte cambiamenti</p> <p>ATTIVITA': Proposte cambiamenti per risolvere i problemi o escalation verso i gruppi di competenza. Individuazione e definizione delle soluzioni possibili e attuabili per risolvere il problema</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>5) Amministrazione dei sistemi</p> <p>Monitoraggio</p> <p>ATTIVITA': Monitoraggio continuativo degli eventi di sistema, inclusa la corretta esecuzione dei job schedulati, e interventi di manutenzione dei sistemi. Il monitoraggio è automatizzato e produce: log invio mail al personale incaricato. Solitamente sono gli amministratori di sistema.</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>6) Gestione delle Richieste degli utenti</p> <p>Presa in carico</p> <p>ATTIVITA': Presa in carico e tracciatura delle richieste di assistenza tecnica degli utenti interni ed esterni (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti)</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Risoluzione</p> <p>ATTIVITA': Gestione e risoluzione delle richieste degli utenti interni</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>ATTIVITA': Gestione e risoluzione delle richieste degli utenti esterni</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>7) Gestione e condivisione della conoscenza</p> <p>ATTIVITA': Organizzazione e aggiornamento del sistema di condivisione della conoscenza, contenente soluzioni per problemi noti, procedure di installazione, configurazione e manutenzione, descrizione di procedure operative, etc. Nella registrazione del problema viene aggiunta la sua risoluzione</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>8) Gestione strumenti produttività individuale (stampanti, PC, scanner, portatili)</p> <p>Distribuzione conoscenza</p> <p>ATTIVITA': Definizione regole di distribuzione. Le procedure vengono condivise periodicamente tra il personale della stessa articolazione</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>Gestione risorse</p> <p>ATTIVITA': Assegnazione delle risorse in base alle regole stabilite, alle disponibilità dei materiali e l'effettiva necessità degli strumenti</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>ATTIVITA': Tracciatura delle risorse assegnate. L'utilizzo delle risorse assegnate è tracciato nei log</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>ATTIVITA': Rimozione, eventuale riallocazione risorse non più necessarie e gestione del fuori uso: fronte del riscontro del non più utilizzo di una o più risorse le stesse vengono tolte ed eventualmente riassegnate</p> <p>FASE: Pulizia</p> <p>ATTIVITA': Pulizia dati su dispositivi: Tutti i beni informatici da rottamare o donare prevedono la cancellazione dei dati, ticket a TBS, vedi PG relativa</p> <p>RESPONSABILITA': Dirigente Sistemi Informativi</p>	<p>4.1) Definizione dei requisiti di disponibilità: Definizione, per ciascun servizio, delle finestre di disponibilità verso l'esterno o derivarli da vincoli normativi/regolamentari/tecnici o da requisiti provenienti dagli uffici</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
		<p>4.2) Monitoraggio della disponibilità dei servizi: Individuazione oggetti da monitorare Configurazione del monitoraggio Produzione della reportistica di disponibilità dei servizi e dell'infrastruttura Verifica degli allarmi generati dalle sonde di monitoraggio Individuazione ed applicazione delle contromisure in caso di livelli di disponibilità inaccettabili</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
		<p>4.3) Gestione degli incidenti: Rilevazione dell'incidente Attivazione contromisure temporanee o attivazione del Disaster Recovery; comunicazione agli stakeholder Risoluzione dell'incidente</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
		<p>4.4) Gestione dei Problemi: Individuazione problemi a sistemi e/o servizi IT, rilevati in autonomia o su richiesta da parte di utenti/personale degli uffici Analisi delle cause tramite ispezione dei log, analisi dei dati, verifiche di raggiungibilità dei servizi, etc. Proposte cambiamenti per risolvere i problemi o escalation verso i gruppi di competenza</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
		<p>4.5) Amministrazione dei sistemi: Monitoraggio continuativo degli eventi di sistema, inclusa la corretta esecuzione dei job schedulati, e interventi di manutenzione dei sistemi</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
		<p>4.6) Gestione delle Richieste degli utenti (Presa in carico e tracciatura delle richieste di assistenza tecnica degli utenti interni ed esterni; attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti) Presa in carico e tracciatura delle richieste di assistenza tecnica degli utenti interni ed esterni (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti) Gestione e risoluzione delle richieste degli utenti interni Gestione e risoluzione delle richieste degli utenti esterni</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
		<p>4.7) Gestione e condivisione della conoscenza Organizzazione e aggiornamento del sistema di condivisione della conoscenza, contenente soluzioni per problemi noti, procedure di installazione, configurazione e manutenzione, descrizione di procedure operative, etc.</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
		<p>4.8) Gestione strumenti produttività individuale (stampanti, PC, scanner, portatili) Le procedure vengono condivise periodicamente tra il personale della stessa articolazione Assegnazione delle risorse in base alle regole stabilite, alle disponibilità dei materiali e l'effettiva necessità degli strumenti L'utilizzo delle risorse assegnate è tracciato nei log A fronte del riscontro del non più utilizzo di una o più risorse le stesse vengono tolte ed eventualmente riassegnate</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi

Controlli verifiche, ispezioni e sanzioni	Estrazione dati	<p>Gestione delle richieste di estrazione dati presenti nelle basi dati aziendali di competenza dei Sistemi Informativi, quando non previste con gli strumenti applicativi a disposizione degli utenti</p> <p>Responsabilità complessiva: Dirigente Sistemi Informativi</p> <p>1) Gestione richieste specifiche di estrazione dati presentate da uffici IZSLER, Altre PA Ricezione Richieste ATTIVITA': Ricezione, tracciamento delle richieste ed analisi delle richieste. Ricezione richiesta, sua registrazione. La richiesta deve essere fatta dal dirigente responsabile di struttura complessa o semplice se in staff. Autorizzata dal Direttore Amministrativo o Sanitario per le aree di propria competenza RESPONSABILITA': Dirigente Sistemi Informativi Analisi ATTIVITA': analisi delle richieste. Definizione dei criteri di estrazione con l'ausilio del personale di reparto coinvolto RESPONSABILITA': Dirigente Sistemi Informativi Evasione richieste ATTIVITA': Predisposizione degli strumenti di selezione ed estrazione dati a fronte delle richieste presentate. Esecuzione delle query di estrazione definite o di eventuali procedure realizzate ad hoc RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>2) Gestione delle richieste di accesso e scambio dati presenti nelle banche dati di IZSLER da parte di altre Pubbliche Amministrazioni Ricezione Richieste ATTIVITA': Ricezione, tracciamento ed Analisi delle richieste. Ricezione richiesta, sua registrazione. La richiesta deve essere autorizzata dal Direttore Amministrativo o Sanitario per le aree di propria competenza RESPONSABILITA': Dirigente Sistemi Informativi Definizione protocolli ATTIVITA': Definizione dei protocolli di intesa in linea con la normativa vigente. Definizione dei criteri di estrazione con l'ausilio del personale di reparto coinvolto RESPONSABILITA': Dirigente Sistemi Informativi Progettazione e realizzazione ATTIVITA': Progettazione e realizzazione di soluzioni per lo scambio dati inclusi eventuali servizi di cooperazione applicativa. Esecuzione delle query di estrazione definite o di eventuali procedure realizzate RESPONSABILITA': Dirigente Sistemi Informativi</p>	<p>5.1) Gestione richieste specifiche di estrazione dati presentate da uffici IZSLER, Altre PA; Ricezione, tracciamento delle richieste Analisi delle richieste Predisposizione degli strumenti di selezione ed estrazione dati a fronte delle richieste presentate</p>	<p>Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi</p>
Controlli verifiche, ispezioni e sanzioni	Gestione dei Cambiamenti: Gestione di tutti i cambiamenti all'infrastruttura e alle implementazioni di software nuovi (o di upgrade) con hardware e documentazione associati, negli ambienti di rilascio, pre-esercizio, esercizio, con lo scopo di minimizzare l'impatto di possibili incidenti correlati sui servizi IT, valutando l'impatto, costi, benefici e rischi dei cambiamenti proposti, gestendo e coordinando l'implementazione delle RFC, etc.	<p>Responsabilità complessiva: Dirigente Sistemi Informativi</p> <p>1) Definizione e revisione delle procedure di Change infrastrutturali / Rilascio di nuovi applicativi o aggiornamenti Definizione ATTIVITA': Definizione e revisione delle procedure di Change/Rilascio di nuovi applicativi. Si segue la procedura indicata nella PG00/076. Se non più adeguata in accordo con la Qualità si provvede ad una sua variazione. RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>2) Ciclo di vita dei change infrastrutturali /Rilascio di nuovi applicativi o aggiornamenti Esecuzione ATTIVITA': Acquisizione delle richieste. Apertura delle richieste di change standard/non standard RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Piano di rilascio delle nuove funzionalità o procedura. Per change non standard o per rilascio di nuove applicazioni: progettazione e pianificazione delle attività RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Valutazione degli impatti del change: valutazione se ci sono impatti pesanti o meno sull'infrastruttura RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Per change non standard o rilascio di nuovi applicativi: approvazione del piano di rilascio RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Esecuzione dei Change/Rilasci. Aggiornamento delle procedure e dei sistemi eventualmente coinvolti RESPONSABILITA': Dirigente Sistemi Informativi Gestione ATTIVITA': Eventuale ripristino (rollback) delle versioni/configurazioni precedenti in caso di anomalie (aggiornamento non andato a buon fine) RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Aggiornamento del database delle configurazioni RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Chiusura dei change e controllo post implementazione RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>3) Ciclo di vita dei change in caso di emergenza Richiesta ATTIVITA': Richiesta di change in caso di emergenza, ad esempio in caso di necessità di applicare contromisure urgenti per casi di incidente (isolamento di parte dei servizi, inserimento di pagine di cortesia, modifiche di configurazione, etc.) RESPONSABILITA': Dirigente Sistemi Informativi Approvazione ATTIVITA': Valutazione impatto e correttezza azioni correttive. Approvazione del change RESPONSABILITA': Dirigente Sistemi Informativi Implementazione delle contromisure adeguate (Firewall, etc.) ATTIVITA': Implementazione del change: esecuzione delle azioni correttive RESPONSABILITA': Dirigente Sistemi Informativi Ripristino ATTIVITA': Eventuale ripristino delle configurazioni originali ad emergenza terminata</p>	<p>6.1) Definizione e revisione delle procedure di Change infrastrutturali / Rilascio di nuovi applicativi o aggiornamenti: Definizione e revisione delle procedure di Change/Rilascio di nuovi applicativi</p> <p>6.2) Ciclo di vita dei change infrastrutturali /Rilascio di nuovi applicativi o aggiornamenti: Apertura delle richieste di change standard/non standard Per change non standard o per rilascio di nuove applicazioni: progettazione e pianificazione delle attività Valutazione degli impatti del change Per change non standard o rilascio di nuovi applicativi: approvazione Esecuzione dei Change/Rilasci Eventuale ripristino (rollback) delle versioni/configurazioni precedenti in caso di anomalie Aggiornamento del database delle configurazioni (CMDB) Chiusura dei change e controllo post implementazione</p> <p>6.3) Ciclo di vita dei change in caso di emergenza: Ricezione della richiesta e sua valutazione. Definizione azioni correttive Valutazione impatto e correttezza azioni correttive Implementazione delle contromisure adeguate (Firewall, etc.) Eventuale ripristino delle configurazioni originali ad emergenza terminata</p>	<p>Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi</p> <p>Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi</p> <p>Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi</p>

Controlli verifiche, ispezioni e sanzioni	Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT  Responsabilità complessiva: Dirigente Sistemi Informativi  1) Predisposizione dei capitolati di gara per lo sviluppo di servizi/applicazioni IT Predisposizione specifiche, vincoli, ... ATTIVITA': Predisposizione del capitolato tecnico. Il capitolato tecnico deve essere steso rispettando le esigenze raccolte nella fase precedente, avallato dal dirigente responsabile della struttura complessa, semplice o in staff richiedente. RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Supporto all'ufficio competente per la predisposizione della documentazione di gara. Fornire eventuali chiarimenti in ambito tecnico RESPONSABILITA': Dirigente Sistemi Informativi  2) Valutazione offerte tecniche Valutazione ATTIVITA': Partecipazione alla commissioni di gara e/valutazioni offerte tecniche- La valutazione è effettuata dalla commissione di gara nominata dal Direttore Generale su proposta del dirigente responsabile dell'U.O. Provveditorato e Vendite. RESPONSABILITA': Dirigente Sistemi Informativi  3) Gestione rapporti con il fornitore ai fini dell'esecuzione delle attività oggetto di intervento. Stati avanzamenti dei lavori sui singoli progetti e complessivo Supporto ATTIVITA': Supporto esecuzione attività RESPONSABILITA': Dirigente Sistemi Informativi  4) Verifica periodica esecuzione attività contrattualizzate Esecuzione ATTIVITA': Esecuzione dei test dei servizi/applicazioni da realizzare. Una procedura prima di essere messa in produzione deve essere collaudata. Il collaudo deve avvenire da parte dell'utilizzatore. RESPONSABILITA': Dirigente Sistemi Informativi Monitoraggio ATTIVITA': Monitoraggio dell'andamento dei costi in relazione al budget allocato per le attività di sviluppo IT. Tenere traccia di ogni aumento della spesa, che dovrebbe essere avallato preventivamente dalla Direzione Dirigente e Collaboratore RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Attività connesse alla Regolare Esecuzione della prestazione o relativa contestazione. RESPONSABILITA': Dirigente Sistemi Informativi	Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	7.1) Predisposizione dei capitolati di gara per lo sviluppo di servizi/applicazioni IT: Predisposizione del capitolato tecnico Supporto all'ufficio competente per la predisposizione della documentazione di gara 7.2) Valutazione offerte tecniche: Partecipazione alla commissioni di gara e/valutazioni offerte tecniche 7.3) Verifica delle modalità di esecuzione del contratto e dei livelli di servizio ed eventuale applicazione di penali: Esecuzione dei test dei servizi/applicazioni da realizzare Monitoraggio dell'andamento dei costi in relazione al budget allocato per le attività di sviluppo IT Attività connesse alla Regolare Esecuzione della prestazione o relativa contestazione 7.4) Rilascio certificato di conformità/regolare esecuzione	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Gestione della Sicurezza delle Informazioni. Allineare la sicurezza delle informazioni alla sicurezza attesa dal business ed assicurarsi che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi, per quanto riguarda le proprietà di disponibilità, integrità, confidenzialità e autenticità delle informazioni  Responsabilità complessiva: Dirigente Sistemi Informativi  1) Gestione dei backup/restore dei dati Definizione strategie ATTIVITA': Definizione delle strategie di backup (giornaliero, settimanale, full, incrementale, etc.) per ciascuno dei sistemi IT (database, server, filesystem, etc.). All'avvio di una nuova procedura viene attivata la procedura di salvataggio dati descritta nella PG00/070. RESPONSABILITA': Dirigenti Sistemi Informativi Pianificazione ATTIVITA': Pianificazione dei backup: le procedure di backup vengono attivate sul singolo db/server RESPONSABILITA': Dirigenti Sistemi Informativi Monitoraggio ATTIVITA': Controllo e monitoraggio dell'esecuzione dei backup: giornalmente vengono verificati i log prodotti dalle procedure di salvataggio RESPONSABILITA': Dirigenti Sistemi Informativi Restore ATTIVITA': Esecuzione Restore su richiesta. Tracciabilità e valutazione dell'autorizzazione di tutte le richieste di restore RESPONSABILITA': Dirigenti Sistemi Informativi  2) Gestione dei permessi per gli utenti Ricezione richieste ATTIVITA': Acquisizione richiesta permessi. RESPONSABILITA': Dirigenti Sistemi Informativi ATTIVITA': Approvazione richiesta, previo verifica requisiti. Le richieste devono essere effettuate dal dirigente di struttura complessa o semplice se si tratta di struttura in staff. La richiesta viene registrata. La richiesta se proviene dal dirigente di struttura complessa o semplice se si tratta di struttura in staff, se non va contro le regole aziendali viene autorizzata. Nei casi dubbi viene richiesta l'autorizzazione del Direttore Amministrativo o Sanitario. RESPONSABILITA': Dirigenti Sistemi Informativi Attribuzione permessi. Viene realizzata la modifica nei permessi del singolo o del gruppo coinvolto ATTIVITA': Attribuzione permessi Rimozione permessi ATTIVITA': Rimozione permessi non più necessari su evento (es. cambio ufficio, cessazione del rapporto di lavoro, etc.) o, periodicamente, su assessment RESPONSABILITA': Dirigenti Sistemi Informativi  3) SOTTOPROCESSO Gestione della sicurezza di rete Definizione ATTIVITA': Definizione dei requisiti di sicurezza di rete. Linee di sicurezza ICT pubblicate dall'AgID RESPONSABILITA': Dirigenti Sistemi Informativi Contromisure ATTIVITA': Implementazione delle contromisure adeguate (Firewall, etc.). Gli accessi "particolari" a livello di perimetro esterno vengono realizzati dalla infrastruttura attraverso il supporto di una ditta esterna (a volte) a seconda della complessità Ogni modifica della configurazione viene automaticamente registrata e salvata RESPONSABILITA': Dirigenti Sistemi Informativi Gestione richieste ATTIVITA': Gestione delle richieste interne/esterne di collegamento a sistemi/servizi; ad es. VPN, FirewallXML, etc. Gli accessi "particolari" a livello di perimetro esterno vengono realizzati dalla infrastruttura attraverso il supporto di una ditta esterna (a volte) a seconda della complessità Ogni modifica della configurazione viene automaticamente registrata e salvata RESPONSABILITA': Dirigenti Sistemi Informativi Analisi eventi sicurezza ATTIVITA': Analisi degli eventi di sicurezza di rete. Gli eventi vengono raccolti in report quotidiani, host-monitor e Firewall e DHCP log amministratori; si deve formalizzare il controllo su più livelli RESPONSABILITA': Dirigenti Sistemi Informativi  4) SOTTOPROCESSO Prevenzione, rilevazione e rimozione di software malevoli Configurazione ATTIVITA': Configurazione sistemi antivirus su postazioni di lavoro e server. Le procedure di installazione sia delle postazioni di lavoro sia dei server prevedono l'installazione e l'aggiornamento dell'antivirus RESPONSABILITA': Dirigenti Sistemi Informativi Monitoraggio ATTIVITA': Monitoraggio delle attività Antivirus e della diffusione di software malevoli. La console centrale dell'antivirus permette agli operatori di verificare eventuali situazioni anomale RESPONSABILITA': Dirigenti Sistemi Informativi Risoluzione di problemi ATTIVITA': Risoluzione di problemi legati a presenza di software malevoli, sensibilizzazione degli utenti  5) Gestione degli incidenti di sicurezza Rilevazione dell'incidente ATTIVITA': Rilevazione dell'incidente. Gli eventi vengono raccolti in report quotidiani, host-monitor e Firewall e DHCP log amministratori; si deve formalizzare il controllo su più livelli. Bisogna formalizzare la procedura di escalation per la gestione dell'incidente RESPONSABILITA': Dirigenti Sistemi Informativi Comunicazione e contromisure temporanee ATTIVITA': Attivazione contromisure temporanee; comunicazione agli stakeholder RESPONSABILITA': Dirigenti Sistemi Informativi Risoluzione ATTIVITA': Risoluzione dell'incidente e adozione contromisure. Viene ripristinata la situazione di normale operatività. Se necessario vengono implementate ulteriori contromisure RESPONSABILITA': Dirigenti Sistemi Informativi  6) Gestione dell'audit su sistemi e dati Gestione audit ATTIVITA': Configurazione, analisi e archiviazione dei dati di audit relativi all'utilizzo dei sistemi (database, filesystem, applicazioni)	Gestione della Sicurezza delle Informazioni. Allineare la sicurezza delle informazioni alla sicurezza attesa dal business ed assicurarsi che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi, per quanto riguarda le proprietà di disponibilità, integrità, confidenzialità e autenticità delle informazioni  Responsabilità complessiva: Dirigente Sistemi Informativi  1) Gestione dei backup/restore dei dati Definizione strategie ATTIVITA': Definizione delle strategie di backup (giornaliero, settimanale, full, incrementale, etc.) per ciascuno dei sistemi IT (database, server, filesystem, etc.). All'avvio di una nuova procedura viene attivata la procedura di salvataggio dati descritta nella PG00/070. RESPONSABILITA': Dirigenti Sistemi Informativi Pianificazione ATTIVITA': Pianificazione dei backup: le procedure di backup vengono attivate sul singolo db/server RESPONSABILITA': Dirigenti Sistemi Informativi Monitoraggio ATTIVITA': Controllo e monitoraggio dell'esecuzione dei backup: giornalmente vengono verificati i log prodotti dalle procedure di salvataggio RESPONSABILITA': Dirigenti Sistemi Informativi Restore ATTIVITA': Esecuzione Restore su richiesta. Tracciabilità e valutazione dell'autorizzazione di tutte le richieste di restore RESPONSABILITA': Dirigenti Sistemi Informativi  2) Gestione dei permessi per gli utenti Ricezione richieste ATTIVITA': Acquisizione richiesta permessi. RESPONSABILITA': Dirigenti Sistemi Informativi ATTIVITA': Approvazione richiesta, previo verifica requisiti. Le richieste devono essere effettuate dal dirigente di struttura complessa o semplice se si tratta di struttura in staff. La richiesta viene registrata. La richiesta se proviene dal dirigente di struttura complessa o semplice se si tratta di struttura in staff, se non va contro le regole aziendali viene autorizzata. Nei casi dubbi viene richiesta l'autorizzazione del Direttore Amministrativo o Sanitario. RESPONSABILITA': Dirigenti Sistemi Informativi Attribuzione permessi. Viene realizzata la modifica nei permessi del singolo o del gruppo coinvolto ATTIVITA': Attribuzione permessi Rimozione permessi ATTIVITA': Rimozione permessi non più necessari su evento (es. cambio ufficio, cessazione del rapporto di lavoro, etc.) o, periodicamente, su assessment RESPONSABILITA': Dirigenti Sistemi Informativi  3) SOTTOPROCESSO Gestione della sicurezza di rete Definizione ATTIVITA': Definizione dei requisiti di sicurezza di rete. Linee di sicurezza ICT pubblicate dall'AgID RESPONSABILITA': Dirigenti Sistemi Informativi Contromisure ATTIVITA': Implementazione delle contromisure adeguate (Firewall, etc.). Gli accessi "particolari" a livello di perimetro esterno vengono realizzati dalla infrastruttura attraverso il supporto di una ditta esterna (a volte) a seconda della complessità Ogni modifica della configurazione viene automaticamente registrata e salvata RESPONSABILITA': Dirigenti Sistemi Informativi Gestione richieste ATTIVITA': Gestione delle richieste interne/esterne di collegamento a sistemi/servizi; ad es. VPN, FirewallXML, etc. Gli accessi "particolari" a livello di perimetro esterno vengono realizzati dalla infrastruttura attraverso il supporto di una ditta esterna (a volte) a seconda della complessità Ogni modifica della configurazione viene automaticamente registrata e salvata RESPONSABILITA': Dirigenti Sistemi Informativi Analisi eventi sicurezza ATTIVITA': Analisi degli eventi di sicurezza di rete. Gli eventi vengono raccolti in report quotidiani, host-monitor e Firewall e DHCP log amministratori; si deve formalizzare il controllo su più livelli RESPONSABILITA': Dirigenti Sistemi Informativi  4) SOTTOPROCESSO Prevenzione, rilevazione e rimozione di software malevoli Configurazione ATTIVITA': Configurazione sistemi antivirus su postazioni di lavoro e server. Le procedure di installazione sia delle postazioni di lavoro sia dei server prevedono l'installazione e l'aggiornamento dell'antivirus RESPONSABILITA': Dirigenti Sistemi Informativi Monitoraggio ATTIVITA': Monitoraggio delle attività Antivirus e della diffusione di software malevoli. La console centrale dell'antivirus permette agli operatori di verificare eventuali situazioni anomale RESPONSABILITA': Dirigenti Sistemi Informativi Risoluzione di problemi ATTIVITA': Risoluzione di problemi legati a presenza di software malevoli, sensibilizzazione degli utenti  5) Gestione degli incidenti di sicurezza Rilevazione dell'incidente ATTIVITA': Rilevazione dell'incidente. Gli eventi vengono raccolti in report quotidiani, host-monitor e Firewall e DHCP log amministratori; si deve formalizzare il controllo su più livelli. Bisogna formalizzare la procedura di escalation per la gestione dell'incidente RESPONSABILITA': Dirigenti Sistemi Informativi Comunicazione e contromisure temporanee ATTIVITA': Attivazione contromisure temporanee; comunicazione agli stakeholder RESPONSABILITA': Dirigenti Sistemi Informativi Risoluzione ATTIVITA': Risoluzione dell'incidente e adozione contromisure. Viene ripristinata la situazione di normale operatività. Se necessario vengono implementate ulteriori contromisure RESPONSABILITA': Dirigenti Sistemi Informativi  6) Gestione dell'audit su sistemi e dati Gestione audit ATTIVITA': Configurazione, analisi e archiviazione dei dati di audit relativi all'utilizzo dei sistemi (database, filesystem, applicazioni)	8.1) Gestione dei backup/restore dei dati: Definizione delle strategie di backup (giornaliero, settimanale, full, incrementale, etc.) per ciascuno dei sistemi IT (database, server, filesystem, etc.) Pianificazione dei backup Controllo e monitoraggio dell'esecuzione dei backup Esecuzione Restore su richiesta 8.2) Gestione dei permessi per gli utenti: Acquisizione richiesta permessi Approvazione richiesta, previo verifica requisiti Attribuzione permessi Rimozione permessi non più necessari su evento (es. cambio ufficio, cessazione del rapporto di lavoro, etc.) o, periodicamente, su assessment 8.3) Gestione della sicurezza di rete: Definizione dei requisiti di sicurezza di rete Implementazione delle contromisure adeguate (Firewall, etc.) Gestione delle richieste interne/esterne di collegamento a sistemi/servizi; ad es. VPN, FirewallXML, etc. Analisi degli eventi di sicurezza di rete 8.4) Prevenzione, rilevazione e rimozione di software malevoli: Configurazione sistemi antivirus su postazioni di lavoro e server Monitoraggio delle attività Antivirus e della diffusione di software malevoli Risoluzione di problemi legati a presenza di software malevoli, sensibilizzazione degli utenti 8.5) Gestione degli incidenti di sicurezza: Rilevazione dell'incidente Attivazione contromisure temporanee; comunicazione agli stakeholder Risoluzione dell'incidente e adozione contromisure 8.6) Gestione dell'audit su sistemi e dati: Configurazione, analisi e archiviazione dei dati di audit relativi all'utilizzo dei sistemi (database, filesystem, applicazioni)	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi

Controlli verifiche, ispezioni e sanzioni	Gestione delle attività volte ad assicurare la sicurezza delle informazioni e la tutela della privacy	<p>Ricognizione normativa applicabile in materia di sicurezza delle informazioni e tutela Privacy</p> <p>Responsabilità complessiva: Dirigente Sistemi Informativi</p> <p>1) Ricognizione normativa applicabile in materia di sicurezza e tutela privacy per i sistemi in gestione ai Sistemi Informativi Gestione ATTIVITA': Gestione adempimenti ai fini delle valutazioni di impatto della normativa vigente sui dati e le informazioni trattate da IZSLER. Gruppo inter reparto coordinata dal responsabile Sistemi Informativi, verificare impatto dei singoli punti RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>2) Applicazione della normativa sicurezza/privacy al contesto delle informazioni e dei trattamenti di dati personali effettuati da IZSLER Verifica ATTIVITA': Verifica della conformità di IZSLER alle previsioni del codice Privacy e CAD. Gruppo di lavoro verificare applicazione dei singoli punti RESPONSABILITA': Dirigente Sistemi Informativi Identificazione interventi - ATTIVITA': Identificazione del piano degli interventi di adeguamento normativo e supporto agli uffici interni ai fini del rispetto delle prescrizioni del Codice Privacy. Gruppo di lavoro verificare applicazione dei singoli punti RESPONSABILITA': Dirigente Sistemi Informativi Supporto - ATTIVITA': Supporto agli uffici nell'attuazione degli interventi necessari per l'adeguamento alla disciplina Privacy e la sicurezza delle informazioni RESPONSABILITA': Dirigente Sistemi Informativi</p>	<p>9.1) Ricognizione normativa applicabile in materia di sicurezza e tutela privacy per i sistemi in gestione ai Sistemi Informativi: Gestione ATTIVITA': Gestione adempimenti ai fini delle valutazioni di impatto della normativa vigente sui dati e le informazioni trattate da IZSLER. Gruppo inter reparto coordinata dal responsabile Sistemi Informativi, verificare impatto dei singoli punti</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	IT Service Continuity Management: supportare il processo di Business Continuity Management assicurando che i servizi IT possano essere ripristinati in tempi e modi predeterminati. Fa parte di questo processo il governo delle procedure e delle infrastrutture di Disaster Recovery	<p>IT Service Continuity Management: supportare il processo di Business Continuity Management assicurando che i servizi IT possano essere ripristinati in tempi e modi predeterminati. Fa parte di questo processo il governo delle procedure e delle infrastrutture di Disaster Recovery</p> <p>Responsabilità complessiva: Dirigente Sistemi Informativi</p> <p>1) Definizione delle risorse critiche ATTIVITA': Definizione delle risorse critiche (applicazioni, servizi, etc.) da sottoporre al piano di business continuity/disaster recovery. In collaborazione con la Direzione e il RAQ vengono definite le risorse critiche RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>2) SOTTOPROCESSO Redazione e mantenimento del piano di IT business continuity Redazione dei piani ATTIVITA': Redazione del piano di IT business continuity / disaster recovery (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti). Il piano viene redatto sulla base delle indicazioni ricevute e concordate con la Direzione per realizzare e garantire i tempi di ripristino del servizio RESPONSABILITA': Dirigente Sistemi Informativi Mantenimento del piano di IT business continuity ATTIVITA': Mantenimento del piano di IT business continuity (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti). Il piano viene modificato sulla base delle indicazioni ricevute e concordate con la Direzione per realizzare e garantire i tempi di ripristino del servizio RESPONSABILITA': Dirigente Sistemi Informativi</p> <p>3) SOTTOPROCESSO Test del piano di Disaster Recovery Test di DR ATTIVITA': Schedulazione del test di Disaster Recovery RESPONSABILITA': Dirigente Sistemi Informativi ATTIVITA': Esecuzione del test di Disaster Recovery RESPONSABILITA': Dirigente Sistemi Informativi Verifica dei risultati del test di Disaster Recovery ATTIVITA': Verifica dei risultati del test di Disaster Recovery RESPONSABILITA': Dirigente Sistemi Informativi</p>	<p>10.1) Definizione delle risorse critiche Definizione delle risorse critiche (applicazioni, servizi, etc.) da sottoporre al piano di business continuity/disaster recovery</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
			<p>10.2) Redazione e mantenimento del piano di IT business continuity: Redazione del piano di IT business continuity / disaster recovery (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti) Mantenimento del piano di IT business continuity (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti)</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi
			<p>10.3) Test del piano di Disaster Recovery: Schedulazione del test di Disaster Recovery Esecuzione del test di Disaster Recovery Verifica dei risultati del test di Disaster Recovery</p>	Programmazione dei servizi tecnici e controllo di gestione-Sistemi Informativi

**IDENTIFICAZIONE DEI RISCHI**

AREA DI RISCHIO	PROCESSO	FASE/ATTIVITA'	EVENTO RISCHIOSO	FATTORE ABILITANTE DEL RISCHIO CORRUTTIVO
Acquisizione e gestione del personale	Gestione del ciclo delle performance	adozione del Piano Performance	NESSUNO	NESSUNO
		individuazione degli obiettivi operativi, indicatori e target	individuazione degli obiettivi al fine di favorire determinati dirigenti o strutture	Conflitto di interessi Inosservanza delle regole procedurali a garanzia della trasparenza e dell'imparzialità
		adozione dell'Albero delle Performance	NESSUNO	NESSUNO
		acquisizione dei report sul raggiungimento degli obiettivi rispetto ai target ed agli indicatori	NESSUNO	NESSUNO
		approvazione Relazione sulla Performance	NESSUNO	NESSUNO
		pubblicazione nella sezione Amministrazione Trasparente del sito web della Relazione sulla Performance	NESSUNO	NESSUNO
		acquisizione delle rendicontazioni di ciascuna struttura sul raggiungimento degli obiettivi	NESSUNO	NESSUNO
		verifica requisiti per erogazione trattamento economico al personale dipendente	Verifiche non corrette al fine di favorire specifici dipendenti	Conflitto di interessi. Inadeguata diffusione cultura della legalità
		determinazione del trattamento economico erogazione del trattamento economico al personale dell'IZSLER	NESSUNO	NESSUNO
Gestione delle entrate, delle spese e del patrimonio	Valorizzazione delle prove di laboratorio	Assegnazione dalla valorizzazione della prova di laboratorio al Dirigente valorizzatore preposto da parte del Dirigente gestore del nomenclatore	Nessun evento rischioso	
		Valorizzazione della prova e invio per la validazione al Dirigente validatore preposto	Alterazione dei valori dei fattori produttivi finalizzata a determinare una tariffa o prezzo di vendita diverso dall'effettivo	Inosservanza della regolamentazione interna (Linee guida valorizzazione analisi/prodotti)
		Verifica della valorizzazione, validazione e comunicazione all'ufficio controllo di gestione e performance	Alterazione dei valori dei fattori produttivi finalizzata a determinare una tariffa o prezzo di vendita diverso dall'effettivo	Inosservanza della regolamentazione interna (Linee guida valorizzazione analisi/prodotti)
		Determinazione della tariffa della prova di laboratorio da parte dell' ufficio controllo di gestione e performance sulla base della valorizzazione validata e predisporre il relativo provvedimento di aggiornamento del tariffario	Nessun evento rischioso	
		Aggiornamento del tariffario da parte dell'ufficio controllo di gestione e performance, dopo l'approvazione da parte del Direttore Generale, pubblicato sul sito istituzionale	Nessun evento rischioso	

Gestione delle entrate, delle spese e del patrimonio	Valorizzazione dei prodotti / prezzo di vendita dei prodotti (tariffazione)	Assegnazione del la valorizzazione del prodotto al Dirigente valorizzatore proposto da parte del Dirigente gestore del magazzino prodotti	Nessun evento rischioso	
		Valorizzazione del prodotto e invio per la validazione al Dirigente validatore preposto	Alterazione dei valori dei fattori produttivi finalizzata a determinare un prezzo di vendita diverso dall'effettivo	Inosservanza della regolamentazione interna (Linee guida valorizzazione analisi/prodotti)
		Verifica della valorizzazione, validazione e comunicazione all'ufficio controllo di gestione e performance e performance	Nessun evento rischioso	
		Proposta del prezzo di vendita da parte del Dirigente valorizzatore	Non corretta determinazione dei prezzi al fine di favorire determinati soggetti	Inosservanza della regolamentazione interna (Linee guida valorizzazione analisi/prodotti)
		Verifica di Congruità del prezzo proposto rispetto alla valorizzazione del prodotto da parte del Direttore Sanitario con l'ufficio controllo di gestione e performance	Nessun evento rischioso	
		Conferma del prezzo di vendita proposto da parte del Direttore Sanitario	Nessun evento rischioso	
		Aggiornamento del catalogo dei prodotti venduti da parte dell'U.O. Provveditorato Economato e Vendite	Nessun evento rischioso	
Gestione delle entrate, delle spese e del patrimonio	Controllo richieste di nota di variazione di fatture emesse	Ricezione da parte dell'ufficio controllo di gestione e performance dall'U.O. Gestione Servizi Contabili delle richieste di emissione di note di variazione	Nessun evento rischioso	
		L'ufficio controllo di gestione e performance effettua un controllo di corrispondenza fra i dati presenti nel software sanitario e quanto indicato nelle richieste di nota di variazione da emettere. Se il controllo è positivo l'ufficio controllo di gestione e performance comunica l'esito al U.O. Gestione Servizi Contabili che procederà ed emettere la nota di variazione, in caso negativo l'ufficio controllo di gestione e performance comunica al reparto che ha emesso la richiesta di procedere con le opportune modifiche nel software sanitario	Omissione del controllo al fine di favorire determinati soggetti	Esercizio dell'attività da parte di un unico soggetto
Gestione delle attività di ricerca	Attivazione piani di monitoraggio	Invio da parte del Dirigente responsabile del piano di monitoraggio alla Direzione Generale di una richiesta di attivazione del piano di monitoraggio	Esecuzione dell'attività di monitoraggio finalizzata a favorire determinati soggetti	Mancanza di attività di controllo nell'esecuzione dei piani di monitoraggio
		Autorizzazione da parte del Direttore Generale dell'attivazione del piano e comunicazione all'ufficio controllo di gestione e performance	Nessun evento rischioso	
		Predisposizione del provvedimento di attivazione del piano e codifica il piano dei software aziendali da parte dell'ufficio controllo di gestione e performance	Nessun evento rischioso	
		Rendicontazione dell'attività svolta al Direttore Generale	Nessun evento rischioso	

Contratti pubblici - Affidamento di lavori, servizi e forniture	Definizione degli standard metodologici, documentali e architetture per la realizzazione e l'erogazione dei servizi IT	Ricognizione: Raccolta ed analisi della documentazione disponibile su Standard e Best Practice di riferimento	Nessun evento rischioso	Non rilevato
		Adozione: Predisposizione ed aggiornamento degli standard IZSLER per lo sviluppo dei servizi e predisposizione della relativa documentazione	Nessun evento rischioso	Non rilevato
Contratti pubblici - Affidamento di lavori, servizi e forniture	Definizione degli standard metodologici, documentali e architetture per la realizzazione e l'erogazione dei servizi IT	Analisi esigenze architetture dell' IT di IZSLER Raccolta ATTIVITA': Raccolta requisiti architetture necessari a supportare lo sviluppo dell'IT IZSLER. Verifica architettura esistente, stima del dimensionamento sulla base delle richieste e progetti noti e delle indicazioni di legge Formalizzazione ATTIVITA': Formalizzazione documento di analisi dei requisiti architetture necessari a supportare lo sviluppo dell'IT IZSLER	Nessun evento rischioso	Non rilevato
Contratti pubblici - Affidamento di lavori, servizi e forniture	Gestione della Capacità dei sistemi/servizi IT Comprendere i requisiti aziendali correnti e futuri, le operazioni dell'organizzazione, l'infrastruttura informatica e garantire che tutti gli aspetti relativi alle prestazioni e alle capacità siano forniti ottimizzando costi, risorse e qualità	Analisi previsionale della capacità dei sistemi Analisi ATTIVITA': Analisi dei dati provenienti dalle attività di monitoraggio relative all'occupazione di spazio storage, memoria, processori, etc. Vengono raccolti dalle console di monitoraggio dell'infrastruttura i principali key indicator sul consumo di memoria, spazio ATTIVITA': Analisi dei trend di crescita della capacità occupata e stima delle ulteriori esigenze di acquisizione di hardware/software, risorse e servizi Valutazione impatto ATTIVITA': In caso di partenza di nuovi progetti, modifiche normative che abbiano impatto su numero utenti dei servizi e/o quantità di dati acquisiti, stima della capacità aggiuntiva necessaria e analisi delle ulteriori esigenze di acquisizione di hardware/software Formalizzazione fabbisogni ATTIVITA': Formalizzazione dei fabbisogni di approvvigionamento di hardware/software, risorse e servizi. Se l'analisi dell'impatto evidenzia la necessità di un upgrade dell'infrastruttura, la stessa viene segnalata e da avvio al processo : "Gestione domanda e pianificazione servizi IT"	2.1.1) Sovrastimare le esigenze o di evidenziare la necessità di soluzioni non effettivamente necessarie in favore del fornitore al fine di ottenere vantaggi illeciti mediante accordi collusivi con lo stesso	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto

Contratti pubblici - Affidamento di lavori, servizi e forniture	Gestione della domanda e Pianificazione servizi IT	Rilevazione e consolidamento dei fabbisogni di servizi/applicazioni IT: Acquisizione, dagli uffici IZSLER, dei fabbisogni di servizi e applicazioni IT Incontri di approfondimento con le strutture al fine di dettagliare le esigenze Elaborazione della documentazione relativa alle specifiche tecniche/applicative di sviluppo dei servizi/applicazioni IT	Nessun evento rischioso	Non rilevato
Contratti pubblici - Affidamento di lavori, servizi e forniture		Definizione delle esigenze di sviluppo di servizi/applicazioni IT e quantificazione degli interventi: Formalizzazione delle esigenze di sviluppo di servizi/applicazioni e relativa quantificazione ai fini di soddisfare la domanda interna Richiesta di approvazione priorità ed interventi di sviluppo da parte della Direzione	Sovrastimare le esigenze o di evidenziare la necessità di soluzioni non effettivamente necessarie in favore del fornitore al fine di ottenere vantaggi illeciti mediante accordi collusivi con lo stesso	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto
Contratti pubblici - Affidamento di lavori, servizi e forniture		Elaborazione piano degli interventi IT: Definizione interventi IT da realizzare nel corso dell'anno Definizione del piano di realizzazione Monitoraggio e controllo dell'attuazione delle attività a piano	Sovrastimare le esigenze o di evidenziare la necessità di soluzioni non effettivamente necessarie in favore del fornitore al fine di ottenere vantaggi illeciti mediante accordi collusivi con lo stesso	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto
Controlli verifiche, ispezioni e sanzioni		Definizione dei requisiti di disponibilità: Definizione, per ciascun servizio, delle finestre di disponibilità verso l'esterno o derivarli da vincoli normativi/regolamentari/tecnici o da requisiti provenienti dagli uffici	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni		Monitoraggio della disponibilità dei servizi: Individuazione oggetti da monitorare Configurazione del monitoraggio Produzione della reportistica di disponibilità dei servizi e dell'infrastruttura Verifica degli allarmi generati dalle sonde di monitoraggio Individuazione ed applicazione delle contromisure in caso di livelli di disponibilità inaccettabili	Non far emergere errori/malfunzionamenti nelle soluzioni realizzate in favore del fornitore al fine di ottenere vantaggi illeciti mediante accordi collusivi con lo stesso o per inerzia o disinteresse verso gli obiettivi dell'Amministrazione	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto
Controlli verifiche, ispezioni e sanzioni		Gestione degli incidenti: Rilevazione dell'incidente Attivazione contromisure temporanee o attivazione del Disaster Recovery; comunicazione agli stakeholder Risoluzione dell'incidente	accessi non autorizzati a sistemi e dati di IZSLER per trarne benefici illegittimi	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto, mancato controllo

Controlli verifiche, ispezioni e sanzioni	Erogazione dei Servizi Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT. Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi	Gestione dei Problemi: Individuazione problemi a sistemi e/o servizi IT, rilevati in autonomia o su richiesta da parte di utenti/personale degli uffici Analisi delle cause tramite ispezione dei log, analisi dei dati, verifiche di raggiungibilità dei servizi, etc. Proposte cambiamenti per risolvere i problemi o escalation verso i gruppi di competenza	accessi non autorizzati a sistemi e dati di IZSLER per trarne benefici illegittimi	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto, mancato controllo
Controlli verifiche, ispezioni e sanzioni		Amministrazione dei sistemi: Monitoraggio continuativo degli eventi di sistema, inclusa la corretta esecuzione dei job schedulati, e interventi di manutenzione dei sistemi	accessi non autorizzati a sistemi e dati di IZSLER per trarne benefici illegittimi	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto, mancato controllo
Controlli verifiche, ispezioni e sanzioni		Gestione delle Richieste degli utenti (Presa in carico e tracciatura delle richieste di assistenza tecnica degli utenti interni ed esterni; attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti) Presa in carico e tracciatura delle richieste di assistenza tecnica degli utenti interni ed esterni (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti) Gestione e risoluzione delle richieste degli utenti interni Gestione e risoluzione delle richieste degli utenti esterni	Nessun evento rischioso	non rilevato
Controlli verifiche, ispezioni e sanzioni		Gestione e condivisione della conoscenza Organizzazione e aggiornamento del sistema di condivisione della conoscenza, contenente soluzioni per problemi noti, procedure di installazione, configurazione e manutenzione, descrizione di procedure operative, etc.	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni		Gestione strumenti produttività individuale (stampanti, PC, scanner, portatili) Le procedure vengono condivise periodicamente tra il personale della stessa articolazione Assegnazione delle risorse in base alle regole stabilite, alle disponibilità dei materiali e l'effettiva necessità degli strumenti L'utilizzo delle risorse assegnate è tracciato nei log A fronte del riscontro del non più utilizzo di una o più risorse le stesse vengono tolte ed eventualmente riassegnate	Assegnazione delle risorse informatiche alle strutture non in base alle reali esigenze dell'istituto ma utilizzando criteri discrezionali	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto

Controlli verifiche, ispezioni e sanzioni	Estrazione dati	Gestione richieste specifiche di estrazione dati presentate da uffici IZSLER, Altre PA; Ricezione, tracciamento delle richieste Analisi delle richieste Predisposizione degli strumenti di selezione ed estrazione dati a fronte delle richieste presentate	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni		Gestione delle richieste di accesso e scambio dati presenti nelle banche dati di IZSLER da parte di altre Pubbliche Amministrazioni: Ricezione, tracciamento ed Analisi delle richieste Definizione dei protocolli di intesa in linea con la normativa vigente Progettazione e realizzazione di soluzioni per lo scambio dati inclusi eventuali servizi di cooperazione applicativa	Modalità di estrazione dati tale da configurare accordi collusivi al fine di falsare la descrizione delle realtà	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto
Controlli verifiche, ispezioni e sanzioni	Gestione dei Cambiamenti: Gestione di tutti i cambiamenti all'infrastruttura e alle implementazioni di software nuovi (o di upgrade) con hardware e documentazione associati, negli ambienti di rilascio, pre-esercizio, esercizio, con lo scopo di minimizzare l'impatto di possibili incidenti correlati sui servizi IT, valutando l'impatto, costi, benefici e rischi dei cambiamenti proposti, gestendo e coordinando l'implementazione delle RFC, etc.	Definizione e revisione delle procedure di Change infrastrutturali / Rilascio di nuovi applicativi o aggiornamenti: Definizione e revisione delle procedure di Change/Rilascio di nuovi applicativi	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni		Ciclo di vita dei change infrastrutturali /Rilascio di nuovi applicativi o aggiornamenti: Apertura delle richieste di change standard/non standard Per change non standard o per rilascio di nuove applicazioni: progettazione e pianificazione delle attività Valutazione degli impatti del change Per change non standard o rilascio di nuovi applicativi: approvazione Esecuzione dei Change/Rilasci Eventuale ripristino (rollback) delle versioni/configurazioni precedenti in caso di anomalie Aggiornamento del database delle configurazioni (CMDB) Chiusura dei change e controllo post implementazione	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni		Ciclo di vita dei change in caso di emergenza: Ricezione della richiesta e sua valutazione. Definizione azioni correttive Valutazione impatto e correttezza azioni correttive Implementazione delle contromisure adeguate (Firewall, etc..) Eventuale ripristino delle configurazioni originali ad emergenza terminata	Nessun evento rischioso	Non rilevato

Controlli verifiche, ispezioni e sanzioni	Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	Predisposizione dei capitolati di gara per lo sviluppo di servizi/applicazioni IT: Predisposizione del capitolato tecnico Supporto all'ufficio competente per la predisposizione della documentazione di gara	Capitolato di gara predisposto con l'intento di favorire uno o più fornitori al fine di ottenere vantaggi illeciti mediante accordi collusivi con lo stesso	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto
Controlli verifiche, ispezioni e sanzioni		Valutazione offerte tecniche: Partecipazione alla commissioni di gara e/valutazioni offerte tecniche	Favorire prodotti o soluzioni non soddisfacenti sotto il profilo dei contenuti o delle funzionalità al fine di ottenere vantaggi illeciti mediante accordi collusivi con lo stesso	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto
Controlli verifiche, ispezioni e sanzioni		Verifica delle modalità di esecuzione del contratto e dei livelli di servizio ed eventuale applicazione di penali: Esecuzione dei test dei servizi/applicazioni da realizzare Monitoraggio dell'andamento dei costi in relazione al budget allocato per le attività di sviluppo IT Attività connesse alla Regolare Esecuzione della prestazione o relativa contestazione	coprire inadempienze dei fornitori	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto, mancato controllo
Controlli verifiche, ispezioni e sanzioni		Rilascio certificato di conformità/regolare esecuzione	irregolare esecuzione del contratto	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto
Controlli verifiche, ispezioni e sanzioni		Gestione dei backup/restore dei dati: Definizione delle strategie di backup (giornaliero, settimanale, full, incrementale, etc.) per ciascuno dei sistemi IT (database, server, filesystem, etc.) Pianificazione dei backup Controllo e monitoraggio dell'esecuzione dei backup Esecuzione Restore su richiesta	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni	Gestione della Sicurezza delle Informazioni	Gestione dei permessi per gli utenti: Acquisizione richiesta permessi Approvazione richiesta, previo verifica requisiti Attribuzione permessi Rimozione permessi non più necessari su evento (es. cambio ufficio, cessazione del rapporto di lavoro, etc.) o, periodicamente, su assessment	Nessun evento rischioso	Non rilevato

Controlli verifiche, ispezioni e sanzioni	<p>Informazioni.</p> <p>Allineare la sicurezza delle informazioni alla sicurezza attesa dal business ed assicurarsi che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi, per quanto riguarda le proprietà di disponibilità, integrità, confidenzialità e autenticità delle informazioni</p>	<p>Gestione della sicurezza di rete:</p> <p>Definizione dei requisiti di sicurezza di rete</p> <p>Implementazione delle contromisure adeguate (Firewall, etc..)</p> <p>Gestione delle richieste interne/esterne di collegamento a sistemi/servizi; ad es. VPN, FirewallXML, etc.</p> <p>Analisi degli eventi di sicurezza di rete</p>	<p>Concessione di autorizzazioni per l'accesso a sistemi e dati di IZSLER a soggetti che non ne hanno titolo, al fine di trarne benefici illegittimi</p>	<p>monopolio delle competenze</p> <p>conflitti di interesse</p> <p>processo completamente realizzato all'interno di un'unica struttura</p> <p>esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto</p>
Controlli verifiche, ispezioni e sanzioni		<p>Prevenzione, rilevazione e rimozione di software malevoli:</p> <p>Configurazione sistemi antivirus su postazioni di lavoro e server</p> <p>Monitoraggio delle attività Antivirus e della diffusione di software malevoli</p> <p>Risoluzione di problemi legati a presenza di software malevoli, sensibilizzazione degli utenti</p>	<p>Nessun evento rischioso</p>	<p>Non rilevato</p>
Controlli verifiche, ispezioni e sanzioni		<p>Gestione degli incidenti:</p> <p>Rilevazione dell'incidente</p> <p>Attivazione contromisure temporanee, comunicazione agli stakeholder</p> <p>Risoluzione dell'incidente e adozione contromisure</p>	<p>Mancato controllo al fine di nascondere il verificarsi di accessi non autorizzati a sistemi e dati di IZSLER per trarne benefici illegittimi</p>	<p>monopolio delle competenze</p> <p>conflitti di interesse</p> <p>processo completamente realizzato all'interno di un'unica struttura</p> <p>esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto</p>
Controlli verifiche, ispezioni e sanzioni		<p>Gestione dell'audit su sistemi e dati:</p> <p>Configurazione, analisi e archiviazione dei dati di audit relativi all'utilizzo dei sistemi (database, filesystem, applicazioni)</p>	<p>Nessun evento rischioso</p>	<p>Non rilevato</p>
Controlli verifiche, ispezioni e sanzioni		<p>Ricognizione normativa applicabile in materia di sicurezza e tutela privacy per i sistemi in gestione ai Sistemi Informativi:</p> <p>Gestione ATTIVITA': Gestione adempimenti ai fini delle valutazioni di impatto della normativa vigente sui dati e le informazioni trattate da IZSLER. Gruppo inter reparto coordinata dal responsabile Sistemi Informativi, verificare impatto dei singoli punti</p>	<p>Nessun evento rischioso</p>	<p>Non rilevato</p>

Controlli verifiche, ispezioni e sanzioni	Gestione delle attività volte ad assicurare la sicurezza delle informazioni e la tutela della privacy	<p>Applicazione della normativa sicurezza/privacy al contesto delle informazioni e dei trattamenti di dati personali effettuati da IZSLER:</p> <p>Verifica  ATTIVITA': Verifica della conformità di IZSLER alle previsioni del codice Privacy e CAD. Gruppo di lavoro verificare applicazione dei singoli punti</p> <p>Identificazione interventi  - ATTIVITA': Identificazione del piano degli interventi di adeguamento normativo e supporto agli uffici interni ai fini del rispetto delle prescrizioni del Codice Privacy. Gruppo di lavoro verificare applicazione dei singoli punti</p> <p>Supporto  - ATTIVITA': Supporto agli uffici nell'attuazione degli interventi necessari per l'adeguamento alla disciplina Privacy e la sicurezza delle informazioni</p>	accessi non autorizzati a sistemi e dati di IZSLER per trarne benefici illegittimi	monopolio delle competenze conflitti di interesse processo completamente realizzato all'interno di un'unica struttura esercizio esclusivo della responsabilità di un processo da parte di pochi o di un unico soggetto, mancato controllo
Controlli verifiche, ispezioni e sanzioni		Definizione delle risorse critiche Definizione delle risorse critiche (applicazioni, servizi, etc.) da sottoporre al piano di business continuity/disaster recovery	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni	IT Service Continuity Management: supportare il processo di Business Continuity Management assicurando che i servizi IT possano essere ripristinati in tempi e modi predeterminati. Fa parte di questo processo il governo delle procedure e delle infrastrutture di Disaster Recovery	Redazione e mantenimento del piano di IT business continuity: Redazione del piano di IT business continuity / disaster recovery (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti) Mantenimento del piano di IT business continuity (attività governata dall'ufficio e realizzata esternamente tramite contratto di fornitura con terze parti)	Nessun evento rischioso	Non rilevato
Controlli verifiche, ispezioni e sanzioni		Test del piano di Disaster Recovery: Schedulazione del test di Disaster Recovery Esecuzione del test di Disaster Recovery Verifica dei risultati del test di Disaster Recovery	Nessun evento rischioso	Non rilevato



B) Contratti pubblici - Affidamento di lavori, servizi e forniture <sup>3</sup>	3) Gestione della domanda e Pianificazione servizi IT	3.3) Elaborazione piano degli interventi IT: Definizione interventi IT da realizzare nel corso dell'anno Definizione del piano di realizzazione Monitoraggio e controllo dell'attuazione delle attività a piano	medio	medio	No	No	No	No	Misure di prevenzione non esistenti	No	basso	basso	Il grado di discrezionalità è legato a conoscenze tecniche esclusive all'interno dei Sistemi Informativi. Il numero di soggetti coinvolti nel processo non è alto, sia per la limitata numerosità del personale dei Sistemi Informativi, sia per la necessaria verticalizzazione delle competenze in campo informatico che limita ulteriormente il campo del possibile personale coinvolgibile. Va però considerato che il pericolo di corruzione per questo rischio è molto improbabile, in quanto la sovrastima dei bisogni non può portare direttamente vantaggi a soggetti precisi, dovendo comunque fatta una gara con più soggetti. Inoltre è norma aderire a convenzioni CONSIP. Si ritiene quindi il rischio basso
Controlli verifiche, ispezioni e sanzioni	4) Erogazione dei Servizi Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT. Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi	4.2) Monitoraggio della disponibilità dei servizi: Individuazione oggetti da monitorare Configurazione del monitoraggio Produzione della reportistica di disponibilità dei servizi e dell'infrastruttura Verifica degli allarmi generati dalle sonde di monitoraggio Individuazione ed applicazione delle contromisure in caso di livelli di disponibilità inaccettabili	basso	basso	No	No	Si	No	Misure di prevenzione non esistenti	No	basso	basso	Il grado di discrezionalità per questi eventi è basso, essendo legato a sistemi che registrano ogni evento, e, oltre a coinvolgere più soggetti dei Sistemi Informativi che ricevono la segnalazione degli eventi, coinvolge anche gli utenti del servizio, che non fanno parte dei Sistemi Informativi. E' anche basso il vantaggio teorico che può essere ottenuto da un accordo collusivo per coprire questi eventi, poiché è limitato il possibile danno per il fornitore. Si ritiene quindi che il rischio corruttivo per questo evento sia basso
Controlli verifiche, ispezioni e sanzioni	4) Erogazione dei Servizi Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT. Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi	4.3) Gestione degli incidenti: Rilevazione dell'incidente Attivazione contromisure temporanee o attivazione del Disaster Recovery; comunicazione agli stakeholder Risoluzione dell'incidente	basso	basso	No	No	Si	No	Misure di prevenzione non esistenti	No	basso	basso	Il grado di discrezionalità per questi eventi è basso, essendo legato a sistemi che registrano ogni evento, e, oltre a coinvolgere più soggetti dei Sistemi Informativi che ricevono la segnalazione degli eventi, coinvolge anche gli utenti del servizio, che non fanno parte dei Sistemi Informativi. E' anche basso il vantaggio teorico che può essere ottenuto da un accordo collusivo per coprire questi eventi, poiché è limitato il possibile danno per il fornitore. Si ritiene quindi che il rischio corruttivo per questo evento sia basso
Controlli verifiche, ispezioni e sanzioni	4) Erogazione dei Servizi Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT. Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi	4.4) Gestione dei Problemi: Individuazione problemi a sistemi e/o servizi IT, rilevati in autonomia o su richiesta da parte di utenti/personale degli uffici Analisi delle cause tramite ispezione dei log, analisi dei dati, verifiche di raggiungibilità dei servizi, etc. Proposte cambiamenti per risolvere i problemi o escalation verso i gruppi di competenza	basso	basso	No	No	Si	No	Misure di prevenzione non esistenti	No	basso	basso	Il grado di discrezionalità per questi eventi è basso, essendo legato a sistemi che registrano ogni evento, e, oltre a coinvolgere più soggetti dei Sistemi Informativi che ricevono la segnalazione degli eventi, coinvolge anche gli utenti del servizio, che non fanno parte dei Sistemi Informativi. E' anche basso il vantaggio teorico che può essere ottenuto da un accordo collusivo per coprire questi eventi, poiché è limitato il possibile danno per il fornitore. Si ritiene quindi che il rischio corruttivo per questo evento sia basso
Controlli verifiche, ispezioni e sanzioni	4) Erogazione dei Servizi Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT. Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi	4.5) Amministrazione dei sistemi: Monitoraggio continuativo degli eventi di sistema, inclusa la corretta esecuzione dei job schedulati, e interventi di manutenzione dei sistemi	basso	basso	No	No	Si	No	Misure di prevenzione non esistenti	No	basso	basso	Il grado di discrezionalità per questi eventi è basso, essendo legato a sistemi che registrano ogni evento, e, oltre a coinvolgere più soggetti dei Sistemi Informativi che ricevono la segnalazione degli eventi, coinvolge anche gli utenti del servizio, che non fanno parte dei Sistemi Informativi. E' anche basso il vantaggio teorico che può essere ottenuto da un accordo collusivo per coprire questi eventi, poiché è limitato il possibile danno per il fornitore. Si ritiene quindi che il rischio corruttivo per questo evento sia basso
Controlli verifiche, ispezioni e sanzioni	4) Erogazione dei Servizi Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT. Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi	4.8) Gestione strumenti produttività individuale (stampanti, PC, scanner, portatili) Le procedure vengono condivise periodicamente tra il personale della stessa articolazione Assegnazione delle risorse in base alle regole stabilite, alle disponibilità dei materiali e l'effettiva necessità degli strumenti L'utilizzo delle risorse assegnate è tracciato nel log A fronte del riscontro del non più utilizzo di una o più risorse le stesse vengono tolte ed eventualmente riassegnate	medio	basso	No	No	No	No	Misure di prevenzione non esistenti	No	basso	basso	Il grado di discrezionalità per questi eventi è medio, perché, pur essendo discrezionale la scelta dell'assegnazione delle risorse da parte dei Sistemi Informativi, coinvolgere più soggetti dei Sistemi Informativi e coinvolge anche i richiedenti, che non fanno parte dei Sistemi Informativi. E' anche basso il vantaggio che può essere ottenuto da una priorità ingiustificata di assegnazione delle risorse. Si ritiene quindi che il rischio corruttivo per questo evento sia basso
Controlli verifiche, ispezioni e sanzioni	5) Estrazione dati	5.2) Gestione delle richieste di accesso e scambio dati presenti nelle banche dati di IZSLER da parte di altre Pubbliche Amministrazioni: Ricezione, tracciamento ed Analisi delle richieste Definizione dei protocolli di intesa in linea con la normativa vigente Progettazione e realizzazione di soluzioni per lo scambio dati inclusi eventuali servizi di cooperazione applicativa	basso	basso	No	No	No	Si	No	No	basso	medio	Le richieste di estrazioni di dati direttamente dalle basi di dati aziendali da parte di personale di Sistemi Informativi, pur difficilmente controllabili nella modalità di effettuazione, sono comunque verificabili dai reparti di cui le estrazioni rappresentano la realtà. In particolare il ufficio controllo di gestione e performance ha accesso alle basi dati in modalità quasi completa. Inoltre le estrazioni possono essere riprodotte in ogni momento successivo per la verifica della correttezza. Il Dirigente dei Sistemi Informativi autorizza ogni richiesta di estrazione. Si ritiene quindi il rischio medio
Controlli verifiche, ispezioni e sanzioni	7) Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	7.1) Predisposizione dei capitolati di gara per lo sviluppo di servizi/applicazioni IT: Predisposizione del capitolato tecnico Supporto all'ufficio competente per la predisposizione della documentazione di gara	alto	medio	No	No	No	No	Misure di prevenzione non esistenti	Si	basso	alto	Il Capitolato di Gara può essere predisposto con l'intento di favorire uno o più fornitori, e sono evidenti i vantaggi per il fornitore. Questo intento è inoltre di difficile verifica per personale non informatico e con conoscenza specifica sull'oggetto della gara (infrastruttura, applicazioni, sistemi web...) E' quindi conseguente un altro rischio per questo evento
Controlli verifiche, ispezioni e sanzioni	7) Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	7.2) Valutazione offerte tecniche: Partecipazione alla commissioni di gara e/valutazioni offerte tecniche	medio	medio	No	No	No	No	Misure di prevenzione non esistenti	Si	basso	medio	Un partecipante ad una Commissione di Gara può discrezionalmente favorire un soggetto. Questo rischio è però mitigato dal fatto che sono comunque presenti più commissari, e la discrezionalità è comunque limitata dall'ambito del Capitolato di Gara, che prevede elementi il più oggettivi possibile. Nel complesso si ritiene quindi il rischio medio

Controlli verifiche, ispezioni e sanzioni	7) Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	7.3) Verifica delle modalità di esecuzione del contratto e dei livelli di servizio ed eventuale applicazione di penali: Esecuzione dei test dei servizi/applicazioni da realizzare Monitoraggio dell'andamento dei costi in relazione al budget allocato per le attività di sviluppo IT Attività connesse alla Regolare Esecuzione della prestazione o relativa contestazione	basso	basso	No	No	No	Si	Si	No	basso	medio	Riguardo alla discrezionalità legata a questi eventi, da una parte è completa responsabilità di chi gestisce il contratto di giudicare il coinvolgimento del fornitore. D'altra parte è legato a situazioni che, oltre a coinvolgere più soggetti dei Sistemi Informativi che ricevono la segnalazione degli eventi, coinvolgono anche gli utenti del servizio, che non fanno parte dei Sistemi Informativi. Inoltre, nel caso dovesse portare a danni economici per l'Istituto per mancanza di fornitura o necessità di ulteriori pagamenti, verrebbe effettuata una analisi della situazione da altri soggetti. Si ritiene quindi che il rischio corruttivo per questo evento sia medio
Controlli verifiche, ispezioni e sanzioni	7) Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	7.4) Rilascio certificato di conformità/regolare esecuzione	basso	basso	No	No	No	Si	Si	No	basso	medio	Riguardo alla discrezionalità legata a questi eventi, da una parte è completa responsabilità di chi gestisce il contratto di giudicare il coinvolgimento del fornitore. D'altra parte è legato a situazioni che, oltre a coinvolgere più soggetti dei Sistemi Informativi che ricevono la segnalazione degli eventi, coinvolgono anche gli utenti del servizio, che non fanno parte dei Sistemi Informativi. Inoltre, nel caso dovesse portare a danni economici per l'Istituto per mancanza di fornitura o necessità di ulteriori pagamenti, verrebbe effettuata una analisi della situazione da altri soggetti. Si ritiene quindi che il rischio corruttivo per questo evento sia medio
Controlli verifiche, ispezioni e sanzioni	8) Gestione della Sicurezza delle Informazioni. Allineare la sicurezza delle informazioni alla sicurezza attesa dal business ed assicurarsi che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi, per quanto riguarda le proprietà di disponibilità, integrità, confidenzialità e autenticità delle informazioni	8.5) Gestione degli incidenti di sicurezza: Rilevazione dell'incidente Attivazione contromisure temporanee; comunicazione agli stakeholder Risoluzione dell'incidente e adozione contromisure	basso	basso	No	No	No	Si	Si	No	basso	medio	Riguardo alla discrezionalità legata a questi eventi, da una parte è completa responsabilità di chi gestisce il contratto di giudicare il coinvolgimento del fornitore. D'altra parte è legato a situazioni che, oltre a coinvolgere più soggetti dei Sistemi Informativi che ricevono la segnalazione degli eventi, coinvolgono anche gli utenti del servizio, che non fanno parte dei Sistemi Informativi. Inoltre, nel caso dovesse portare a danni economici per l'Istituto per mancanza di fornitura o necessità di ulteriori pagamenti, verrebbe effettuata una analisi della situazione da altri soggetti. Si ritiene quindi che il rischio corruttivo per questo evento sia medio
Controlli verifiche, ispezioni e sanzioni	9) Gestione delle attività volte ad assicurare la sicurezza delle informazioni e la tutela della privacy	9.2) Applicazione della normativa sicurezza/privacy al contesto delle informazioni e dei trattamenti di dati personali effettuati da IZSLER: Verifica ATTIVITA': Verifica della conformità di IZSLER alle previsioni del codice Privacy e CAD. Gruppo di lavoro verificare applicazione dei singoli punti Identificazione interventi - ATTIVITA': Identificazione del piano degli interventi di adeguamento normativo e supporto agli uffici interni ai fini del rispetto delle prescrizioni del Codice Privacy. Gruppo di lavoro verificare applicazione dei singoli punti Supporto - ATTIVITA': Supporto agli uffici nell'attuazione degli interventi necessari per l'adeguamento alla disciplina Privacy e la sicurezza delle informazioni	medio	basso	No	No	No	Si	Si	No	basso	medio	L'accesso ai dati personali nelle risorse informatiche è tracciato dai sistemi di log, e sono individuati puntualmente gli ambiti di intervento da Amministratore di Sistema degli operatori, per non permettere accessi privilegiati a risorse a cui non si ha interesse lavorativo. E' inoltre basso il valore che hanno i dati personali presenti sui sistemi IZSLER. Poiché però la discrezionalità del personale che effettua tali accessi è comunque non bassa e, l'evento, dovesse accadere, possa difficilmente essere riscontrato, si ritiene che nel complesso il rischio sia medio
Controlli verifiche, ispezioni e sanzioni	8) Gestione della Sicurezza delle Informazioni. Allineare la sicurezza delle informazioni alla sicurezza attesa dal business ed assicurarsi che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi, per quanto riguarda le proprietà di disponibilità, integrità, confidenzialità e autenticità delle informazioni	8.3) Gestione della sicurezza di rete: Definizione dei requisiti di sicurezza di rete Implementazione delle contromisure adeguate (Firewall, etc.) Gestione delle richieste interne/esterne di collegamento a sistemi/servizi; ad es. VPN, FirewallXML, etc. Analisi degli eventi di sicurezza di rete	medio	medio	No	No	Si	Si	Si	No	basso	medio	La procedura di accesso da parte di esterni ai dati e sistemi IZSLER viene effettuata dal personale delle infrastrutture dei Sistemi Informativi, attualmente un gruppo di 4 persone in grado di verificare il non corretto operare dei colleghi. Il potenziale vantaggio da parte di un esterno di accesso a dati presenti sui sistemi IZSLER è medio. Nel complesso si ritiene quindi il rischio medio

**INDIVIDUAZIONE E PROGRAMMAZIONE DELLE MISURE**

AREA DI RISCHIO	PROCESSO	FASE/ATTIVITA'	MISURA	TIPOLOGIA DI MISURA	TEMPI DI ATTUAZIONE DELLA MISURA	INDICATORE	TARGET	RESPONSABILE DELL'ATTUAZIONE	UNITA' ORGANIZZATIVA
Gestione delle entrate, delle spese e del patrimonio	Valorizzazione delle prove di laboratorio	Valorizzazione della prova e invio per la validazione al Dirigente validatore preposto	Validazione delle tariffe e/o corrispettivi da parte di un soggetto diverso dal valorizzatore	Controllo	Continua	N. tariffe e/o corrispettivi validati da un soggetto diverso dal valorizzatore/ N. tariffe e/o corrispettivi valorizzati	100%	Dirigente Responsabile UO Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance	UO Programmazione dei servizi tecnici e controllo di gestione
Gestione delle entrate, delle spese e del patrimonio	Valorizzazione delle prove di laboratorio	Verifica della valorizzazione, validazione e comunicazione all'ufficio Controllo di Gestione e performance	Controllo coerenza costi materiali di laboratorio utilizzati dalla struttura rispetto alle prestazioni erogate quando lo scostamento è ≥ 5%	Controllo	Annuale entro il 30 settembre	n. anomalie verificate/n. anomalie riscontrate	100%	Dirigente Responsabile UO Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance	UO Programmazione dei servizi tecnici e controllo di gestione
Gestione delle entrate, delle spese e del patrimonio	Valorizzazione dei prodotti/prezzo di vendita dei prodotti (tariffazione)	Valorizzazione del prodotto e invio per la validazione al Dirigente validatore preposto	Validazione del prodotto da parte di un soggetto diverso dal valorizzatore	Controllo	Continua	N. prodotti validati da un soggetto diverso dal valorizzatore/ N. prodotti valorizzati	100%	Dirigente Responsabile UO Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance	UO Programmazione dei servizi tecnici e controllo di gestione
Gestione delle entrate, delle spese e del patrimonio	Valorizzazione dei prodotti/prezzo di vendita dei prodotti (tariffazione)	Proposta del prezzo di vendita da parte del Dirigente valorizzatore	Valutazione congiunta della Direzione Generale e dell'ufficio Controllo di Gestione e performance sulla proposta del prezzo di vendita, in considerazione degli aspetti strategici, remunerativi, competitivi del prodotto	Controllo/regolamentazione	Continua	N. valutazioni formulate dal Direttore Generale e dall'ufficio Controllo di Gestione e performance sul prezzo di vendita/ N. prezzi di vendita proposti	100%	Dirigente Responsabile UO Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance	UO Programmazione dei servizi tecnici e controllo di gestione
Gestione delle entrate, delle spese e del patrimonio	Controllo richieste di nota di variazione di fatture emesse	L'ufficio Controllo di Gestione e performance effettua un controllo di corrispondenza fra i dati presenti nel software sanitario e quanto indicato nelle richieste di nota di variazione da emettere. Se il controllo è positivo l'ufficio Controllo di Gestione e performance comunica l'esito al U.O. Gestione Servizi Contabili che procederà ed emettere la nota di variazione, in caso negativo l'ufficio Controllo di Gestione e performance comunica al reparto che ha emesso la richiesta di procedere con le opportune modifiche nel software sanitario	Verifica a campione della coerenza tra le note di variazione emesse nel 2020 e i dati presenti nel gestionale sanitario	Controllo	Annuale entro il 30 settembre	N. note di variazione coerenti con i dati presenti nel gestionale sanitario/N. note di variazione oggetto di verifica	100%	Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Gestione delle attività di ricerca	Attivazione piani di monitoraggio	Invio da parte del Dirigente responsabile del piano di monitoraggio alla Direzione Generale di una richiesta di attivazione del piano di monitoraggio	Verifica congiunta della Direzione Generale e dell'ufficio Controllo di Gestione e performance a consuntivo dell'attività svolta nell'ambito del piano di monitoraggio	Controllo	Continua	N. verifiche effettuate dal Direttore Generale e dall'ufficio Controllo di Gestione e performance/n. piani di monitoraggio conclusi	100%	Dirigente Responsabile UO Programmazione dei servizi tecnici e controllo di gestione - ufficio controllo di gestione e performance	UO Programmazione dei servizi tecnici e controllo di gestione
Controlli verifiche, ispezioni e sanzioni	Estrazione dati	Gestione delle richieste di accesso e scambio dati presenti nelle banche dati di IZSLER da parte di altre Pubbliche Amministrazioni: Ricezione, tracciamento ed Analisi delle richieste Definizione dei protocolli di intesa in linea con la normativa vigente Progettazione e realizzazione di soluzioni per lo scambio dati inclusi eventuali servizi di cooperazione applicativa	Autorizzazione preventiva Direzione Competente	Misura di controllo	Continuo	Richieste autorizzate / Richieste ricevute	100%	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi

Controlli verifiche, ispezioni e sanzioni	Estrazione dati	5.2) Gestione delle richieste di accesso e scambio dati presenti nelle banche dati di IZSLER da parte di altre Pubbliche Amministrazioni: Ricezione, tracciamento ed Analisi delle richieste Definizione dei protocolli di intesa in linea con la normativa vigente Progettazione e realizzazione di soluzioni per lo scambio dati inclusi eventuali servizi di cooperazione applicativa	Verifica puntuale sulle segnalazioni di anomalia del dato estratto	Misura di controllo	Continuo	Segnalazioni con anomalie non giustificate	0	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	Predisposizione dei capitolati di gara per lo sviluppo di servizi/applicazioni IT: Predisposizione del capitolato tecnico Supporto all'ufficio competente per la predisposizione della documentazione di gara	Capitolato redatto da almeno due persone o altrimenti verifica del capitolato tecnico da altra persona con adeguata competenza	Misura di controllo	Continuo	N. capitolati tecnici redatti da più persone o validati da altra persona/ N. capitolati tecnici proposti	100%	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	Valutazione offerte tecniche: Partecipazione alle commissioni di gara e/valutazioni offerte tecniche	Partecipazione a commissione di gara solo per persone che non hanno partecipato al capitolato tecnico	Misura di rotazione	Continuo	N. verifiche di non coinvolgimento al CT / N. nomine	100%	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	Rilascio certificato di conformità/regolare esecuzione	Controlli periodici su modalità di vigilanza della corretta esecuzione del contratto e dell'avanzamento lavori	Misura di controllo	semestrale	Report al 31 maggio e 31 ottobre al Direttore Amministrativo attestante l'attività di vigilanza sull'esecuzione contrattuale	2	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Gestione della Sicurezza delle Informazioni. Allineare la sicurezza delle informazioni alla sicurezza attesa dal business ed assicurarsi che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi, per quanto riguarda le proprietà di disponibilità, integrità, confidenzialità e autenticità delle informazioni	Gestione della sicurezza di rete: Definizione dei requisiti di sicurezza di rete Implementazione delle contromisure adeguate (Firewall, etc.) Gestione delle richieste interne/esterne di collegamento a sistemi/servizi; ad es. VPN, FirewallXML, etc. Analisi degli eventi di sicurezza di rete	Vaglio preventivo del responsabile dei Sistemi Informativi	Misura di controllo	Continuo	N richieste vagliate dal responsabile Sistemi Informativi / N. richieste	100%	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Erogazione dei Servizi Mantenere e gradualmente migliorare la qualità e la disponibilità dei servizi IT. Gestione e progettazione dell'infrastruttura e dell'architettura dei servizi erogati, gestione degli eventi, delle richieste, degli incidenti e dei problemi	8Gestione degli incidenti: Rilevazione dell'incidente Attivazione contromisure temporanee o attivazione del Disaster Recovery; comunicazione agli stakeholder Risoluzione dell'incidente	Apertura di non conformità interna al verificarsi di eventi rilevanti nella sicurezza e registrazione nel sistema di ticket	Misura di controllo	Continuo	N. ticket / N. segnalazione di incidenti	100%	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Gestione dei Fornitori Esterni - Gestire i fornitori ed i servizi da essi forniti, in modo da assicurare il giusto rapporto costi qualità dei servizi IT	Verifica delle modalità di esecuzione del contratto e dei livelli di servizio ed eventuale applicazione di penali: Esecuzione dei test dei servizi/applicazioni da realizzare Monitoraggio dell'andamento dei costi in relazione al budget allocato per le attività di sviluppo IT Attività connesse alla Regolare Esecuzione della prestazione o relativa contestazione	Esecuzione sistematica delle verifiche contrattuali previste	Misura di controllo	Continuo	N° verifiche effettuale/Numero verifiche richieste dai contratti per i quali i Sistemi Informativi sono DEC	>=90%	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi

Controlli verifiche, ispezioni e sanzioni	Gestione delle attività volte ad assicurare la sicurezza delle informazioni e la tutela della privacy	Applicazione della normativa sicurezza/privacy al contesto delle informazioni e dei trattamenti di dati personali effettuati da IZSLER: Verifica ATTIVITA': Verifica della conformità di IZSLER alle previsioni del codice Privacy e CAD. Gruppo di lavoro verificare applicazione dei singoli punti Identificazione interventi - ATTIVITA': Identificazione del piano degli interventi di adeguamento normativo e supporto agli uffici interni ai fini del rispetto delle prescrizioni del Codice Privacy. Gruppo di lavoro verificare applicazione dei singoli punti Supporto - ATTIVITA': Supporto agli uffici nell'attuazione degli interventi necessari per l'adeguamento alla disciplina Privacy e la sicurezza delle informazioni	Utilizzo di procedure e metodi di pulizia a basso livello dei dispositivi che vengono rottamati o donati	Misura di controllo	Continuo	N°PC con pulizia dei dati/N°PC Cessati o donati	>=0,9	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	Gestione delle attività volte ad assicurare la sicurezza delle informazioni e la tutela della privacy	Applicazione della normativa sicurezza/privacy al contesto delle informazioni e dei trattamenti di dati personali effettuati da IZSLER: Verifica ATTIVITA': Verifica della conformità di IZSLER alle previsioni del codice Privacy e CAD. Gruppo di lavoro verificare applicazione dei singoli punti Identificazione interventi - ATTIVITA': Identificazione del piano degli interventi di adeguamento normativo e supporto agli uffici interni ai fini del rispetto delle prescrizioni del Codice Privacy. Gruppo di lavoro verificare applicazione dei singoli punti Supporto - ATTIVITA': Supporto agli uffici nell'attuazione degli interventi necessari per l'adeguamento alla disciplina Privacy e la sicurezza delle informazioni	Registrazione Accessi da parte degli Amministratori di Sistema	Misura di controllo	Continuo	N°Log mensili / n. mesi		1 Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi
Controlli verifiche, ispezioni e sanzioni	9) Gestione delle attività volte ad assicurare la sicurezza delle informazioni e la tutela della privacy	Applicazione della normativa sicurezza/privacy al contesto delle informazioni e dei trattamenti di dati personali effettuati da IZSLER: Verifica ATTIVITA': Verifica della conformità di IZSLER alle previsioni del codice Privacy e CAD. Gruppo di lavoro verificare applicazione dei singoli punti Identificazione interventi - ATTIVITA': Identificazione del piano degli interventi di adeguamento normativo e supporto agli uffici interni ai fini del rispetto delle prescrizioni del Codice Privacy. Gruppo di lavoro verificare applicazione dei singoli punti Supporto - ATTIVITA': Supporto agli uffici nell'attuazione degli interventi necessari per l'adeguamento alla disciplina Privacy e la sicurezza delle informazioni	Autorizzazione preventiva Direzione Competente	Misura di controllo	Continuo	Richieste autorizzate / Richieste ricevute	100%	Dirigente responsabile Sistemi Informativi	UO Programmazione dei servizi tecnici e controllo di gestione - Sistemi Informativi