REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS ENTES LOCALES, FINÀNTZIAS E URBANÌSTICA
ASSESSORATO DEGLI ENTI LOCALI, FINANZE E URBANISTICA

AFFIDAMENTO DEL SERVIZIO DI POLIZZA ASSICURATIVA "CYBER" – REGIONE AUTONOMA DELLA SARDEGNA.

In relazione all'affidamento del servizio di polizza assicurativa "Rischio Cyber", il Servizio Gestione Contratti per il funzionamento degli uffici regionali, facente parte della Direzione Generale degli Enti Locali e Finanze, avente competenza sul procedimento di affidamento del servizio di polizza, trasmette la documentazione compilata dalla Direzione Generale dell'Innovazione e Sicurezza It, dalla Direzione Generale dei Servizi Finanziari, dalla Direzione Generale del Lavoro, dalla Direzione Generale del Personale e Riforma della Regione, dalla Direzione Generale delle Politiche Sociali e dalla Direzione Generale della Sanità: queste due ultime Direzioni Generali, come indicato nelle rispettive note introduttive, hanno provveduto alla compilazione di due questionari distinti, uno relativo al dominio interno "Sanita" e l'altro relativo ai sistemi e servizi gestiti per il tramite della In House "Sardegna IT" o direttamente da fornitori esterni (SISaR).

In considerazione delle peculiarità di ciascuna Direzione Generale, si è proceduto a richiedere la compilazione da parte di ognuna di esse, di un Questionario e un "Ransomware Supplemental", introdotti da una breve presentazione descrittiva.

Si riportano, di seguito e **nell'ordine indicato**, le introduzioni descrittive inviate da ciascuna Direzione Generale, seguite dal relativo Questionario e, separatamente nel formato trasmesso dalle stesse Direzioni, i relativi "Ransomware Supplemental".

1) **Direzione Generale dell'Innovazione e Sicurezza It: nota introduttiva e questionario;**
2) **Direzione Generale dei Servizi Finanziari: nota introduttiva e questionario;**
3) **Direzione Generale del Lavoro: nota introduttiva e questionario;**
4) **Direzione Generale del Personale e Riforma della Regione: nota introduttiva e questionario;**
5) **Direzione Generale della Sanità: nota introduttiva e questionario**
6) **Direzione Generale delle Politiche Sociali: nota introduttiva e questionario;**
7) **Sardegna IT: questionario.**

MASSIMILIANO
COTZA
27.11.2025
16:57:51
GMT+01:00

Si ravvisa che l'amministrazione è certificata :

ISO9001 : 2015 COORDINAMENTO STRATEGICO, SVILUPPO, PIANIFICAZIONE, PROGRAMMAZIONE, MONITORAGGIO E CONTROLLO PER LA TRANSIZIONE DIGITALE DELLA REGIONE AUTONOMA DELLA SARDEGNA E SUPPORTO AGLI ENTI LOCALI

ISO/IEC 20000-1:2018 SISTEMA DI GESTIONE DEI SERVIZI A SUPPORTO DEI SERVIZI INFRASTRUTTURALI EROGATI AGLI ASSESSORATI REGIONALI E AI COMUNI ADERENTI AL POLO STRATEGICO REGIONALE

ISO 22301:2019 PROGETTAZIONE E EROGAZIONE DI SISTEMI E SERVIZI DI DATA CENTER AGLI ASSESSORATI REGIONALI E AI COMUNI ADERENTI AL POLO STRATEGICO REGIONALE. PROGETTAZIONE E GESTIONE RETE TELEMATICA REGIONALE

ISO/IEC 27001:2013 - UNI CEI EN ISO/IEC 27001:2017 PROGETTAZIONE ED EROGAZIONE DI SISTEMI E SERVIZI DI DATA CENTER AGLI ASSESSORATI REGIONALI E AI COMUNI ADERENTI AL POLO STRATEGICO REGIONALE. PROGETTAZIONE E GESTIONE RETE TELEMATICA REGIONALE.

DIREZIONE GENERALE DELL'INNOVAZIONE E DELLA SICUREZZA IT

Strategia di allineamento per il rinnovo della polizza cyber della Regione Autonoma di Sardegna in scadenza: Premessa al questionario

Come definito dalla deliberazione di giunta regionale 24/27 del 14.05.2018, in particolare nel suo allegato:

"L'infrastruttura informatica della RAS è oggi caratterizzata da diversi domini Windows. Le seguenti direzioni generali dispongono di un dominio autonomo, gestito dal proprio organico informatico:

• Assessorato dell'igiene e sanità e dell'assistenza sociale

- Ufficio di Gabinetto
- Direzione generale della sanità
- Direzione generale delle politiche sociali

• Assessorato della programmazione, bilancio, credito e assetto del territorio

- Ufficio di Gabinetto
- Direzione generale dei Servizi finanziari

• Assessorato degli affari generali, personale e riforma della Regione

- Direzione generale del personale e riforma della Regione

• Assessorato del lavoro, formazione professionale, cooperazione e sicurezza sociale

- Ufficio di Gabinetto
- Direzione generale del lavoro, formazione professionale, cooperazione e sicurezza sociale

Le strutture e le relative direzioni generali non presenti nell'elenco di cui sopra costituiscono diverse unità organizzative (organizational unit – OU) di un unico dominio "Regione Sardegna" (RS).

L'Amministrazione regionale, al passo con l'evoluzione tecnologica e nell'ottica del risparmio generato dalle economie di scala, ha scelto di centralizzare quei servizi che, per loro stessa natura, sono trasversali all'intera organizzazione regionale, quali:

- connettività di rete;
- servizi documentali e HR (SIBAR);
- servizi contabili (SAP SCI);
- sistemi virtualizzati[1];
- spazi di archiviazione.

Parallelamente, data l'eterogeneità dei procedimenti e dei dati trattati dai vari assessorati (si consideri, ad esempio, la peculiarità dei dati trattati dalla direzione generale della Sanità e la tipologia ed eterogeneità di soggetti utilizzatori di tali dati: dipendenti della DG Sanità, ASL, farmacisti, medici di base, pazienti o altri nell'ambito dell'ampia rete del lavoro, ecc.), ogni staff informatico ha configurato, anche attraverso l'acquisto di hardware, spazi cloud e software

[1] Per virtualizzazione, in ambiti informatici, si intende la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente. Qualunque tipo di risorsa può essere virtualizzata, ma gli usi più frequenti riguardano la virtualizzazione dei server, dei sistemi operativi, della memoria e dello spazio fisico di un disco, etc.

specifici, una serie di servizi in modo da soddisfare in tempo reale le esigenze operative dell'Assessorato di appartenenza.

Tra i servizi posti in essere:

- tenuta e protezione dei dati, garantendone l'integrità:
- procedure di office automation;
- distribuzione automatizzata dei software di produttività e dei relativi aggiornamenti;
- stampanti di rete condivise (print server).

I servizi peculiari dei singoli domini sono stati offerti nel corso del tempo nel rispetto delle norme di sicurezza e protezione vigenti, e sono stati gestiti dall'organico informatico di riferimento con buone pratiche da analizzare e condividere in sede di coordinamento tra le direzioni generali.
La presenza in organico di tecnici informatici esperti in ciascun Assessorato è l'elemento chiave che garantisce una risposta efficace ed efficiente alle quotidiane e caratteristiche esigenze delle strutture e che ha consentito nel tempo di definire livelli di risposta gestionale adeguati alle specificità e complessità dei processi trattati, in molti casi con l'adozione di soluzioni di buon livello che costituiscono un importante valore aggiunto della capacità operativa della RAS da salvaguardare e potenziare".

***

A livello di ripartizione delle **responsabilità di governance**, in particolare nell'ambito cybersecurity si descrivono i seguenti attori e ruoli:

1 Direzione Generale dell'Innovazione e Sicurezza IT

- definisce e pianifica la strategia di sicurezza (medio-lungo termine) dell'Amministrazione, definisce gli interventi e l'adozione delle misure tecniche atte a prevenire e contrastare, in termini uniformi per tutta l'Amministrazione regionale, i rischi connessi alla sicurezza informatica correlati alla tutela della Riservatezza, Integrità e Disponibilità dei dati personali, coordinando, limitatamente a tal fine, l'attività dell'Amministrazione regionale, specificando i propri ambiti di intervento e quelli che residuano, in materia, in capo alle altre strutture, in base a specifica delega definita dalla Deliberazione di Giunta regionale n. 45/3 del 20.12.2023 [2]. Distribuisce le risorse economiche di supporto per le iniziative inerenti alla sicurezza del Sistema di Gestione di Sicurezza delle Informazioni (SGSI). Inoltre, raccoglie, organizza e condivide informazioni sullo stato della sicurezza informatica (principalmente attraverso indicatori sintetici);

- supportata dai Servizi che la compongono, è responsabile di definire procedure/policy in materia di cybersecurity. Tuttavia, tali policy e procedure non hanno carattere vincolante per le Direzioni autonome della Federazione Unica che si trovano al di fuori del dominio RS.
- supportata dai Servizi che la compongono è responsabile dell'attività di verifica e controllo circa la corretta applicazione delle regole di sicurezza definite. Tuttavia, le Direzioni autonome della Federazione Unica che si trovano al di fuori del dominio RS hanno la facoltà di eseguire in autonomia tali attività;

- Il Direttore generale dell'Innovazione e Sicurezza IT e il Dirigente del Servizio Sicurezza IT, in qualità di responsabili IT dell'Amministrazione regionale, fanno parte integrante del gruppo di soggetti attivi coinvolti nella valutazione del rischio per gli interessati in caso di violazione dei dati personali che investa problematiche collegate alle loro competenze in base alla Deliberazione di Giunta regionale n. 45/3 del 20.12.2023;

- Cura la combinazione ottimale delle risorse umane definendo i ruoli e le responsabilità relativi alla sicurezza delle informazioni e agli altri aspetti organizzativi (es. contatti con gruppi specialistici, come CSIRT, Fornitori Security, CERT AgID, polizia postale, autorità..., con autorità...);
- Promuove e incoraggia la crescita professionale del personale della Regione tramite la pianificazione ed esecuzione di attività di training e campagne di awareness in ambito di sicurezza delle informazioni;
- Promuove il riesame e il monitoraggio, a intervalli pianificati, della sicurezza informatica dei sistemi dei fornitori di servizi IT e mitigazione dei rischi associati[2];
- Cura e promuove l'aggiornamento delle normative, delle politiche, delle procedure e degli standard di sicurezza;
- Promuove la realizzazione di una procedura sulla gestione degli incidenti di sicurezza (con o senza impatto sui dati personali) che disciplini la segnalazione, la raccolta, l'analisi, la gestione e il reporting;
- Gestisce la protezione fisica dei sistemi informatici strategici dell'Amministrazione, ospitati nel Data Center Regionale, contro calamità naturali, attacchi malevoli o accidentali;
- Protegge tramite appropriati controlli per l'ingresso i sistemi informatici strategici, ospitati nel Data Center Regionale, in modo da garantire l'accesso al solo personale autorizzato;
- Definisce le policy di protezione fisica e logica dei sistemi informatici dell'Organizzazione, definendo gli utenti, i loro ruoli e i permessi associati;
- Gestisce la protezione logica dei sistemi informatici di diretta responsabilità;
- Cura e promuove la gestione del ciclo di vita e dello sviluppo sicuro del software (SDLC);
- Promuove e definisce le policy per la manutenzione degli asset dell'Organizzazione attribuendo responsabilità e definendo criteri per la loro protezione e gestione;
- Coordina e promuove le attività di verifica per garantire una corretta attuazione delle leggi e dei regolamenti (nazionali e internazionali) applicabili alla sicurezza informatica;
- Assicura la raccolta delle informazioni relative alle minacce che possono impattare la sicurezza delle informazioni per individuare eventuali nuovi punti deboli all'interno dell'infrastruttura;
- Favorisce l'acquisizione, l'uso e la gestione dei servizi cloud in conformità con i requisiti di sicurezza definiti dall'Organizzazione;
- Verifica i cambiamenti dei processi IT, delle strutture di elaborazione delle informazioni e dei sistemi che potrebbero influenzare la sicurezza delle informazioni dell'Amministrazione;
- Collabora con il Coordinatore della gestione documentale della RAS incardinato nella Direzione Generale della Presidenza per la gestione dei cambiamenti in ambito documentale che potrebbero influenzare la sicurezza delle informazioni dell'Organizzazione;
- Svolge il coordinamento in materia di innovazione tecnologica e per le tecnologie dell'informazione e delle comunicazioni;

[2] TBD

- Assicura l’integrazione dei requisiti inerenti alla sicurezza delle informazioni all’interno dell’Organizzazione;
- Assicura che il Sistema di Gestione per la Sicurezza delle Informazioni consegua gli esiti previsti;
- Comunica l’importanza di un’efficace gestione della sicurezza delle informazioni e dell’essere conforme ai requisiti del SGSI;
- Revisiona, a intervalli pianificati, il Sistema di Gestione per la Sicurezza delle Informazioni dell’Organizzazione;
- Assicura la corretta implementazione delle misure fisiche e ambientali in linea alla norma ISO 27001, tra cui:
    - Definisce e usa i perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni;
    - Controlla e isola, dalle strutture di elaborazione delle informazioni, i punti di accesso come le aree di carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali.
- Collabora con gli organi di Direzione politica, esprimendo pareri, formulando proposte e fornendo le informazioni necessarie e utili per l’assunzione di decisioni e l’adozione di atti;
- Cura l'attuazione delle direttive generali, dei piani e dei programmi definiti dagli organi di Direzione politica; dirige, controlla e coordina l'attività dei Direttori dei Servizi e degli altri Dirigenti facenti capo alla Direzione generale, anche con potere sostitutivo in caso di inerzia.

2 Direzioni Generali RS ed extra RS

- Coordinano, nell’ambito della gestione dei fornitori, gli aspetti di sicurezza legati alle attività e ai servizi in outsourcing (contratti e requisiti di sicurezza, gestione SLA, monitoraggio, NDA...) consultando il Servizio Sicurezza IT (attività in carico ai CdR presenti in ogni Direzione Generale RS ed extra RS);
- Gestiscono gli aspetti di sicurezza legati alle attività e ai servizi in outsourcing (contratti e requisiti di sicurezza, gestione SLA, monitoraggio, NDA...) consultando il Servizio Sicurezza IT (attività in carico ai CdR presenti in ogni Direzione Generale RS ed extra RS);
- Definiscono la progettazione per le gare di competenza e ne curano l’attuazione e la gestione (attività in carico ai CdR presenti in ogni Direzione Generale RS ed extra RS).

2.1 Direzioni Generali RS

Le Direzioni Generali (si includono in questa definizione sia le Direzioni Generali in senso stretto che le Unità di Progetto e gli Uffici Speciali) presenti all’interno della Federazione Unica che operano su Dominio RS si occupano di:

- Collaborare con la Direzione generale dell’Innovazione e Sicurezza IT nella gestione dell’Active Directory per l’Unità Organizzativa di competenza;
- Gestire le Unità Organizzative del Dominio RS di propria competenza;

- Curare l’adozione e la gestione di un modello di Business Continuity (BIA, analisi dei rischi, piano di BC/Disaster Recovery, verifiche e test).

Inoltre, ereditano tutte le politiche di sicurezza generale fornite dalla Direzione generale dell’Innovazione e Sicurezza IT; le stesse politiche, per l’Unità Organizzativa di competenza, possono essere rese più stringenti dalle Direzioni Generali in base alle specifiche proprie esigenze, previa condivisione con la Direzione generale dell’Innovazione e Sicurezza IT.

2.2 Direzioni Generali extra RS

Direzioni Generali della Federazione Unica che si trovano al di fuori del Dominio RS e si occupano di:

- Provvedere autonomamente alla gestione degli aspetti di cybersecurity relativamente al proprio ambito di competenza, adeguandosi alla definizione degli interventi e all’adozione delle misure tecniche atte a prevenire e contrastare, in termini uniformi per tutta l’Amministrazione regionale, i rischi connessi alla sicurezza informatica correlati alla tutela della Riservatezza, Integrità e Disponibilità dei dati personali da parte della Direzione generale dell’Innovazione e Sicurezza IT che, limitatamente a tal fine, coordina l’attività dell’Amministrazione regionale, specificando i propri ambiti di intervento e quelli che residuano, in materia, in capo alle altre strutture in base a specifica delega definita dalla Deliberazione di Giunta regionale n. 45/3 del 20.12.2023;

- Recepire, se lo ritengono opportuno, le altre politiche di sicurezza generale fornite dalla Direzione generale dell’Innovazione e Sicurezza IT.

3 Servizio Agenda Digitale

- Collabora con la Direzione generale dell’Innovazione e Sicurezza IT per l’attuazione della strategia per la sicurezza delle informazioni;

- Coopera con il Servizio Sicurezza IT nella pianificazione ed esecuzione di attività di training e campagne di awareness in ambito di cybersecurity;

- Collabora con il Servizio Sicurezza IT per la definizione delle normative, delle politiche, delle procedure e degli standard di sicurezza;

- Nell’ambito del processo di Risk Management collabora con il Servizio Sicurezza IT per la gestione e la valutazione del rischio;

- Cura la definizione, l’adozione e la gestione della Business Continuity per il Data Center (BIA, analisi dei rischi, piano di BC/Disaster Recovery, verifiche e test);

- Collabora con le Direzioni Generali dominio RS per l’adozione e gestione di un modello di Business Continuity (BIA, analisi dei rischi, piano di BC/Disaster Recovery, verifiche e test);

- In ambito di Incident Management collabora con il Servizio Sicurezza IT per la gestione e la risoluzione degli incidenti di sicurezza;

- Gestisce gli aspetti inerenti alla sicurezza fisica delle infrastrutture (es. accessi fisici, sicurezza fisica per uffici, disegno stanze e strutture, videosorveglianza, protezione minacce fisiche e ambientali, guasti utenze di supporto, protezione cavi alimentazione e di rete, clear desk/screen);

- Collabora con il Servizio Sicurezza IT nella gestione degli aspetti inerenti alla sicurezza logica (ad es. firewalling, gestione IDS/IPS, anti-malware, patching, hardening…) delle infrastrutture IT;
- Collabora con il Servizio Sicurezza IT per la gestione delle autorizzazioni da rilasciare agli utenti (in conformità al ruolo ricoperto) per accedere al sistema;
- Si occupa di identificare e mantenere gli asset strategici (Data center) dell'Organizzazione, definendo responsabilità e procedure per la loro protezione e gestione. Inoltre, assicura che le informazioni, in essi trattate, ricevano un adeguato livello di protezione in linea con la loro importanza per l'Organizzazione;
- Gestisce i processi relativi all'acquisizione, l'uso, la gestione e l'uscita dai servizi cloud nel rispetto dei requisiti di sicurezza delle informazioni;
- Collabora con il Servizio Sicurezza IT per la gestione e il controllo dei cambiamenti dei processi IT, delle strutture di elaborazione delle informazioni e dei sistemi che potrebbero influenzare la sicurezza delle informazioni;
- Cura gli interventi per la realizzazione della rete telematica regionale e dei suoi sviluppi per la Pubblica Amministrazione;
- Gestisce il data center e il centro servizi regionale e ne progetta e mette in attuazione adeguamento tecnologico e sviluppi;
- Programma, in raccordo e secondo l'indirizzo del RTD e della Direzione generale, coordina, attua e comunica le azioni dell'Agenda Digitale per il sistema regione aventi impatto sulla collettività, sulle imprese e sulle Pubbliche Amministrazioni del territorio, curando la relativa attività amministrativa per gli interventi di competenza;
- Promuove l'equità digitale e la cittadinanza digitale e la fruizione di servizi pubblici online e mobile oriented;
- Promuove la partecipazione effettiva di cittadini e imprese al procedimento amministrativo per via elettronica;
- Cura lo sviluppo delle infrastrutture materiali per l'attività di polo strategico e di soggetto aggregatore – erogatore di servizi ICT in Sardegna;
- Cura la riprogettazione del sistema integrato dei portali della Regione secondo i principi della centralità dell'utente, dell'accessibilità, dell'usabilità, della responsività e della circolarità dei dati in possesso dell'Amministrazione Regionale;
- Rappresenta la regione nei tavoli di coordinamento con le altre regioni, con il governo, con l'Agenzia per l'Italia Digitale;
- Eroga i contributi ai cittadini emigrati per la partecipazione alle consultazioni elettorali;
- Favorisce l'utilizzo di sistemi di misurazione e valutazione della qualità dei servizi erogati e della reale soddisfazione dei cittadini e delle imprese;
- Supporta la Direzione generale nelle attività necessarie al raggiungimento della certificazione di qualità EN ISO 9000;
- Identifica, mappa e classifica i processi, promuove la diffusione delle competenze digitali;
- Promuove la realizzazione dell'osservatorio sull'innovazione;

- Promuove e diffonde le opportunità offerte dalle tecnologie digitali;
- Misura le ricadute delle azioni e degli strumenti regionali nel campo dell'innovazione;
- Favorisce la contaminazione e le partnership pubblico/private.

4 Servizio Sicurezza IT

- Coordina la realizzazione degli interventi e attività che mirano ad assicurare la protezione dei sistemi informatici a livello di disponibilità, riservatezza e integrità dei dati, ovvero tutte quelle attività che permettono di proteggere le infrastrutture telematiche dell'Amministrazione regionale aventi impatto sulla collettività, sulle imprese e sulle Pubbliche Amministrazioni del territorio. Gli interventi e l'adozione delle misure tecniche atte a prevenire e contrastare, in termini uniformi per tutta l'Amministrazione regionale, i rischi connessi alla sicurezza informatica correlati alla tutela della riservatezza, integrità e disponibilità dei dati personali, sono delegati specificamente alla Direzione generale dell'Innovazione e Sicurezza IT in base alla Deliberazione di Giunta regionale n. 45/3 del 20.12.2023 [2];
- Il Direttore generale dell'Innovazione e Sicurezza IT e il dirigente del Servizio Sicurezza IT, in qualità di responsabili IT dell'Amministrazione regionale, fanno parte integrante del gruppo di soggetti attivi coinvolti nella valutazione del rischio per gli interessati in caso di violazione dei dati personali che investa problematiche collegate alle loro competenze in base alla Deliberazione di Giunta regionale n. 45/3 del 20.12.2023 [2];
- Collabora con la Direzione generale dell'Innovazione e Sicurezza IT per l'attuazione della strategia per la sicurezza delle informazioni;
- Definisce e aggiorna i ruoli e le responsabilità relativi alla sicurezza delle informazioni e altri aspetti organizzativi (es. contatti con gruppi specialistici come CSIRT, Fornitori Security, CERT AgID, polizia postale, autorità...);
- Cura la tutela dei dati e dei sistemi informatici attraverso la definizione di policy indirizzate al personale IT;
- Esegue attività di training e campagne di awareness in ambito sicurezza delle informazioni;
- Collabora con i CDR per la gestione degli aspetti di sicurezza legati alle attività e ai servizi in outsourcing (contratti e requisiti di sicurezza, gestione SLA, monitoraggio, NDA...);
- Valuta e monitora la sicurezza dei fornitori di servizi IT e la mitigazione dei rischi a essi associati, in particolare per i servizi ad alto rischio, a seguito di analisi dei rischi;
- Fornisce le linee guida inerenti alla sicurezza delle informazioni (Es: gestione fornitori, sviluppo software sicuro, ecc.);
- Svolge il processo di Risk Management (analisi di contesto e analisi dei rischi che impattano sulla Sicurezza IT e individuazione e adozione delle necessarie misure di mitigazione).
- Collabora con il Servizio Agenda Digitale nell'attuazione del modello di Business Continuity per il Data Center (BIA, analisi dei rischi, piano di BC/Disaster Recovery, verifiche e test);
- Collabora con le Direzioni Generali dominio RS per l'adozione e gestione di un modello di Business Continuity (BIA, analisi dei rischi, piano di BC/Disaster Recovery, verifiche e test);

- Nell’ambito del processo di gestione degli incidenti di sicurezza occorsi all’interno del perimetro della RAS, effettua la classificazione dell’incidente di sicurezza ovvero procede ad attivare il “Comitato di crisi” ove le circostanze lo richiedano. Il Servizio Sicurezza IT altresì procede a effettuare le notifiche necessarie (Vertice Amministrativo RAS, CSIRT Italia) nonché implementa le azioni di contenimento/correttive di propria competenza. Il Servizio Sicurezza IT RAS, infine, procede con l’analisi post incidente al fine di rilevare possibili azioni di miglioramento (cd. lesson learned);
- Gestisce e coordina il CSIRT Regionale;
- Nell’ambito del processo di Real Time Security Monitoring supporta il Fornitore Security nelle attività di monitoraggio per gli ambiti di propria competenza;
- Collabora con il Servizio Agenda Digitale nella gestione degli aspetti inerenti alla sicurezza fisica delle infrastrutture della RAS;
- Monitora l’infrastruttura IT e i relativi aspetti di sicurezza sui sistemi (patching, hardening…);
- Si occupa della definizione, configurazione e gestione della sicurezza perimetrale (firewalling, gestione IDS/IPS, anti-malware...);
- Cura le attività tecniche inerenti all’implementazione e manutenzione di soluzioni di sicurezza (log management, backup, vulnerability management…);
- Cura il ciclo di vita delle utenze;
- Cura il processo di gestione delle nomine degli Amministratori di Sistema;
- Collabora con le Direzioni Generali Dominio RS per la gestione del ciclo di vita e dello sviluppo sicuro del software (SDLC);
- Collabora con il Servizio Agenda Digitale nell’assicurare che le informazioni presenti all’interno degli asset dell’Organizzazione ricevano un adeguato livello di protezione;
- Assicura la protezione degli asset dell’Organizzazione accessibili da parte dei fornitori;
- Pianifica attività di verifica per garantire una corretta attuazione delle leggi e dei regolamenti (nazionali e internazionali) applicabili alla sicurezza informatica;
- Coopera con le Direzioni Generali Dominio RS per assicurare la privacy e la protezione dei dati personali (mascheramento, misure di prevenzione per la perdita di dati...) come richiesto dalla legislazione e dai regolamenti in vigore;
- Identifica, raccoglie e analizza le informazioni relative alle minacce che possono impattare la sicurezza delle informazioni per individuare eventuali vulnerabilità all’interno dell’Amministrazione;
- Collabora con il Servizio Agenda Digitale per la definizione dei processi, l'acquisizione, l'uso, la gestione e l'uscita dai servizi cloud in conformità con i requisiti di sicurezza delle informazioni dell'Organizzazione;
- Approva i piani di progettazione delle change delle strutture di elaborazione delle informazioni e dei sistemi che potrebbero influenzare la sicurezza delle informazioni della RAS;
- Collabora con il Coordinatore della gestione documentale della RAS incardinato nella Direzione Generale della Presidenza per la gestione dei cambiamenti in ambito

documentale che potrebbero influenzare la sicurezza delle informazioni dell'Organizzazione;

- Progetta, sviluppa e gestisce i sistemi di sicurezza informatica a tutela dell'infrastruttura dell'Amministrazione regionale e definisce in merito unità di indirizzo alle altre strutture;
- Supporta la Direzione Generale e gli uffici dell'Amministrazione nella definizione, la predisposizione e gestione del piano per la sicurezza informatica dell'Amministrazione regionale;
- Attua le azioni del CAD e dell'Agenda Digitale dell'amministrazione regionale inerenti alla sicurezza informatica del cittadino e del territorio.

5 Servizio Sistemi

- Collabora con la Direzione generale dell'Innovazione e Sicurezza IT per l'attuazione della strategia per la sicurezza delle informazioni;
- Collabora con il Servizio Sicurezza IT nella gestione e valutazione del rischio;
- Collabora con il Servizio Agenda Digitale nell'adozione e gestione del modello di Business Continuity per il Data Center;
- In ambito di Incident Management collabora con il Servizio Sicurezza IT per la gestione e la risoluzione degli incidenti di sicurezza;
- Coopera con il Servizio Agenda Digitale nella gestione degli aspetti inerenti alla sicurezza fisica delle infrastrutture (es. accessi fisici, sicurezza fisica per uffici, disegno stanze e strutture, videosorveglianza, protezione minacce fisiche e ambientali, guasti utenze di supporto, protezione cavi alimentazione e di rete, clear desk/screen);
- Collabora con il Servizio Sicurezza IT per la gestione degli aspetti inerenti alla sicurezza logica (ad es. firewalling, gestione IDS/IPS, anti-malware, patching, hardening…) delle infrastrutture IT;
- Collabora con le Direzioni Generali Dominio RS per la gestione del ciclo di vita e dello sviluppo sicuro del software (SDLC);
- Coopera con il Servizio Sicurezza IT nell'assicurare che le informazioni presenti all'interno degli asset dell'Organizzazione ricevano un adeguato livello di protezione;
- Collabora con il Servizio Agenda Digitale per la definizione dei processi volti all'acquisizione, l'uso, la gestione e l'uscita dai servizi cloud in conformità con i requisiti di sicurezza delle informazioni dell'Organizzazione;
- Collabora con il Servizio Sicurezza IT per la gestione e il controllo dei cambiamenti dei processi IT, delle strutture di elaborazione delle informazioni e dei sistemi che potrebbero influenzare la sicurezza delle informazioni;
- Coordina la realizzazione e la gestione dei sistemi informativi trasversali di base e verticali per l'Amministrazione Regionale, gli Enti e le Agenzie Regionali e gli Enti Locali, con finanziamenti regionali, nazionali e comunitari;
- Coordina l'interoperabilità tra sistemi informativi;

- Definisce la progettazione per le gare di competenza e ne cura l'attuazione e la gestione di concerto con la Direzione CRC;
- Supporta la Direzione generale e gli uffici dell'Amministrazione nella definizione di linee guida e di indirizzi per l'attuazione del CAD e in materia di affidamenti in house;
- Attua la redazione e l'aggiornamento dei piani regionali per l'informatizzazione;
- Cura lo sviluppo delle infrastrutture immateriali per l'attività di polo strategico e di soggetto aggregatore-erogatore di servizi ICT in Sardegna secondo la pianificazione europea e nazionale;
- Attua le azioni dell'Agenda Digitale inerenti all'implementazione di servizi informatici per l'Amministrazione, i cittadini e le imprese, in raccordo con gli altri uffici regionali, compresa la relativa attività Amministrativa per gli interventi di competenza;
- Coordina e gestisce l'evoluzione normativa ICT dell'Amministrazione Regionale.

6 Servizio Tecnologia

- Collabora con la Direzione generale dell'Innovazione e Sicurezza IT per l'attuazione della strategia per la sicurezza delle informazioni;
- Collabora con il Servizio Sicurezza IT nella gestione e valutazione del rischio;
- Collabora con il Servizio Agenda Digitale nell'adozione e gestione del modello di Business Continuity per il Data Center;
- Collabora con il Servizio Sicurezza IT per la gestione e la risoluzione degli incidenti di sicurezza;
- Coopera con il Servizio Agenda Digitale nella gestione degli aspetti inerenti alla sicurezza fisica delle infrastrutture (es. accessi fisici, sicurezza fisica per uffici, disegno stanze e strutture, videosorveglianza, protezione minacce fisiche e ambientali, guasti utenze di supporto, protezione cavi alimentazione e di rete, clear desk/screen);
- Collabora con il Servizio Sicurezza IT nella gestione degli aspetti inerenti alla sicurezza logica (ad es. firewalling, gestione IDS/IPS, anti-malware, patching, hardening…) delle infrastrutture IT;
- Collabora con il Servizio Sicurezza IT per la gestione e il controllo dei cambiamenti dei processi IT, delle strutture di elaborazione delle informazioni e dei sistemi che potrebbero influenzare la sicurezza delle informazioni;
- Cura la realizzazione della banda ultra-larga;
- Cura la gestione della sicurezza dei server delle piattaforme di rete dei dati;
- Cura la gestione della posta elettronica standard e certificata;
- Cura le manutenzioni sulla banda ultra-larga;
- Cura la gestione finanziamenti per attivazione BUL;
- Gestisce i rapporti con organismi nazionali sul tema della realizzazione e gestione della banda ultra-larga.

7 Descrizione dell'infrastruttura data Center

L'infrastruttura data center CSR (Centro Servizi Regionale), di seguito denominata anche INFRA-DC-CSR, è un'infrastruttura di erogazione risorse data center condivise, costituita da un insieme eterogeneo di sistemi hardware e software che conferiscono le proprie caratteristiche e funzionalità ad una piattaforma di virtualizzazione che le integra e le orchestra.

Le risorse hardware e software conferite dai diversi sistemi appartenenti all'infrastruttura CSR, che sono integrate dalla piattaforma di virtualizzazione, vengono raggruppate da questa in sottoinsiemi definiti cluster, questi sono tecnologicamente omogenei e/o finalizzati ad uno scopo.

L'infrastruttura data center CSR per sua natura è costituita da risorse hardware e software conferite da molteplici sistemi, questi non sono amministrati da un unico gestore e amministratore bensì da diversi presidi tecnici, che ne detengono l'amministrazione sin dalla loro fornitura a cui era associato il servizio di gestione operativa.

Il presidio tecnico CSR-ICT Sistemi contrattualizzato dal Servizio Agenda Digitale, responsabile del Data Center Regionale, è identificato come gestore dell'infrastruttura data center CSR perché ha l'amministrazione della piattaforma di virtualizzazione, che integra e aggrega tutte le risorse conferite da molteplici sistemi hardware e software ognuno con un proprio gestore. È anche vero che il presidio tecnico CSR-ICT Sistemi oltre ad amministrare la piattaforma di virtualizzazione e anche il gestore della maggior parte dei sistemi hardware e software che conferiscono le proprie risorse all'infrastruttura data center CSR.

I sistemi hardware e software che conferiscono le proprie risorse all'infrastruttura data center CSR si trovano nel CED di Via Posada 1, questi però costituiscono solo un sottoinsieme dei sistemi presenti nei locali del suddetto CED.

I sistemi hardware e software principali che costituiscono l'infrastruttura data center CSR appartengono alle seguenti categorie: blade server, storage ibrido, storage all flash, storage capacitivo, apparati di rete san, apparati di rete lan, software di virtualizzazione data center e strumenti di monitoraggio, storage backup, software backup e sistemi operativi.

L'infrastruttura del data center CSR è stata implementata secondo un modello di architettura Converged Infrastructure. Lo scopo principale di questo approccio "convergente" è in generale ridurre la complessità di gestione del data center. I componenti di una Converged Infrastructure (sistemi server, unità di storage, apparati di networking, software di gestione e virtualizzazione) sono studiati per operare in maniera integrata e ottimizzata sin dall'inizio e questo permette di

risparmiare tempo e risorse sia nella fase di prima installazione sia nella gestione ordinaria quotidiana (Reference Architecture).

Aldilà della composizione tecnologica dell'infrastruttura data center CSR, è importante sottolineare come sulla base dei sistemi che la compongono e delle risorse condivise che vengono messe a disposizione degli utenti, sono presenti diversi livelli di amministrazione e delega di gestione dei sistemi o delle risorse condivise stesse.

La piattaforma di virtualizzazione è il sistema che aggrega e mette a fattor comune tutte le risorse che provengono da server blade, unità di storage, apparati di rete e sistema di backup. Il presidio CSR-ICT Sistemi è l'amministratore della piattaforma di virtualizzazione, che mette a disposizione degli utenti le risorse data center CSR .

È importante anche avere evidenza che il presidio CSR-ICT Sistemi non amministra tutti i sistemi che conferiscono risorse totalmente o in parte all'infrastruttura data center CSR, infatti ci sono sistemi server blade, unità di storage, apparati di rete e sistema di backup amministrati ad esempio dal presidio S-Cloud e da SardegnaIT che forniscono delle porzioni di risorse alla piattaforma di virtualizzazione per l'infrastruttura data center

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Nota: la polizza richiesta attraverso il presente questionario è una polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Si prega di leggere e compilare attentamente il seguente questionario.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Nominativo:	Fare clic qui per immettere testo.
Indirizzo:	Fare clic qui per immettere testo.
Sede legale:	Fare clic qui per immettere testo.
Telefono:	Fare clic qui per immettere testo.
Indirizzo Web:	Fare clic qui per immettere testo.

1.2 Numero di Dipendenti: Fare clic qui per immettere testo.

1.3 Si prega di allegare copia dell'ultimo bilancio

1.4 Si prega di indicare:

1.4.1 Budget spesa per la corrente annualità: Fare clic qui per immettere testo.

1.4.2 Numero di cittadini serviti: Fare clic qui per immettere testo.

1.4.3 Importo retribuzioni: Fare clic qui per immettere testo.

Sezione 2. Carte di Pagamento

2.1 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☐ NO☐

Se si:

2.1.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: Fare clic qui per immettere testo.

2.2 La proponente(se soggetta) è conforme alle vigenti norme di sicurezza emesse dalle istituzioni finanziarie con le quali è convenzionata (Payment Card industry Data Security Standards PCI DSS)?

NON SOGGETTA ☐
CONFORME ☐
NON CONFORME ☐

Se non conforme:

2.2.1 Si prega di descrivere lo stato attuale di qualsiasi opera di adeguamento e la relativa data di completamento prevista: Fare clic qui per immettere testo.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI☒ NO☐

3.2 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? SI☒ NO☐

3.3 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	☐	Fare clic qui per immettere testo.
Dati sensibili (Informazioni sanitarie)	☒	Fare clic qui per immettere testo.
Dati personali	☒	Fare clic qui per immettere testo.
Proprietà Intellettuale di Terzi	☐	Fare clic qui per immettere testo.
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La Proponente organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI☒ NO☐

Se si, si prega di indicare la frequenza di tali corsi: Annuale

4.2 La Proponente dispone di un:

Piano di disaster recovery	SI☐	NO☒
Piano di risposta alle intrusioni di rete e infezioni da virus	SI☒	NO☐

Se si dispone di uno o più dei sopra-citati documenti, *si prega di allegarne copia.*

4.3 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda? SI☒ NO☐

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Controlli di accesso alla rete	☒
Anti virus	☒
Firewall	☒
Rilevatori di intrusione	☒

4.5 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale SI☐ NO☒

4.6 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni? SI☐ NO☒

Se no, descrivere le procedure utilizzate dalla Proponente, se presenti, per archiviare o proteggere le copie dei dati importanti/sensibili fuori sede: Non sono presenti procedure.

4.7 La Proponente possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna? SI☐ NO☒

4.8 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? SI☒ NO☐

Se si:

4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio? SI☐ NO☐

4.9 La proponente utilizza esclusivamente sistemi operativi supportati e aggiornati dalla software house licenziante? SI☐ NO☒

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI☒ NO☐

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	☒
Raccolta dati e/o processo	☐
Call center / Service desk	☒
Operational business process	☐
Altro *(specificare sotto)*	☐

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	☒
Esternalizzati in Host	☐
Esternalizzati in Cloud	☐

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

5.3 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☐ NO☐

5.4 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT SI☒ NO☐

Sezione 6. Contenuti multimediali, Website e Social Network

6.1 La proponente dispone di una procedura di risposta ad eventuali accuse che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☐ NO☐

Sezione 7. Sinistri e circostanze

7.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☒ NO☐

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa: Data breach febbraio 2021

7.2 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta o? SI☒ NO☐

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o

per ricostruire i database o i software: Data breach febbraio 2021

7.3 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO☐

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

AVVISO IMPORTANTE

La persona autorizzata a sottoscrivere il presente questionario dichiara, ai sensi degli artt. 1892 e 1893 c.c., che, per quanto in sua conoscenza in relazione alle funzioni espletate, le affermazioni precedentemente riportate sono veritiere e che qualora insorgano modifiche tra la data di firma del presente e la data di entrata in vigore della copertura, egli darà immediata notifica di tali modifiche, e la società assicuratrice potrà ritirare oppure modificare la propria proposta e/o conferma di copertura. Il presente questionario ed ogni suo allegato possono essere parti integranti della polizza

Indicare nome e titolo della persona autorizzata a sottoscrivere in nome della Società Proponente.

Firmato: Fare clic qui per immettere testo.

Data: Fare clic qui per immettere testo.

DIREZIONE GENERALE DEI SERVIZI FINANZIARI

Active Directory DGBILANCIO

Il presente documento viene redatto ad integrazione della compilazione del “Questionario Cyber”, utile per il rinnovo della polizza Cyber della Regione Autonoma della Sardegna (RAS).

Il documento contiene una breve descrizione schematica della Microsoft Active Directory denominata “DGBILANCIO” con la quale è gestita una porzione degli uffici della RAS.

Descrizione generale

La Microsoft Active Directory (AD) DGBILANCIO è utilizzata per la gestione delle risorse relative a tre (3) diversi uffici dell’Assessorato della programmazione, bilancio, credito e assetto del territorio. La responsabilità della gestione ricade sul Settore Sistema informativo interno, appartenente al Servizio tecnico informatico per la contabilità integrata della Direzione generale dei servizi finanziari. La sede lavorativa degli uffici si trova in V. Cesare Battisti snc a Cagliari.

Uffici gestiti

Gli uffici gestiti tramite l’AD DGBILANCIO sono i seguenti:

- Direzione generale dei servizi finanziari.
- Ufficio di gabinetto dell’Assessore della programmazione, bilancio, credito e assetto del territorio.
- Unità di progetto Certificazione della Spesa dei fondi PO FESR FSE e FSC.

Risorse, servizi e dati

Le risorse gestite consistono in computer desktop, stampanti, gruppo di server su infrastruttura virtuale VMware. Le postazioni utente, corrispondenti a persone fisiche, attualmente gestite sono in numero di 148 (il numero può variare velocemente nel tempo ma ricade in quest’ordine di misura).

I server che reggono i servizi interni delle strutture nominate risiedono presso il Centro Servizi Regionale (CSR), il CED presente in V. Posada n.1 a Cagliari e gestito centralmente dalla Direzione generale della Innovazione e Sicurezza IT. Il Presidio Datacenter del CSR assicura l’esecuzione giornaliera e la conservazione dei backup della infrastruttura virtuale che regge la AD DGBILANCIO.

I servizi interni erogati dalla infrastruttura descritta consistono principalmente in:

- Autenticazione sulle postazioni di lavoro e sulle aree condivise;
- Installazione e configurazione dei sistemi operativi, delle interfacce di rete e degli applicativi delle postazioni di lavoro;
- Gestione di cartelle condivise (fruizione, gestione diritti di accesso in accordo con Responsabile/Titolare trattamento dati);
- Monitoraggio vulnerabilità (tramite strumento centralizzato) e gestione anomalie presenti su *dashboard* e segnalate dal Presidio Sicurezza (CSR);

I dati gestiti internamente tramite l’infrastruttura virtuale di server riguardano la documentazione amministrativa e archivi documentali a supporto delle attività degli uffici.

I dati principali dell’attività amministrativa sono fruiti dagli utenti accedendo ai sistemi centralizzati (SIBAR) relativi a: Documentale (Protocollo), Contabilità, HR.

Utilizzo dei servizi centralizzati

La maggior parte dei servizi utilizzati ha una gestione centralizzata presso il CSR.

I servizi principali sono i seguenti:

- Utilizzo di rete telematica (RTR) segmentata e monitorata con Firewall centrale;
- Posta elettronica istituzionale;
- Sistemi di Base (SIBAR) per la gestione documentale, contabile e del personale (HR);
- Protezione antivirus e anti-malware (server centrale EDR/XDR);
- Monitoraggio attivo e passivo vulnerabilità (server centrale di raccolta e analisi dei dati, server centrale di monitoraggio attivo con prove di intrusione

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Nota: la polizza richiesta attraverso il presente questionario è una polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Si prega di leggere e compilare attentamente il seguente questionario.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Nominativo:	Regione Autonoma della Sardegna - Active Directory DGBILANCIO
Indirizzo:	Via Cesare Battisti snc - Cagliari
Sede legale:	Viale Trento 69 - Cagliari
Telefono:	070.606.7000
Indirizzo Web:	https://www.regione.sardegna.it

1.2 Numero di Dipendenti: 153

1.3 Si prega di allegare copia dell'ultimo bilancio

1.4 Si prega di indicare:

1.4.1 Budget spesa per la corrente annualità: Fare clic qui per immettere testo.

1.4.2 Numero di cittadini serviti: Fare clic qui per immettere testo.

1.4.3 Importo retribuzioni: Fare clic qui per immettere testo.

Sezione 2. Carte di Pagamento

2.1 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☐ NO☐

Se si:

2.1.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: Fare clic qui per immettere testo.

2.2 La proponente(se soggetta) è conforme alle vigenti norme di sicurezza emesse dalle istituzioni finanziarie con le quali è convenzionata (Payment Card industry Data Security Standards PCI DSS)?

NON SOGGETTA ☐
CONFORME ☐
NON CONFORME ☐

Se non conforme:

2.2.1 Si prega di descrivere lo stato attuale di qualsiasi opera di adeguamento e la relativa data di completamento prevista: Fare clic qui per immettere testo.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI☒ NO☐

3.2 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? SI☒ NO☐

3.3 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	☒	Sistema SIBAR
Dati sensibili (Informazioni sanitarie)	☒	Sistema SIBAR
Dati personali	☒	SIBAR - Active Directory
Proprietà Intellettuale di Terzi	☐	Fare clic qui per immettere testo.
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La Proponente organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI☒ NO☐

Se si, si prega di indicare la frequenza di tali corsi: Organizzazione a livello centrale

4.2 La Proponente dispone di un:

Piano di disaster recovery	SI☐	NO☒
Piano di risposta alle intrusioni di rete e infezioni da virus	SI☐	NO☒

Se si dispone di uno o più dei sopra-citati documenti, *si prega di allegarne copia.*

4.3 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda? SI☒ NO☐

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Controlli di accesso alla rete	☒
Anti virus	☒
Firewall	☒
Rilevatori di intrusione	☐

4.5 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale SI☐ NO☒

4.6 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni? SI☐ NO☐

Se no, descrivere le procedure utilizzate dalla Proponente, se presenti, per archiviare o proteggere le copie dei dati importanti/sensibili fuori sede: Fare clic qui per immettere testo.

4.7 La Proponente possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna? SI☐ NO☒

4.8 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? SI☒ NO☐

Se si:

4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio? SI☐ NO☒

4.9 La proponente utilizza esclusivamente sistemi operativi supportati e aggiornati dalla software house licenziante? SI☒ NO☐

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI☒ NO☐

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	☒
Raccolta dati e/o processo	☐
Call center / Service desk	☐
Operational business process	☐
Altro *(specificare sotto)*	☐

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	☒
Esternalizzati in Host	☐
Esternalizzati in Cloud	☐

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

5.3 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☐ NO☐

5.4 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT SI☐ NO☐

Sezione 6. Contenuti multimediali, Website e Social Network

6.1 La proponente dispone di una procedura di risposta ad eventuali accuse che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☐ NO☐

Sezione 7. Sinistri e circostanze

7.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☒ NO☐

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa: incidente 2022 gestito a livello centrale dalla Dg Innovazione

---

7.2 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta o? SI☐ NO☒

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o

per ricostruire i database o i software: Fare clic qui per immettere testo.

7.3 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

AVVISO IMPORTANTE

La persona autorizzata a sottoscrivere il presente questionario dichiara, ai sensi degli artt. 1892 e 1893 c.c., che, per quanto in sua conoscenza in relazione alle funzioni espletate, le affermazioni precedentemente riportate sono veritiere e che qualora insorgano modifiche tra la data di firma del presente e la data di entrata in vigore della copertura, egli darà immediata notifica di tali modifiche, e la società assicuratrice potrà ritirare oppure modificare la propria proposta e/o conferma di copertura. Il presente questionario ed ogni suo allegato possono essere parti integranti della polizza

Indicare nome e titolo della persona autorizzata a sottoscrivere in nome della Società Proponente.

Firmato: Fare clic qui per immettere testo.

Data: Fare clic qui per immettere testo.

DIREZIONE GENERALE DEL LAVORO

Introduzione al questionario polizza assicurativa attacchi cyber

L'attività di gestione e governo delle infrastrutture IT dell'Assessorato del Lavoro si articola su due principali temi in parte sovrapposti:

- tutta l'infrastruttura IT – hardware e software – che permette ai circa 300 dipendenti di svolgere efficientemente le proprie attività;
- il sistema informativo del lavoro (SIL) della Sardegna.

La gestione delle risorse IT e del sistema informativo è svolta dal personale del *Settore gestione risorse IT e sistema informativo* incardinato nel *Servizio funzioni trasversali, sistema informativo e controlli di primo livello* della Direzione Generale del Lavoro.

L'infrastruttura IT dell'Assessorato del Lavoro

La *Direzione Generale del Lavoro, Formazione Professionale, Cooperazione e Sicurezza Sociale* è costituita da 12 sedi operative, di cui 2 sedi centrali nel comune di Cagliari e 9 sedi periferiche denominate *Centri Polifunzionali del Lavoro e Formazione* (nel seguito CPLF), con Infrastrutture di rete e sistemi ICT differenti e gestite da soggetti diversi.

Le due sedi centrali, site nel comune di Cagliari, e la sede di Oristano, sono completamente gestite dal personale dell'Assessorato al Lavoro, e tutte collegate alla RTR attraverso la quale raggiungono il Datacenter dell'Assessorato del Lavoro posizionato all'interno del Centro Servizi Regionale di Via Posada. L'infrastruttura IT è gestita attraverso un dominio dedicato denominato LAVORO a cui afferiscono 12 Server e 225 computer. Di seguito la tabella di riepilogo.

Sede	Numero PDL	Dominio	Indirizzo	RTR
CAGLIARI - Via San Simone	184	Lavoro	Via San Simone n° 60	si
CAGLIARI - Viale TRIESTE	31	Lavoro	Viale Trieste n° 115	si
Oristano – Via Madrid	10	Lavoro	Via Madrid n° 1	si

Nel dettaglio i 12 server che compongono il Dominio Lavoro sono dislocati presso il CSR di via Posada e gestiscono appunto i servizi di Dominio, ovvero l'autenticazione, la sincronizzazione con il Tenant LAVORO, la gestione delle stampe e l'inventario. A questi servizi si aggiungono i server JobPaghe e JobTime che gestiscono le buste paga e i cartellini dei dipendenti della ex Lista Speciale – Formazione Professionale.

Le restanti 9 sedi (CPLF), sono distribuite su tutto il territorio regionale e sono gestite dal punto di vista IT direttamente dalla Direzione Generale dell'Innovazione Tecnologica e Sicurezza IT. Tuttavia, benché tutte le sedi siano raggiunte dalla RTR solo le 2 sedi collegate in fibra ottica (Cagliari e Nuoro) risultano gestite attraverso il Dominio RS. Di seguito la tabella dei CPLF.

Sede	Numero Dipendenti	Dominio	Indirizzo	RTR
CAGLIARI MULINU BECCIU	24	RS	Via Piero della Francesca - Cagliari	Si
CARBONIA	35		Via Costituente n. 43 - Carbonia	Si
LANUSEI	3		Via Ilbono snc - Lanusei	Si
NUORO	15	RS	Via Ragazzi del '99 n. 60 - Nuoro	Si
OLBIA	2		Via Piemonte n. 27 - Olbia	Si
SAN GAVINO MONREALE	6		Via Roma n. 259 - San Gavino	Si
SASSARI - LA CRUCCA	22		Via Auzzas 1F Strada Prov.le La Crucca - Sassari	Si
SASSARI - SAN CAMILLO	4		Località Taniga S.S. 200 KM 4,500 - Sassari	Si
TONARA	2		Via S. Antonio n. 5 - Tonara	Si

Il SIL Sardegna

Il "SIL Sardegna" è la piattaforma applicativa della Regione Autonoma della Sardegna per la gestione e l'erogazione dei servizi pubblici per il lavoro e la formazione professionale, opera su una banca dati unica, accessibile, attraverso differenti canali, ed eroga servizi ai soggetti istituzionali competenti in materia di mercato del lavoro e formazione professionale, secondo i rispettivi ruoli, funzioni e compiti.

Il “SIL Sardegna”, conta circa 660.000 utenti registrati a vario titolo nel portale SardegnaLavoro www.sardegnalavoro.it e oltre 2.800.000 di anagrafiche di cittadini e imprese censiti nel portale MonitorWeb monitorweb.sardegnalavoro.it dedicato agli operatori della Pubblica Amministrazione.

Circa 2.100 operatori dislocati negli uffici territoriali del lavoro della Pubblica Amministrazione, profilati secondo ruoli definiti in funzione delle proprie competenze, utilizzano quotidianamente il “SIL Sardegna” per gli adempimenti amministrativi.

Gli **uffici pubblici** che operano quotidianamente sul “SIL Sardegna” fanno riferimento a:

- L’Assessorato del lavoro e formazione professionale, cooperazione e sicurezza sociale – RAS;
- L’Agenzia Sarda per le Politiche Attive del Lavoro – ASPAL;
- I Centri per l’Impiego ex CSL (29 sedi principali più 7 sedi decentrate) - CPI.
- La Direzione regionale del lavoro – Ministero del Lavoro e delle Politiche Sociali;
- La Presidenza, Ufficio Ispettivo – RAS;
- L’Assessorato della programmazione, bilancio, credito e assetto del territorio – Servizio autorità di certificazione, Centro regionale di programmazione – RAS;
- L’Assessorato della pubblica istruzione, beni culturali, informazione, spettacolo e sport – RAS;
- L’Assessorato dell’Igiene e Sanità e dell’Assistenza Sociale – RAS;

Il “SIL Sardegna”, in esercizio sull’intero territorio regionale dal 2004, è costituito da più sottosistemi specializzati che, grazie a tecnologie “web”, supporta la Pubblica Amministrazione, attraverso i servizi di *back office* monitorweb.sardegnalavoro.it, nello svolgimento delle funzioni e nell’erogazione dei servizi di loro competenza in materia di lavoro e formazione e agevola gli Utenti Privati (Cittadini, Datori di lavoro, Enti di Formazione, Soggetti Abilitati, Organizzazioni Sindacali, Soggetti Accreditati all’erogazione dei servizi per il lavoro, Enti Bilaterali e Cooperative Sociali) nell’accesso ai servizi lavoro sia per il tramite delle strutture presenti nel territorio, sia per il tramite del portale di *front office* www.sardegnalavoro.it.

Il SIL Sardegna è erogato attraverso Cloud Service Provider AWS; la gestione applicativa e operativa in cloud e l’evoluzione della piattaforma sono affidate a Fornitori esterni attraverso specifiche procedure di affidamento

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Nota: la polizza richiesta attraverso il presente questionario è una polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Si prega di leggere e compilare attentamente il seguente questionario.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Nominativo:	Fare clic qui per immettere testo.
Indirizzo:	Fare clic qui per immettere testo.
Sede legale:	Fare clic qui per immettere testo.
Telefono:	Fare clic qui per immettere testo.
Indirizzo Web:	Fare clic qui per immettere testo.

1.2 Numero di Dipendenti: Fare clic qui per immettere testo.

1.3 Si prega di allegare copia dell'ultimo bilancio

1.4 Si prega di indicare:

1.4.1 Budget spesa per la corrente annualità: Fare clic qui per immettere testo.

1.4.2 Numero di cittadini serviti: Fare clic qui per immettere testo.

1.4.3 Importo retribuzioni: Fare clic qui per immettere testo.

Sezione 2. Carte di Pagamento

2.1 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☐ NO☒

Se si:

2.1.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: Fare clic qui per immettere testo.

2.2 La proponente(se soggetta) è conforme alle vigenti norme di sicurezza emesse dalle istituzioni finanziarie con le quali è convenzionata (Payment Card industry Data Security Standards PCI DSS)?

NON SOGGETTA ☐
CONFORME ☐
NON CONFORME ☐

Se non conforme:

2.2.1 Si prega di descrivere lo stato attuale di qualsiasi opera di adeguamento e la relativa data di completamento prevista: Fare clic qui per immettere testo.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI☒ NO☐

3.2 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? SI☒ NO☐

3.3 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	☐	Fare clic qui per immettere testo.
Dati sensibili (Informazioni sanitarie)	☒	Fare clic qui per immettere testo.
Dati personali	☒	Fare clic qui per immettere testo.
Proprietà Intellettuale di Terzi	☐	Fare clic qui per immettere testo.
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La Proponente organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI☐ NO☒

Se si, si prega di indicare la frequenza di tali corsi: Fare clic qui per immettere testo.

4.2 La Proponente dispone di un:

Piano di disaster recovery	SI☐	NO☒
Piano di risposta alle intrusioni di rete e infezioni da virus	SI☐	NO☒

Se si dispone di uno o più dei sopra-citati documenti, *si prega di allegarne copia.*

4.3 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda? SI☒ NO☐

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Controlli di accesso alla rete	☐
Anti virus	☒
Firewall	☒
Rilevatori di intrusione	☐

4.5 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale SI☐ NO☐

4.6 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni? SI☐ NO☒

Se no, descrivere le procedure utilizzate dalla Proponente, se presenti, per archiviare o proteggere le copie dei dati importanti/sensibili fuori sede: Fare clic qui per immettere testo.

4.7 La Proponente possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna? SI☐ NO☒

4.8 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? SI☐ NO☒

Se si:

4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio? SI☐ NO☒

4.9 La proponente utilizza esclusivamente sistemi operativi supportati e aggiornati dalla software house licenziante? SI☒ NO☐

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI☐ NO☒

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	☐
Raccolta dati e/o processo	☐
Call center / Service desk	☐
Operational business process	☐
Altro *(specificare sotto)*	☐

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	☐
Esternalizzati in Host	☐
Esternalizzati in Cloud	☐

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

5.3 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☐ NO☐

5.4 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT SI☐ NO☐

Sezione 6. Contenuti multimediali, Website e Social Network

6.1 La proponente dispone di una procedura di risposta ad eventuali accuse che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☐ NO☒

Sezione 7. Sinistri e circostanze

7.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☐ NO☒

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa: Fare clic qui per immettere testo.

7.2 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta o? SI☐ NO☒

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o per ricostruire i database o i software: Fare clic qui per immettere testo.

7.3 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

AVVISO IMPORTANTE

La persona autorizzata a sottoscrivere il presente questionario dichiara, ai sensi degli artt. 1892 e 1893 c.c., che, per quanto in sua conoscenza in relazione alle funzioni espletate, le affermazioni precedentemente riportate sono veritiere e che qualora insorgano modifiche tra la data di firma del presente e la data di entrata in vigore della copertura, egli darà immediata notifica di tali modifiche, e la società assicuratrice potrà ritirare oppure modificare la propria proposta e/o conferma di copertura. Il presente questionario ed ogni suo allegato possono essere parti integranti della polizza

Indicare nome e titolo della persona autorizzata a sottoscrivere in nome della Società Proponente.

Firmato: Fare clic qui per immettere testo.

Data: Fare clic qui per immettere testo.

Infrastruttura informatica Direzione Generale del Personale e riforma della Regione

1. Introduzione

Con il presente documento si intende descrivere brevemente l'infrastruttura informatica della Direzione Generale del Personale e riforma della Regione.

2. Architettura infrastruttura

L'infrastruttura applicativa di tipo server-client è composta da 3 server fisici, **di cui un cluster formato da 2 nodi virtualizzati che insistono su uno storage condiviso a doppio controller** utilizzando il prodotto commerciale **VMware vSphere (Unix-based)**, per consolidare i carichi di lavoro e ottimizzare l'utilizzo delle risorse.

a. Server fisici

- Server HPE Proliant Gen 11 DL360
- Server HPE Proliant Gen 10 DL380
- Server HPE Proliant Gen 9 DL380

All'interno del server **HPE Proliant Gen 9 DL380** è attualmente installata la piattaforma Veeam Backup & Replication adottata per la realizzazione di backup automatizzati e l'implementazione di procedure di ripristino delle macchine virtuali presenti all'interno dell'infrastruttura.

Un server **QNAP TS-h1277XU-RP** all'interno del quale vengono salvati i backup delle **macchine virtuali** presenti all'interno del dominio della Direzione generale.

Su tutti i server suindicati è attivo il servizio di assistenza e manutenzione.

b. Macchine Virtuali

Attualmente il cluster contiene le 8 macchine virtuali che erogano i servizi ed i ruoli essenziali nel dominio (pers.local) su piattaforma Windows Server 2022:

- Domain controller primario e secondario
- File Server
- Print Server
- DHCP
- DFS
- WSUS
- Certification Authority

Oltre a quelle sopra richiamate, possiamo menzionare ulteriori macchine virtuali, tra cui:

- 2 per il monitoraggio (ManageEngine ADAudit Plus, Endpoint Central)
- 1 firewall software (pfSense)
- 2 web server e applicativi (Utility, help desk, fascicolo del personale, simulazioni di calcolo)

c. Antivirus e software per backup e monitoraggio

- **Antivirus e EDR**: È stata adottata la soluzione CrowdStrike, installata su tutte le postazioni desktop, per garantire protezione in tempo reale contro le minacce informatiche.
- **Backup e Ripristino**: Veeam Backup & Replication gestisce backup automatizzati su un server QNAP TS-h1277XU-RP e ripristini delle macchine virtuali.
- **Monitoraggio Active Directory**: ADAudit Plus monitora le modifiche nell'Active Directory, rilevando minacce interne e uso improprio dei privilegi. Effettua inoltre il monitoraggio gli accessi al File server e alle postazioni desktop dei colleghi
- **Gestione Endpoint**: Endpoint Central assicura una gestione centralizzata di tutti gli endpoint, automatizzando installazioni di patch e distribuzioni software.
- **Gestione degli accessi:** L'Active Directory gestisce l'autenticazione e l'autorizzazione degli utenti.

3. Infrastruttura di rete

L'infrastruttura di rete si sviluppa su 3 piani e la sala server, situata al secondo piano, è collegata tramite dorsali in fibra ottica e ospita l'infrastruttura fisica.

a. **Topologia:** La rete è a stella, con i server collocati in una sala server centrale.
b. **Cablaggio:** La rete è cablata con cavi Cat.6 e utilizza switch al Gb.
c. **Sicurezza:** Il firewall pfsense consente il tracciamento del traffico internet in uscita ed in ingresso alla rete locale, scartando il traffico malevolo aggiungendo un ulteriore layer di sicurezza rispetto ai firewall perimetrali di RTR.
d. **Continuità e protezione**: Il rack della sala server è dotato di un gruppo di continuità che assicura, per brevi periodi, la continuità dei servizi in caso di assenza della corrente elettrica.

4. Collegamento alla Rete Regionale

La rete locale interna della DG del Personale è collegata tramite un firewall software (pfSense) alla rete regionale. Gli accessi esterni avvengono tramite VPN RAS, che reindirizza il traffico al firewall interno. L'accesso dall'esterno alle postazioni desktop avviene mediante credenziali pers.local, aggiungendo un ulteriore SSO rispetto alle postazioni del dominio RS.

5. Business continuity e Disaster Recovery

È in corso la progettazione di un piano di disaster recovery e business continuity per garantire la continuità dei servizi in caso di guasti e/o incidenti. Il piano prevede la creazione di una sede secondaria con un'infrastruttura gemella per il ripristino rapido dei servizi e la realizzazione dei backup off site.

6. Postazioni desktop e Notebook

Attualmente su tutte le postazioni desktop dei colleghi (circa 155) è installato il sistema operativo Windows 11 aggiornato all'ultima versione. Vengono gestite in modo automatizzato l'introduzione delle patch di sicurezza.

I Notebook assegnati dalla Direzione ai colleghi che svolgono la propria attività in lavoro agile (smart working) utilizzano come strumento di protezione e sicurezza Windows Defender. Inoltre, sui portatili è abilitata la crittografia BitLocker per l'unità del sistema operativo e le unità fisse .[1] I portatili sono configurati in modo che l'utente abbia accesso alle sole funzioni necessarie per lo svolgimento delle attività lavorative.

[1] Si sta valutando l'opportunità di dotare ogni collega di un portatile aziendale di ultima generazione e installare su ciascuno l'antivirus CrowdStrike

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Nota: la polizza richiesta attraverso il presente questionario è una polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Si prega di leggere e compilare attentamente il seguente questionario.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Nominativo:	Fare clic qui per immettere testo.
Indirizzo:	Viale Trieste 190
Sede legale:	Fare clic qui per immettere testo.
Telefono:	Fare clic qui per immettere testo.
Indirizzo Web:	Fare clic qui per immettere testo.

1.2 Numero di Dipendenti: 135

1.3 Si prega di allegare copia dell'ultimo bilancio

1.4 Si prega di indicare:

1.4.1 Budget spesa per la corrente annualità: Fare clic qui per immettere testo.

1.4.2 Numero di cittadini serviti: Fare clic qui per immettere testo.

1.4.3 Importo retribuzioni: Fare clic qui per immettere testo.

Sezione 2. Carte di Pagamento

2.1 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☐ NO☐

Se si:

2.1.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: Gli unici pagamenti ricevuti sono relativi alle tasse di partecipazione ai concorsi, pagate dai candidati attraverso PagoPA Sardegna.

2.2 La proponente(se soggetta) è conforme alle vigenti norme di sicurezza emesse dalle istituzioni finanziarie con le quali è convenzionata (Payment Card industry Data Security Standards PCI DSS)?

NON SOGGETTA ☐
CONFORME ☐
NON CONFORME ☐

Se non conforme:

2.2.1 Si prega di descrivere lo stato attuale di qualsiasi opera di adeguamento e la relativa data di completamento prevista: Fare clic qui per immettere testo.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI☐ NO☐

3.2 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? SI☐ NO☐

3.3 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	☐	Fare clic qui per immettere testo.
Dati sensibili (Informazioni sanitarie)	☒	Impossibile quantificare
Dati personali	☒	Impossibile quantificare
Proprietà Intellettuale di Terzi	☒	Impossibile quantificare
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La Proponente organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI☐ NO☐

Se si, si prega di indicare la frequenza di tali corsi: I corsi sono gestiti dalla DG Innovazione

4.2 La Proponente dispone di un:

Piano di disaster recovery	SI☐	NO☒
Piano di risposta alle intrusioni di rete e infezioni da virus	SI☐	NO☒

Se si dispone di uno o più dei sopra-citati documenti, *si prega di allegarne copia.* Il piano di disaster recovery è in fase di progettazione.

4.3 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda? SI☒ NO☐

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Controlli di accesso alla rete	☒
Anti virus	☒
Firewall	☒
Rilevatori di intrusione	☒

I controlli sulla rete RTR vengono effettuata dalla DG Innovazione

4.5 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale SI☒ NO☐

Attualmente sui notebook è installato il firewall di windows. Si ha l'obiettivo di dotare tutti i portatili di CrowdStrike

4.6 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni? SI☐ NO☒

Abbiamo avviato interlocuzioni per individuzione sito secondario per backup

Se no, descrivere le procedure utilizzate dalla Proponente, se presenti, per archiviare o proteggere le copie dei dati importanti/sensibili fuori sede: Fare clic qui per immettere testo.

4.7 La Proponente possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna? SI☐ NO☒

4.8 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? SI☒ NO☐

Se si:

4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio? SI☒ NO☐

4.9 La proponente utilizza esclusivamente sistemi operativi supportati e aggiornati dalla software house licenziante? SI☐ NO☒

Tre Microsoft Windows (2 server e 1 client) e una linux (server). I server in questione ospitano applicativi compatibili solo con sistemi operativi superati e hanno accesso esclusivamente alla rete interna LAN

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI☐ NO☒

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	☐
Raccolta dati e/o processo	☐
Call center / Service desk	☐
Operational business process	☐
Altro *(specificare sotto)*	☐

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	☒
Esternalizzati in Host	☐

Esternalizzati in Cloud ☐

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

5.3 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☐ NO☐

5.4 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT SI☒ NO☐

Non è permesso ai fornitori l'accesso a dati privati o sensibili. L'accesso è consentito ai soli dipendenti della DG Personale

Sezione 6. Contenuti multimediali, Website e Social Network

6.1 La proponente dispone di una procedura di risposta ad eventuali accuse che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☐ NO☒

Sezione 7. Sinistri e circostanze

7.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☒ NO☐

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa:

7.2 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta o? SI☐ NO☐

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o per ricostruire i database o i software:

7.3 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO☐

Se si, si prega di fornire maggiori dettagli:

AVVISO IMPORTANTE

La persona autorizzata a sottoscrivere il presente questionario dichiara, ai sensi degli artt. 1892 e 1893 c.c., che, per quanto in sua conoscenza in relazione alle funzioni espletate, le affermazioni precedentemente riportate sono veritiere e che qualora insorgano modifiche tra la data di firma del presente e la data di entrata in vigore della copertura, egli darà immediata notifica di tali modifiche, e la società assicuratrice potrà ritirare oppure modificare la propria proposta e/o conferma di copertura. Il presente questionario ed ogni suo allegato possono essere parti integranti della polizza

Indicare nome e titolo della persona autorizzata a sottoscrivere in nome della Società Proponente.

Firmato: Fare clic qui per immettere testo.

Data: Fare clic qui per immettere testo.

DIREZIONE GENERALE DELLA SANITA'

Si è provveduto alla compilazione di 2 questionari distinti, uno relativo al dominio interno SANITA e l'altro relativo ai sistemi e servizi gestiti per il tramite della InHouse Sardegna IT o direttamente da fornitori esterni (SISaR), in ragione del fatto che la Direzione Generale della Sanità è titolare sia della gestione del proprio dominio (all'interno della rete telematica regionale) sia di sistemi e servizi a beneficio dei cittadini o degli enti del Servizio Sanitario Regionale.

Al fine di riscontrare la richiesta di fornire una breve introduzione descrittiva di contesto in relazione ai suddetti questionari, si provvede di seguito a illustrare sinteticamente l'oggetto degli ambiti sopra citati.

Dominio SANITA

La varietà e complessità dei processi gestiti dalla Regione nell'attuale modello organizzativo federato trova corrispondenza nell'organizzazione della sua infrastruttura ICT, come rappresentato nella DGR n. 24/27 del 14.05.2018, per cui la rete informatica della RAS è costituita da diversi domini autonomi presso alcune DDGG, gestiti dal proprio organico informatico, e da un dominio unico "Regione Sardegna" (RS) in cui confluiscono le altre DDGG non autonome, strutturate al suo interno come distinte Unità Organizzative (UO).

Il dominio SANITA, dell'Assessorato dell'igiene e sanità e dell'assistenza sociale, è uno dei domini autonomi ed è costituito da 3 UO ospitate nella medesima infrastruttura ICT ma funzionalmente distinte: Gabinetto, DG Sanità e DG Politiche Sociali.

Il dominio SANITA usufruisce, come tutti gli altri autonomi e RS, dei servizi generali gestiti dall'Assessorato degli affari generali, personale e riforma della Regione - Direzione generale dell'innovazione e Sicurezza IT (come, ad esempio, la rete telematica regionale, il sistema documentale, la posta elettronica, etc.) in quanto servizi funzionali alla gestione tecnico-amministrativa degli uffici dell'amministrazione regionale. Oltre ciò, in relazione alle specifiche attività d'istituto delle due direzioni generali (Sanità e Politiche sociali), tramite il dominio SANITA è gestito l'accesso ai sistemi esterni del SISaR, funzionali alle attività del Servizio Sanitario Regionale in capo alla InHouse SardegnaIT, sul cui dettaglio si specifica di seguito.

Il dominio SANITA, all'interno della rete telematica regionale, è subordinato alle policy ed ai sistemi di cyber security previsti per tutta l'amministrazione regionale, ma ne ha di ulteriori a maggior tutela dell' operatività e sicurezza della propria infrastruttura.

Sistemi e servizi gestiti per il tramite di Sardegna IT o direttamente di fornitori esterni

Il sistema informativo sanitario della Regione Sardegna è costituito da un insieme di sistemi informativi Integrati acquisiti dall'Amministrazione regionale a beneficio delle Aziende Sanitarie e dell'Assessorato dell' Igiene e Sanità e dell'Assistenza Sociale, di cui si citano, fra i principali, i sistemi: SISaR (Sistema Informativo Sanitario integrato Regionale), FSE - Fascicolo Sanitario Elettronico, ANAGS (Anagrafe Sanitaria) in corso di sostituzione col nuovo sistema Zente, SISM (Sistema informativo Salute Mentale), SIND Sistema Informativo dipendenze, NPIA Neuropsichiatria Infantile, SIRMES Sistema gestione rischio clinico, etc., e

rappresenta uno strumento essenziale per il governo clinico ed economico del servizio sanitario regionale nel suo complesso.
La Direzione Generale della Sanità è titolare fino al 30.06.2026 del contratto per la gestione e manutenzione del sistema informativo sanitario integrato regionale (SISaR). Il SISaR rappresenta il nucleo centrale del sistema informativo regionale sanitario. Esso è stato realizzato attraverso una specifica gara d' appalto pubblicata nel 2006 con avvio nel 2008. Dal 2008 ad oggi il sistema SISaR è stato sottoposto a numerose evoluzioni. Attualmente il SISaR è un sistema integrato di sottosistemi e moduli software gestionali a carattere sia amministrativo che clinico, pressoché omogeneo su tutto il territorio regionale, le cui funzionalità assicurano la copertura della maggioranza dei processi essenziali al funzionamento della sanità regionale. In particolare, il sistema SISaR è costituito dai seguenti principali moduli:

- AMC:Contabilità Generale, Contabilità Analitica, Controllo di Gestione, Approvvigionamenti: Acquisiti e Contratti,,Logistica: Magazzini/Farmaci, Richieste Approvvigionamento, Armadietto di Reparto, Gestione Attrezzature e Manutenzioni;
- HR: Trattamento Giuridico, Gestione Dotazione Organica, Gestione Economica e Contributiva, Gestione Presenze e Assenze (Rilevazione Presenze),Gestione Pensioni, Gestione Concorsi e Selezioni, Gestione Fondi, Dichiarazioni 770, Portale del Dipendente (Intranet del Personale SSR);
- Protocollo e Documentale:Protocollo Informatico, Atti Amministrativi, Gestione Documentale;
- SIO (Ospedaliero):Anagrafe;ADT e Liste di Attesa,Pronto Soccorso + OBI, Order Entry di Prestazioni, Sale Operatorie, Trasfusionale,SRC (ex CRCC);
- AAP (Territoriale):Consultorio, CSS Cartella Socio-Sanitaria, PUA, ADI, Medicina dello Sport, Medicina Legale, SPRESAL, SISP, SIAN, RSA, Protesica, Portale Prevenzione: Portale Notifica Preliminare dei Cantieri e Portale Amianto;
- CUP:CUP,E-Prescription,CUPWEB,Ambulatorio;
- DIR (Direzionale):Strumento ETL: Talend Open Studio, Flussi ETL,Datawarehouse,Strumento di BI: SpagoBI,Report ed Indicatori;
- EPI (Epidemiologico): CEDAP, RENCAM;
- SIDI:Sistema debito informativo;
- Accesso al Sistema e CDA: Sistema di accesso SSO, tramite CNS, produzione dei documenti sanitari firmabili digitalmente;
- Integrazioni: Integrazioni con Sistemi Terzi Regionali e Aziendali Non appartenenti alla Suite SISaR Fascicolo Sanitario Elettronico, SILUS, , RIS, A.P., etc.), Integrazioni intra-SISaR,Middleware di Integrazione.

Lo schema di deployment del sistema SISaR prevede sistemi installati centralmente presso il CSR della Regione Sardegna e altri invece installati presso i data center delle Aziende Sanitarie (c.d. installazioni

dipartimentali).In particolare:

- AMC: Centralizzato
- HR: Centralizzato
- Protocollo Informatico: Centralizzato
- Atti Amministrativi: Centralizzato
- Gestione Documentale: Centralizzato
- SIO (Ospedaliero) [trasfusionale ELIOT incluso]: Dipartimentale
-
- Monitor Pronto Soccorso: Centralizzato
- SRC: Centralizzato
- Anagrafe (XMPI): Centralizzata e Dipartimentale
- AAP (Territoriale: CSS, PUA, ADI, RSA, CONSULTORIO, PROTESICA; SPRESAL, SIAN, MEDICINA LEGALE): Dipartimentale
- Portale Prevenzione (NPC WEB e Portale Amianto): Centralizzato
- CUP:Centralizzato
- E-Prescription: Centralizzato
- CUPWEB: Centralizzato
- Cartella Clinica Ambulatoriale: Dipartimentale
- Cartella Clinica Ambulatoriale GM: Centralizzato
- DIR: Centralizzato
- CEDAP:Dipartimentale
- RENCAM: Centralizzato
- Sistema debito informativo (SIDI):Centralizzato
- Accesso al Sistema: Dipartimentale\Centralizzato
- Sistema di accesso SSO, tramite CNS, produzione dei documenti sanitari firmabili digitalmente: Dipartimentale\Centralizzato
- Integrazioni con Sistemi Terzi Non SISaR (Fascicolo Sanitario Elettronico, SILUS, etc.): Dipartimentale: FSE, SILUS, RIS, AP, INPS... / Centralizzato: ANAGS, Sistema Recall, SIBAR, Sistema di Conservazione, ...
- Middleware di Integrazione: Dipartimentale\Centralizzato

Per quanto concerne gli aspetti infrastrutturali e architetturali, attualmente i sistemi dipartimentali sono 11, corrispondenti alle 8 ASSL e alle 3 Aziende Ospedaliere. Il sistema poggia su un’infrastruttura cloud regionale, denominata H-CLOUD, gestita da un fornitore terzo contrattualizzato da Sardegna IT. Allo stato attuale, a seguito della riforma sanitaria di cui alla L.R. 24/2020 le Aziende del SSR configurate sul SISaR sono 13: 8 ASL, AOU Cagliari, AOU Sassari, ARNAS Brotzu, ARES, AREUS.

Allo stato attuale il SISaR è gestito in capo alla DG Sanità mediante il contratto "Art. 63, comma 5, D. lgs. n. 50/2016 e ss.mm.ii. – Procedura per l'affidamento della ripetizione di servizi analoghi dell'appalto SISAR 2.0 (CIG 7686214073 – CUP E77H18001780002) - servizi di gestione, manutenzione e reingegnerizzazione dell'architettura del sistema informativo sanitario integratoregionale (SISAR) e acquisizione dell'infrastruttura di integrazione", per brevità SISaR 2.0 Ripetizione Servizi Analoghi - CIG B0D5CEB987 - CUP E77H23003000002 -CUP PNRR E77H23001260002 (prot. n. 16743, Rep. serie Contratti n. 3, del13.06.2024), stipulato in data 13.06.2024 con Accenture S.p.A. in qualità dimandataria del RTI aggiudicatario dell'appalto, costituito con le mandanti Almaviva S.p.A. e Dedalus S.p.A..

La DG Sanità è inoltre titolare di una serie di altri servizi e sistemi gestiti per il tramite della società in house Sardegna IT. Le attività svolte da Sardegna IT all'interno dell'affidamento sottoscritto con la Direzione Generale della Sanità possono essere ricomprese nel seguente elenco non esaustivo:

- Reingegnerizzazione, manutenzione e gestione dei portali delle Aziende Sanitarie: realizzazione nuovi portali istituzionali per le Aziende sanitarie e relativa manutenzione e gestione (compresi gli esistenti);
- Servizio di supporto ed assistenza Help Desk (1° e 2° livello): servizio di supporto ed assistenza Help Desk (1° e 2° livello) per i sistemi informativi sanitari, rivolto ai cittadini ed agli operatori sanitari;
- Supporto Specialistico per il sistema SISaR: Team Supporto Operativo su SISaR, Gruppo di coordinamento CUP regionale;
- Servizi di Formazione, supporto e affiancamento per la messa a regime dei nuovi sistemi informativi sanitari o di nuove funzionalità implementate: formazione, supporto ed affiancamento agli operatori per il progetto SIRMES (Sistema Informativo per la Gestione del Rischio Clinico)
- Potenziamento infrastruttura tecnologica dei sistemi informativi sanitari: acquisizione forniture HW e SW potenziamento infrastruttura on premise per sistemi quali SISaR, ANAGS, MEDIR, etc;
- Piccole Manutenzioni evolutive dei sistemi informativi esistenti: manutenzioni evolutive di modesta entità sui sistemi informativi esistenti e sviluppo di nuovi sistemi ad hoc;
- Interventi per il completamento della Dematerializzazione delle prescrizioni: procedure per la manutenzione ed adeguamento dei software di cartella clinica dei medici di medicina generale e pediatri di libera scelta ai fini della dematerializzazione della ricetta farmaceutica e specialistica;
- Gestione operativa applicativa dei sistemi sanitari esistenti quali ANAGS, Anagrafiche SISaR, AXAN, Posta elettronica e PEC per le ASL, SIRMES;
- Gestione operativa sistemistica dei sistemi sanitari esistenti;
- Erogazione servizi specialistici, MAC e assistenza specialistica da parte di fornitori esterni: MAC e assistenza specialistica ANAGS, SIND – Salute Mentale, DRG e Analisi SDO, Servizio 1533, centralino regionale, Servizio di Conservazione a norma per le Aziende Sanitarie, Servizio PEC per le Aziende sanitarie, Manutenzione HW e SW sistemi informativi esistenti;
- Presa in carico e gestione operativa sistemistica nuovi sistemi informativi sanitari: Presa in carico e

gestione applicativa e sistemistica, Servizi sistemistici ad hoc per interventi evolutivi su HCLOUD e sistemi sanitari, Servizi sistemistici gestione infrastruttura H-Cloud;

- Supporto alla corretta gestione e governo del SISaR: Servizi professionali a supporto della corretta gestione ed il governo del SISaR;
- Servizi di consulenza specialistica in ambito e-HEALTH, ivi compreso gli aspetti di privacy e rispetto delle normative e linee guida nazionali ed internazionali: supporto sugli aspetti privacy in ambito di sanità elettronica, supporto consulenziale e specialistico all'Assessorato Sanità su attività strategiche in ambito di sanità elettronica, servizi di consulenza a supporto nella definizione del modello di governo del Sistema informativo Sanitario, alla luce della nuova struttura organizzativa del SSR;
- Servizi di Direzione dell'esecuzione del contratto per le procedure in corso e da realizzare: direzione dell'esecuzione contratto di gestione, manutenzione ed evoluzione del SISaR, attività di Direzione dell'Esecuzione del contratto per altri sistemi informativi sanitari (MEV, NPIA, SISM, Salute Penitenziaria, SW CC MMG, Conservazione a Norma, Telemedicina, Comunità terapeutiche, Registri, CRG, SARECM);
- Servizio di assistenza specialistica nella gestione delle postazioni di lavoro e l'infrastruttura tecnologica dell'Assessorato Sanità;
- Coordinamento e gestione del progetto;
- Servizi di supporto, assistenza, monitoraggio, tutoraggio rivolto agli operatori sanitari ed ai cittadini: fornitura Numeri Verdi per assistenza operatori sanitari e cittadini, presidio di Attivazione TS-CNS ed FSE presso fiere, eventi, presidi ospedalieri, ecc. e Supporto Attivazione Farmacie, divulgazione FSE, gestione sistemistica MEDIR;
- Realizzazione, evoluzione e gestione sistemi informativi complementari: evoluzione Anagrafe Regionale (ANAGS 2.0), servizi di redazione documentazione di gara, pubblicazione e Direzione esecuzione del contratto;
- Potenziamento infrastruttura hardware e software per il CUP e per i sistemi informativi complementari: acquisizione potenziamento infrastruttura HW e SW H-Cloud, redazione documentazione di gara e servizio di DEC;
- Interventi per favorire l'integrazione sul sistema CUP;
- Manutenzione evolutiva e Gestione Piattaforma "Gestione casi e contatti Covid-19";

Inoltre, in ambito PNRR:

- Adeguamenti al FSE 2.0, inerenti l'integrazione degli applicativi: adeguamenti applicativi SISaR, cartella clinica MMG e PLS ed altri applicativi sanitari (gestione farmacie, ambito ospedaliero, ambito di laboratorio, salute mentale e dipendenze, privati accreditati);
- Adeguamenti al FSE 2.0, inerenti l'infrastruttura ed i servizi digitali al cittadino ed ai professionisti;
- Servizi professionali per la gestione del FSE 2.0 e delle procedure per le acquisizioni esterne: redazione

documentazioni di gara e servizi di DEC dei contratti delle forniture esterne, attività di analisi e progettazione, servizio di accreditamento applicativi da integrare al FSE 2.0, servizi specialistici di attività sistemistiche e di sviluppo applicativo per la realizzazione del FSE 2.0:

- Project Management dell'Intervento;
- Formazione dei formatori per l'adozione e utilizzo del FSE 2.0: acquisizione servizi specialistici di formazione dei formatori sull'adozione ed utilizzo del FSE 2.0:
- Formazione degli stakeolder per l'adozione ed utilizzo del FSE 2.0.

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Si sono isolate solo le sezioni e i relativi quesiti che avessero la possibilità di essere gestiti autonomamente dal dominio in oggetto, escludendo gli aspetti non di competenza o risolvibili da altre strutture, direzioni.

Sezione 1. Informazioni generali sul dominio SANITA

1.1 Sede operativa c/o Assessorato Igiene, Sanità e Assistenza sociale
Sede fisica c/o Assessorato degli affari generali, personale e riforma della Regione - Direzione generale dell'innovazione e Sicurezza IT

Nominativo: **SANITA** – 3 UO distinte: Gabinetto, DG Sanità e DG Politiche Sociali
Indirizzo sede: Operativa Via Roma, 223 – 231 e 253 CAGLIARI Fisica Via Posada,1 CAGLIARI

1.2 Numero di utenti alla data di compilazione del presente questionario:

Complessivi registrati: **359**

Attivi negli ultimi 90gg: **239** (***10*** UO Gabinetto, ***148*** UO DG Sanità, ***81*** UO DG Politiche Sociali)

Sezione 3. Gestione delle esposizioni della privacy

3.1 La struttura è in possesso di una policy sulla privacy a livello aziendale?	**SI**
3.2 La struttura limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali?	**SI**

3.3 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	**NO**	
Dati sensibili (Informazioni sanitarie)	**SI**	Oltre alle informazioni e dati gestiti dagli uffici per altre linee di attività, nel caso dei flussi informativi sanitari, potenzialmente accesso a record riferibili a tutti coloro che sono o potrebbero essere potenziali utenti del SSR sia come assistibili, sia come destinatari di prestazioni sociali, sanitarie e socio-sanitaria erogate da strutture regionali o, se residenti, da strutture extra regione (nazionali e/o internazionali). Vedasi al riguardo il questionario SISaR (SardegnaIT).
Dati personali (Informazioni anagrafiche)	**SI**	
Proprietà intellettuali di terzi	**SI**	
Informazioni previdenziali	**SI**	
Coordinate bancarie	**SI**	

Sezione 4. Controlli dei sistemi informatici

4.1 La struttura organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? La struttura ha predisposto un Vademecum ed un'informativa consegnati assieme alle credenziali di primo accesso al dominio. Inoltre, la formazione in ambito di sicurezza informatica per i dipendenti RAS è in capo alla Direzione generale dell'innovazione e Sicurezza IT che veicola le proprie attività tramite gli amministratori di sicurezza della struttura e dominio Sanita.	**NO**

4.2 La struttura dispone di un:

Piano di disaster recovery	**NO**
Piano di risposta alle intrusioni di rete e infezioni da virus	**NO**

4.3 La struttura sospende tutti gli accessi ai computer e agli account quando un dipendente lascia l'azienda?	**SI**

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della struttura:

Controlli di accesso alla rete	Non gestiti direttamente
Anti virus	**SI**
Firewall	**SI** (aggiuntivo rispetto al perimetro RAS)
Rilevatori di intrusione	Funzioni integrate in Firewall e protezione degli endpoint

4.5.1 Indicare se i laptop siano o meno protetti da firewall personali.	**SI**
4.5.2 Indicare se i laptop possano connettersi solo tramite la rete aziendale.	**NO**
4.6 La struttura dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni?	

	Backup completo in altro rack-server presso il medesimo datacenter.
4.7 La struttura possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna?	**NO**
4.8 La struttura impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? Se si: 4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio?	**SI** **SI**
4.9 La struttura utilizza esclusivamente sistemi operativi supportati e aggiornati dalla software house licenziante?	**SI**

Sezione 5. Fornitori e Terze Parti

5.1 La struttura esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete?

SI

La Struttura si avvale di consulenze esterne a seguito di specifica contrattualizzazione per il supporto alla gestione della propria infrastruttura di dominio e dei servizi forniti dall'InHouse SardegnaIT.

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

IT Security	
Raccolta dati e/o processo	
Call center / Service desk	**SI**
Operational business process	
Managed Detection & Response di Sophos	**SI**

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	**SI**
Esternalizzati in Host	**NO**
Esternalizzati in Cloud	**NO**

5.2 La struttura esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

SI

5.3 La struttura richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi?	**SI**
5.4 Indicare se la struttura permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT	**SI,** attraverso porta di dominio gestita da farm di gateway di desktop remoto (Microsoft).

Sezione 7. Sinistri e circostanze

7.1 La struttura è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della struttura nei tre anni precedenti a questa richiesta?	**NO**
7.2 La struttura ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta?	**NO**
7.3 La struttura, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta?	**NO**

DIREZIONE GENERALE DELLE POLITICHE SOCIALI

Si è provveduto alla compilazione di 2 questionari distinti, uno relativo al dominio interno SANITA e l'altro relativo ai sistemi e servizi gestiti per il tramite della InHouse Sardegna IT o direttamente da fornitori esterni (SISaR), in ragione del fatto che la Direzione Generale delle Politiche Sociali è titolare sia della gestione del proprio dominio (all'interno della rete telematica regionale) sia di sistemi e servizi a beneficio dei cittadini o degli enti Regionali e del Servizio Sanitario.

Al fine di riscontrare la richiesta di fornire una breve introduzione descrittiva di contesto in relazione ai suddetti questionari, si provvede di seguito a illustrare sinteticamente l'oggetto degli ambiti sopra citati.

Dominio SANITA

La varietà e complessità dei processi gestiti dalla Regione nell'attuale modello organizzativo federato trova corrispondenza nell'organizzazione della sua infrastruttura ICT, come rappresentato nella DGR n. 24/27 del 14.05.2018, per cui la rete informatica della RAS è costituita da diversi domini autonomi presso alcune DDGG, gestiti dal proprio organico informatico, e da un dominio unico "Regione Sardegna" (RS) in cui confluiscono le altre DDGG non autonome, strutturate al suo interno come distinte Unità Organizzative (UO).

Il dominio SANITA, dell'Assessorato dell'igiene e sanità e dell'assistenza sociale, è uno dei domini autonomi ed è costituito da 3 UO ospitate nella medesima infrastruttura ICT ma funzionalmente distinte: Gabinetto, DG Sanità e DG Politiche Sociali.

Il dominio SANITA usufruisce, come tutti gli altri autonomi e RS, dei servizi generali gestiti dall'Assessorato degli affari generali, personale e riforma della Regione - Direzione generale dell'innovazione e Sicurezza IT (come, ad esempio, la rete telematica regionale, il sistema documentale, la posta elettronica, etc.) in quanto servizi funzionali alla gestione tecnico-amministrativa degli uffici dell'amministrazione regionale. Oltre ciò, in relazione alle specifiche attività d'istituto delle due direzioni generali (Sanità e Politiche sociali), tramite il dominio SANITA è gestito l'accesso ai sistemi esterni del SISaR, funzionali alle attività del Servizio Sanitario Regionale in capo alla InHouse SardegnaIT, sul cui dettaglio si specifica di seguito.

Il dominio SANITA, all'interno della rete telematica regionale, è subordinato alle policy ed ai sistemi di cyber security previsti per tutta l'amministrazione regionale, ma ne ha di ulteriori a maggior tutela dell' operatività e sicurezza della propria infrastruttura.

Sistemi e servizi gestiti per il tramite di Sardegna IT o direttamente di fornitori esterni

L’unica attività svolta da SardegnaIT all’interno dell’affidamento sottoscritto con la Direzione Generale delle Politiche Sociali è quella relativa al SIWE.

SIWE (sistema informativo integrato del welfare regionale) è un sistema per la raccolta e l’elaborazione di dati afferenti alle politiche regionali di welfare, che ha l'obiettivo di migliorare la conoscenza dei bisogni sociali, dell’offerta di servizi a valenza sociale, degli interventi attuati e dei finanziamenti erogati. E' uno strumento a supporto dell'attività amministrativa pensato per sostenere in via continuativa e senza interruzioni i processi di finanziamento e attuazione dei programmi regionali di inclusione sociale e per fornire ai diversi attori, pubblici e privati, a vario titolo coinvolti nelle fasi di programmazione, attuazione e monitoraggio delle politiche regionali di settore, una visione sempre più ampia e approfondita dei bisogni sociali della popolazione, degli interventi attuati e delle risorse economiche messe in campo.

L'incarico per lo sviluppo, gestione e manutenzione del sistema è affidato a Sardegna IT (scadenza incarico 31.12.2025).

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Si sono isolate solo le sezioni e i relativi quesiti che avessero la possibilità di essere gestiti autonomamente dal dominio in oggetto, escludendo gli aspetti non di competenza o risolvibili da altre strutture, direzioni.

Sezione 1. Informazioni generali sul dominio SANITA

1.1 Sede operativa c/o Assessorato Igiene, Sanità e Assistenza sociale
Sede fisica c/o Assessorato degli affari generali, personale e riforma della Regione - Direzione generale dell'innovazione e Sicurezza IT

Nominativo: **SANITA** – 3 UO distinte: Gabinetto, DG Sanità e DG Politiche Sociali
Indirizzo sede: Operativa Via Roma, 223 – 231 e 253 CAGLIARI Fisica Via Posada,1 CAGLIARI

1.2 Numero di utenti alla data di compilazione del presente questionario:

Complessivi registrati: **359**

Attivi negli ultimi 90gg: **239** (***10*** UO Gabinetto, ***148*** UO DG Sanità, ***81*** UO DG Politiche Sociali)

Sezione 3. Gestione delle esposizioni della privacy

3.1	**La struttura è in possesso di una policy sulla privacy a livello aziendale?**	**SI**
3.2	**La struttura limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali?**	**SI**

3.3 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	**NO**	
Dati sensibili (Informazioni sanitarie)	**SI**	Oltre alle informazioni e dati gestiti dagli uffici per altre linee di attività, nel caso dei flussi informativi sanitari, potenzialmente accesso a record riferibili a tutti coloro che sono o potrebbero essere potenziali utenti del SSR sia come assistibili, sia come destinatari di prestazioni sociali, sanitarie e socio-sanitaria erogate da strutture regionali o, se residenti, da strutture extra regione (nazionali e/o internazionali). Vedasi al riguardo il questionario SISaR (SardegnaIT).
Dati personali (Informazioni anagrafiche)	**SI**	
Proprietà intellettuali di terzi	**SI**	
Informazioni previdenziali	**SI**	
Coordinate bancarie	**SI**	

Sezione 4. Controlli dei sistemi informatici

4.1 La struttura organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? La struttura ha predisposto un Vademecum ed un'informativa consegnati assieme alle credenziali di primo accesso al dominio. Inoltre, la formazione in ambito di sicurezza informatica per i dipendenti RAS è in capo alla Direzione generale dell'innovazione e Sicurezza IT che veicola le proprie attività tramite gli amministratori di sicurezza della struttura e dominio Sanita.	**NO**

4.2 La struttura dispone di un:

Piano di disaster recovery	**NO**
Piano di risposta alle intrusioni di rete e infezioni da virus	**NO**

4.3 La struttura sospende tutti gli accessi ai computer e agli account quando un dipendente lascia l'azienda?	**SI**

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della struttura:

Controlli di accesso alla rete	Non gestiti direttamente
Anti virus	**SI**
Firewall	**SI** (aggiuntivo rispetto al perimetro RAS)
Rilevatori di intrusione	Funzioni integrate in Firewall e protezione degli endpoint

4.5.1 Indicare se i laptop siano o meno protetti da firewall personali.	**SI**
4.5.2 Indicare se i laptop possano connettersi solo tramite la rete aziendale.	**NO**
4.6 La struttura dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni?	

	Backup completo in altro rack-server presso il medesimo datacenter.
4.7 La struttura possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna?	**NO**
4.8 La struttura impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? Se si: 4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio?	**SI** **SI**
4.9 La struttura utilizza esclusivamente sistemi operativi supportati e aggiornati dalla software house licenziante?	**SI**

Sezione 5. Fornitori e Terze Parti

5.1 La struttura esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete?

SI

La Struttura si avvale di consulenze esterne a seguito di specifica contrattualizzazione per il supporto alla gestione della propria infrastruttura di dominio e dei servizi forniti dall'InHouse SardegnaIT.

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

IT Security	
Raccolta dati e/o processo	
Call center / Service desk	**SI**
Operational business process	
Managed Detection & Response di Sophos	**SI**

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	**SI**
Esternalizzati in Host	**NO**
Esternalizzati in Cloud	**NO**

5.2 La struttura esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

SI

5.3 La struttura richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi?	**SI**
5.4 Indicare se la struttura permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT	**SI,** attraverso porta di dominio gestita da farm di gateway di desktop remoto (Microsoft).

Sezione 7. Sinistri e circostanze

7.1 La struttura è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della struttura nei tre anni precedenti a questa richiesta?	**NO**
7.2 La struttura ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta?	**NO**
7.3 La struttura, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta?	**NO**

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Nota: la polizza richiesta attraverso il presente questionario è una polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Si prega di leggere e compilare attentamente il seguente questionario.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Nominativo:	Sardegna IT S.r.l.
Indirizzo:	Via dei Giornalisti n.6, 09122 Cagliari
Sede legale:	Via dei Giornalisti n.6, 09122 Cagliari
Telefono:	070 606 9015
Indirizzo Web:	https://www.sardegnait.it

1.2 Numero di Dipendenti: 120

1.3 Si prega di allegare copia dell'ultimo bilancio

1.4 Si prega di indicare:

1.4.1 Budget spesa per la corrente annualità: Fare clic qui per immettere testo.

1.4.2 Numero di cittadini serviti: Fare clic qui per immettere testo.

1.4.3 Importo retribuzioni: Fare clic qui per immettere testo.

Sezione 2. Carte di Pagamento

2.1 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☐ NO☐

Se si:

2.1.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: Fare clic qui per immettere testo.

2.2 La proponente(se soggetta) è conforme alle vigenti norme di sicurezza emesse dalle istituzioni finanziarie con le quali è convenzionata (Payment Card industry Data Security Standards PCI DSS)?

NON SOGGETTA ☒
CONFORME ☐
NON CONFORME ☐

Se non conforme:

2.2.1 Si prega di descrivere lo stato attuale di qualsiasi opera di adeguamento e la relativa data di completamento prevista: Fare clic qui per immettere testo.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI☒ NO☐

3.2 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? SI☒ NO☐

3.3 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	☐	Fare clic qui per immettere testo.
Dati sensibili (Informazioni sanitarie)	☒	1.600.000
Dati personali	☒	1.600.000
Proprietà Intellettuale di Terzi	☐	Fare clic qui per immettere testo.
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La Proponente organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI☒ NO☐

Se si, si prega di indicare la frequenza di tali corsi: annuale

4.2 La Proponente dispone di un:

Piano di disaster recovery	SI☒	NO☐
Piano di risposta alle intrusioni di rete e infezioni da virus	SI☐	NO☒

Se si dispone di uno o più dei sopra-citati documenti, *si prega di allegarne copia.*

4.3 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda? SI☒ NO☐

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Controlli di accesso alla rete	☒
Anti virus	☒
Firewall	☒
Rilevatori di intrusione	☐

4.5 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale SI☐ NO☒

4.6 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni? SI☐ NO☒

Se no, descrivere le procedure utilizzate dalla Proponente, se presenti, per archiviare o proteggere le copie dei dati importanti/sensibili fuori sede: Fare clic qui per immettere testo.

4.7 La Proponente possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna? SI☐ NO☒

4.8 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? SI☐ NO☒

Se si:

4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio? SI☐ NO☒

4.9 La proponente utilizza esclusivamente sistemi operativi supportati e aggiornati dalla software house licenziante? SI☐ NO☒

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI☐ NO☒

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	☐
Raccolta dati e/o processo	☐
Call center / Service desk	☐
Operational business process	☐
Altro *(specificare sotto)*	☐

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	☐
Esternalizzati in Host	☐
Esternalizzati in Cloud	☐

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate?

5.3 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☐ NO☒

5.4 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT SI☒ NO☐

Sezione 6. Contenuti multimediali, Website e Social Network

6.1 La proponente dispone di una procedura di risposta ad eventuali accuse che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☐ NO☒

Sezione 7. Sinistri e circostanze

7.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☐ NO☒

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa: Fare clic qui per immettere testo.

7.2 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta o? SI☐ NO☒

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o per ricostruire i database o i software: Fare clic qui per immettere testo.

7.3 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

AVVISO IMPORTANTE

La persona autorizzata a sottoscrivere il presente questionario dichiara, ai sensi degli artt. 1892 e 1893 c.c., che, per quanto in sua conoscenza in relazione alle funzioni espletate, le affermazioni precedentemente riportate sono veritiere e che qualora insorgano modifiche tra la data di firma del presente e la data di entrata in vigore della copertura, egli darà immediata notifica di tali modifiche, e la società assicuratrice potrà ritirare oppure modificare la propria proposta e/o conferma di copertura. Il presente questionario ed ogni suo allegato possono essere parti integranti della polizza

Indicare nome e titolo della persona autorizzata a sottoscrivere in nome della Società Proponente.

Firmato: Fare clic qui per immettere testo.

Data: Fare clic qui per immettere testo.