

 AZIENDA TUTELA DELLA SALUTE LIGURIA	CENTRALE REGIONALE DI ACQUISTO PER LA SANITA' Tel.: 010 5488541 email: direzione.areals@atsliguria.it	 AREA LIGURIA SALUTE
--	---	--

Dirigente Responsabile:
 Dott. Giorgio Sacco- tel. 010/5488560
 e-mail: giorgio.sacco@regione.liguria.it
 Funzionario referente:
 Dott. David Burlando - tel. 010/5488565
 e-mail: david.burlando@regione.liguria.it

1

Oggetto: Procedura di gara aperta ai sensi dell'art. 71 D.Lgs. n. 36/2023, svolta attraverso la piattaforma telematica Sintel, per l'affidamento dei servizi assicurativi - occorrenti ad ATSL, AOM, EE.OO. e I.R.C.C.S. della Regione Liguria per un periodo di 60 mesi con opzione di proroga contrattuale per ulteriori 6 mesi. Lotti 2. ID SINTEL: 220913765.

RISPOSTE A RICHIESTE CHIARIMENTI PERVENUTI A TUTTO IL 13/07/2026

Quesito n. 18

Relativamente al lotto 2 Cyber Risk si richiedono i chiarimenti di seguito riportati:

- Indicare termini e condizioni in corso con attuale assicuratore (premio lordo annuo, massimali per garanzia, franchigie/scoperti).

-ASL 1:

o Nel questionario non risultano formalizzati Business Continuity Plan, Disaster Recovery Plan e Incident Response Plan. Si chiede di fornire un aggiornamento sul livello di implementazione di tali presidi e sulle iniziative eventualmente intraprese negli ultimi anni in materia di resilienza operativa.

o Considerata l'assenza di una funzione CISO formalmente indicata nel questionario, si chiede di descrivere l'attuale modello organizzativo adottato per la governance della sicurezza informatica.

- ASL 2:

o Quando sono stati testati l'ultima volta i backup?

o Si chiede di fornire maggior dettaglio in merito alle misure adottate per la segmentazione degli ambienti clinici, amministrativi e biomedicali.

o Con riferimento alla gestione degli accessi privilegiati, si chiede di fornire maggior dettaglio sulle misure adottate per il controllo, il monitoraggio e la revisione periodica dei privilegi amministrativi, inclusi quelli attribuiti a fornitori e soggetti terzi.

- ASL 3:

o Nel questionario non risultano formalizzati Business Continuity Plan e Disaster Recovery Plan. Si chiede di fornire un aggiornamento sul livello di implementazione di tali presidi e sulle iniziative eventualmente intraprese negli ultimi anni in materia di resilienza operativa.

o Si chiede di fornire maggior dettaglio sulle misure adottate per la protezione degli accessi remoti e degli account privilegiati e quando verrà implementata l'MFA.

- ASL 4:

o Nel questionario non risultano formalizzati alcuni presidi di continuità operativa. Si chiede di fornire un aggiornamento sulle iniziative eventualmente intraprese per rafforzare Business Continuity e Disaster Recovery.

o Si chiede di fornire maggior dettaglio sulle attività di vulnerability assessment, penetration test e monitoraggio continuativo della sicurezza eventualmente svolte (nel questionario non è presente la risposta).

- ASL 5:

o Nel questionario non risultano formalizzati Business Continuity Plan, Disaster Recovery Plan e incident response plan. Si chiede di fornire un aggiornamento sul livello di implementazione di tali presidi e sulle iniziative eventualmente intraprese negli ultimi anni in materia di resilienza operativa.

o Si chiede di fornire maggior dettaglio sulle attività di vulnerability assessment, penetration test e monitoraggio continuativo della sicurezza eventualmente svolte.

o Con riferimento alle attività di formazione e sensibilizzazione del personale sui rischi cyber, si chiede di fornire maggior dettaglio sulle iniziative attualmente svolte, sulla relativa periodicità e sull'eventuale utilizzo di campagne di phishing simulato o analoghe attività di awareness. Attualmente sul questionario è stato indicato "no" come risposta.

- Evangelico:

o Si chiede di descrivere le misure adottate per la gestione degli accessi privilegiati e la protezione delle infrastrutture critiche.

o Non risultano criptati i backup: si chiede, pertanto, di fornire maggior dettaglio sulle misure adottate per garantirne riservatezza, integrità e protezione rispetto a eventi cyber, nonché sugli eventuali interventi di rafforzamento pianificati o recentemente implementati.

- A.O Metropolitana:

o Si chiede di fornire un riscontro alle domande 19,20,21,22,23 del questionario.

 ATS LIGURIA AZIENDA TUTELA DELLA SALUTE LIGURIA	CENTRALE REGIONALE DI ACQUISTO PER LA SANITA' Tel.: 010 5488541 email: direzione.areals@atsliguria.it	 Liguria Salute AREA LIGURIA SALUTE
---	---	--

o Nel questionario non risultano formalizzati Business Continuity Plan, Disaster Recovery Plan e incident response plan. Si chiede di fornire un aggiornamento sul livello di implementazione di tali presidi e sulle iniziative eventualmente intraprese negli ultimi anni in materia di resilienza operativa.

o Si chiede di fornire maggior dettaglio sulle misure adottate per la protezione degli accessi remoti e degli account privilegiati e quando verrà implementata l'MFA

- Gaslini:

o Si chiede di inviare il questionario relativo alla postura di sicurezza informatica. Il documento caricato non è relativo ad un risk assessment.

-Area Liguria Salute:

o Nel questionario non risultano formalizzati Business Continuity Plan, Disaster Recovery Plan e incident response plan. Si chiede di fornire un aggiornamento sul livello di implementazione di tali presidi e sulle iniziative eventualmente intraprese negli ultimi anni in materia di resilienza operativa.

o Si chiede di fornire maggior dettaglio sulle misure adottate per la protezione degli accessi remoti e degli account privilegiati e quando verrà implementata l'MFA.

o Sono mai state effettuate simulazioni di phishing?

- Galliera:

o Con riferimento alla presenza dichiarata di sistemi e componenti non più supportati dal produttore, si chiede di fornire maggior dettaglio circa la tipologia degli asset coinvolti, la relativa esposizione al rischio cyber e le principali misure compensative adottate.

o Con riferimento all'evento di Business Email Compromise occorso tra il 2022 e il 2023, si chiede di fornire un aggiornamento sulle principali misure organizzative e tecnologiche introdotte successivamente all'evento e sul relativo stato di attuazione.

o Considerata l'assenza di una figura CISO formalmente individuata, si chiede di descrivere sinteticamente il modello di governance adottato per il coordinamento delle attività di cybersecurity e gestione del rischio cyber.

Risposta

Premio annuo lordo € 331.985,41, Franchigia per perdita € 100.000.

ASL 1

- E' stata definita una procedura per la continuità operativa dei servizi in assenza di strumenti informatici. Il Disaster Recovery è implementato sui sistemi di Laboratorio e PACS ed è ora attivabile anche sugli altri servizi critici dell'azienda (previa identificazione delle risorse economiche per l'acquisizione del servizio ad oggi non disponibili) a seguito dell'avvenuto completamento delle migrazioni in IaaS dei sistemi presso il Data Center di Liguria Digitale, certificato ACN, che hanno permesso di elevare ulteriormente il livello di affidabilità,

ridondanza, disponibilità e resilienza dei sistemi. A seguito della fusione degli enti dell'SSR in ATSL, in relazione al nuovo POA in via di definizione, tutta l'infrastruttura tecnologica e applicativa sarà oggetto di revisione, omogeneizzazione e riorganizzazione. Saranno altresì rifinite le politiche di sicurezza, di governo e di gestione che includeranno anche le politiche Business Continuity Plan, Disaster Recovery Plan e Incident Response Plan.

- Il CISO è una figura presente all'interno del SOC di Liguria Digitale attraverso il quale l'ente ha stipulato un contratto per la fornitura di servizi di cybersicurezza. Il SOC di Liguria Digitale opera in raccordo con il personale tecnico dei Sistemi Informativi di Area1, e si appoggia agli strumenti di cybersicurezza presenti nell'Area a livello di endpoint e sistemi (antivirus, firewall, xdr, ndr, antispam, SIEM, NAC, ecc.).

ASL 2

- I test sui backup sono in carico al fornitore del cloud e IAAS (Liguria Digitale), le copie dei backup vengono correntemente utilizzate dai sistemisti SIA per migrazioni, restore e passaggi dati e quindi frequentemente verificate.
- I vari ambienti sono segmentati logicamente attraverso l'uso delle VLAN
- Le utenze privilegiate vengono fornite solo su specifica e motivata richiesta e sono limitate ai soli sistemi di interesse e per il tempo necessario (es. fornitori esterni). Per quanto riguarda le utenze amministrative, sono incaricati unicamente gli amministratori di sistema del SIA, che dispongono di specifiche utenze amministrative distinte che vengono regolarmente revisionate e controllate.

ASL 4

- **Al momento, complice la fusione, non sono state implementate ulteriori iniziative. I server sono ospitati nel datacenter di LD, certificato da AgID come cloud provider e in possesso di tutti i requisiti per la realizzazione di bandi PNRR**
- **Attualmente le attività di vulnerability assessment sono sospese per cambio di tecnologia. Per quanto riguarda il monitoraggio della sicurezza sono presenti e attivi (come indicato nel questionario) sistemi XDR ed EDR per monitoraggio continuo e proattivo dei server e delle postazioni di lavoro**

ASL 5

- Area5 si colloca nella nuova realtà ATSL di recente costituzione. In assenza di un Atto Aziendale è molto difficile redigere procedure. Area 5 non ha provveduto alla redazione dei suddetti piani. Area 5 ha aderito all'opzione DR dell'offerta cloud di Liguria Digitale. Tale prestazione è in corso di attivazione con il contributo del fornitore di servizi di outsourcing. La stesura delle procedure potrà avvenire quando vi sarà maggior chiarezza sull'assetto organizzativo. Liguria Digitale fornirà indicazioni metodologiche e supporto nella redazione nei limiti delle forniture in essere.
- Area 5 dispone di un monitoraggio continuativo basato sul prodotto Cynet e i servizi di SOC di Liguria Digitale. Le attività di VA sono state realizzate sui principali segmenti di rete (reti server, infrastrutture). Liguria Digitale esegue periodicamente attività di VA sulla propria infrastruttura Cloud. Queste attività saranno fatte dall'outsourcer in modo sistematico entro fine 2026.
- Nel piano di formazione offerto dall'outsourcer sono previste attività di formazione per il personale tecnico ICT di Area 5 sulle diverse materie ICT tra cui una sensibilizzazione di base

in materia cyber security. Sono in fase di attivazione (la raccolta delle adesioni si concluderà entro il corrente mese) le prossime attività formative a tema Cybersicurezza promosse dalla Regione Liguria, dedicate a dirigenti e funzionari e relative a:

1. corso base di cyber security, durata di fruizione circa 6 ore (+ test finale)
2. corso avanzato di cyber security, durata di fruizione circa 6 ore (+ test finale)

5

per il personale tecnico ICT di Area 5 sono altresì previsti i seguenti corsi:

3. formazione su NIS2 e Legge 90/2024, durata di fruizione di circa 4 ore (+ test finale)
4. formazione CISO, durata di fruizione circa 6 ore (+ test finale).

I corsi saranno fruibili via web (comprensivi dei test finali) fino a tutto il mese di ottobre 2026.

LIGURIA SALUTE

- Attualmente non sono implementati. Negli ultimi anni sono state e adottate misure volte a rafforzare la sicurezza e la continuità dei servizi ICT. In particolare, l'infrastruttura server è ospitata presso il Data Center di Liguria Digitale S.p.A., cloud provider qualificato da AgID e in possesso dei requisiti previsti per l'erogazione dei servizi cloud alla Pubblica Amministrazione. È previsto un servizio di eXtended Detection and Response (XDR) erogato tramite il Security Operations Center (SOC) di Liguria Digitale, finalizzato al monitoraggio continuo degli endpoint, alla rilevazione delle minacce informatiche e al supporto nella gestione degli incidenti di sicurezza, con servizio di reperibilità H24.
- Per quanto riguarda l'autenticazione a più fattori (MFA), è già stato implementato un servizio di autenticazione che consente il controllo degli accessi alla VPN e alla posta elettronica aziendale mediante autenticazione multifattore.
- Non sono mai state effettuate simulazioni di phishing.

GALLIERA

- Abbiamo una procedura di vulnerability assessment automatica di tenable settimanale che ci notifica tutte le vulnerabilità presenti all'interno dei vari segmenti della nostra rete LAN e esposte su internet. In base a questi report ci muoviamo notificando ai fornitori e chiedendo in prima battuta l'aggiornamento dei sistemi, nel frattempo mitigiamo in vari modi a seconda del caso (ad es. web application firewall, creando "air gap" isolando le installazioni e apponendo opportuni firewall per permettere la comunicazione solo dove necessario).
- Dal punto di vista tecnologico abbiamo implementato uno IAM che obbliga tutti gli utenti che accedono alle applicazioni web attraverso multifactor authentication in SSO al sito web, alla webmail, al telelavoro, al dossier sanitario, al cedolino paga, al fascicolo del personale, alle applicazioni IBMDR e alla prescrizione ricette.
- L'Ente si avvale di un SOC erogato in modalità MSSP 24/7 con vari livelli di escalation. Si avvale anche di un advisor di rischio cyber con cui abbiamo riunioni trimestrali che prioritizza il lavoro di gestione del rischio sulla base dei VA settimanali di cui abbiamo parlato in precedenza e della postura generale di sicurezza che emerge dai vari report del SOC.

È al vaglio della direzione l'istituzione di un ufficio sicurezza all'interno del dipartimento tecnico-informatico che abbia la titolarità della gestione della sicurezza di tutti gli apparati di IT, Ingegneria Clinica e Ufficio tecnico

Quesito n. 29

Si chiede di conoscere la somma assicurata relativa alle apparecchiature elettromedicali e alle apparecchiature elettroniche.

Risposta:

Apparecchiature elettronici e apparecchiature elettromedicali sono all'interno della partita beni Mobili e la loro valorizzazione è una quota preponderante della somma assicurata

Quesito n. 30

Si chiede di indicare se tra i beni assicurati siano presenti baracche e/o costruzioni in legno o plastica e quanto in essi contenuto, capannoni pressostatici e quanto in essi contenuto, tensostrutture e quanto in essi contenuto, tendostrutture e simili e quanto in essi contenuto.

Risposta:

Seppur non rappresentino un valore rilevante rispetto alla complessità assicurata si conferma l'esistenza di capannoni pressostatici e tensostrutture e simili

Quesito n. 33

Si chiede di confermare che nel novero dei beni assicurati non siano presenti fabbricati, impianti e/o macchinari destinati alla gestione del ciclo dei rifiuti (raccolta, smaltimento, trattamento) anche se in uso a terzi.

Nel caso siano presenti invece si prega di comunicare:

ubicazione precisa, destinazione d'uso, valore (fabbricati e contenuto), se in uso a terzi. Si chiede di confermare che nel novero dei beni assicurati non siano presenti impianti / pannelli fotovoltaici e impianti solari termici.

Nel caso siano presenti invece si prega di comunicare:

ubicazione precisa, valore, se in uso a terzi.

Si chiede conferma che lo stop loss sia il massimo indennizzo di polizza per sinistro annualità assicurativa in aggregato per tutti gli Enti assicurati fermi i sotto limiti previsti per le singole garanzie.

Risposta:

Si conferma che non sono presenti fabbricati, impianti e/o macchinari destinati alla gestione del ciclo dei rifiuti (raccolta, smaltimento, trattamento) anche se in uso a terzi – resta inteso che i rifiuti prodotti vengono stoccati in modo provvisorio i rifiuti presso dedicate aree per quindi essere poi raccolti dai soggetti terzi deputati allo svolgimento del servizio raccolta rifiuti.

Quesito n. 48

Si richiedono i seguenti chiarimenti (suddivisi per struttura):

- AOM

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente AOM quanto segue.

1. Si chiede di confermare se l'autenticazione a più fattori (MFA) sia applicata a tutti gli accessi remoti ai sistemi informativi interni. In alternativa, si chiede di indicare se siano adottate misure di sicurezza equivalenti, specificando quali.
2. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della
Struttura.

- ASL 1

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente ASL 1 quanto segue.

1. Si chiede di confermare la strategia di backup includa almeno una delle seguenti misure di sicurezza:
 - o backup eseguiti su supporti rimovibili, rimossi dopo la creazione e conservati in ambiente sicuro;
 - o backup effettuati tramite servizio cloud sicuro e dedicato;
 - o backup protetti da funzioni di immutabilità;
 - o backup dissociati dall'Active Directory;
 - o oppure se non sia presente nessuna delle misure sopra indicate, specificando eventuali misure compensative.
2. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

- ASL 2

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente ASL 2 quanto segue.

1. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

 ATS LIGURIA AZIENDA TUTELA DELLA SALUTE LIGURIA	CENTRALE REGIONALE DI ACQUISTO PER LA SANITA' Tel.: 010 5488541 email: direzione.areals@atsliguria.it	 Liguria Salute AREA LIGURIA SALUTE
---	---	--

- ASL 3

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente ASL 3 quanto segue.

8

1. Si chiede di confermare se l'autenticazione a più fattori (MFA) sia applicata a tutti gli accessi remoti ai sistemi informativi interni. In alternativa, si chiede di indicare se siano adottate misure di sicurezza equivalenti, specificando quali.

2. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

- ASL 3

A integrazione del precedente quesito relativo alla statistica sinistri Cyber, con specifico riferimento al sinistro indicato per ASL 3 in data 02/01/2026, si chiede di fornire ulteriori dettagli anche qualora l'evento dovesse risultare ad oggi chiuso o risolto.

In particolare, si chiede di precisare:

1. natura dell'evento cyber e modalità di accadimento;
2. eventuale coinvolgimento di dati personali, dati sanitari o dati particolari;
3. stato attuale dell'eventuale interlocuzione con il Garante Privacy;
4. stato del sinistro, con indicazione di eventuali importi pagati, riservati o stimati.

- ASL 4

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente ASL 4 quanto segue.

1. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

- ASL 5

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente ASL 5 quanto segue.

1. Si chiede di confermare se l'autenticazione a più fattori (MFA) sia applicata a tutti gli accessi remoti ai sistemi informativi interni. In alternativa, si chiede di indicare se siano adottate misure di sicurezza equivalenti, specificando quali.

2. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

3. Si chiede di confermare se sia implementato un tool per la protezione delle e-mail e, in caso affermativo, se lo stesso preveda almeno una tra le seguenti misure di sicurezza:

- o rilevamento degli allegati dannosi;
- o rilevamento dei link dannosi;
- o funzionalità di quarantena.

4. Si chiede di confermare se, sul perimetro IT, sia implementato un programma di gestione delle patch di sicurezza.

- Ospedale Evangelico

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente Ospedale Evangelico quanto segue.

1. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

- E.O. Galliera

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente E.O. Galliera quanto segue.

1. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

- Istituto Giannina Gaslini

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk, si segnala che nella documentazione ricevuta non risulta disponibile il Cyber Risk Proposal Form compilato. Si chiede pertanto di voler trasmettere il Cyber Risk Proposal Form compilato per tale struttura e di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente Istituto Giannina Gaslini quanto segue.

1. Si chiede di confermare se l'autenticazione a più fattori (MFA) sia applicata a tutti gli accessi remoti ai sistemi informativi interni. In alternativa, si chiede di indicare se siano adottate misure di sicurezza equivalenti, specificando quali.

2. Si chiede di confermare la strategia di backup includa almeno una delle seguenti misure di sicurezza:

- o backup eseguiti su supporti rimovibili, rimossi dopo la creazione e conservati in ambiente sicuro;
- o backup effettuati tramite servizio cloud sicuro e dedicato;
- o backup protetti da funzioni di immutabilità;
- o backup dissociati dall'Active Directory;
- o oppure se non sia presente nessuna delle misure sopra indicate, specificando eventuali misure

compensative.

3. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

4. Si chiede di confermare se sia implementato un tool per la protezione delle e-mail e, in caso affermativo, se lo stesso preveda almeno una tra le seguenti misure di sicurezza:

- o rilevamento degli allegati dannosi;
- o rilevamento dei link dannosi;
- o funzionalità di quarantena.

- Liguria Salute

Con riferimento al Capitolato Speciale del Lotto 2 – Cyber Risk e ai Cyber Risk Proposal Form trasmessi, si chiede di integrare le informazioni tecniche mancanti o non chiaramente desumibili dalla documentazione ricevuta, confermando per l'ente Liguria Salute quanto segue.

1. Si chiede di confermare se venga impedita l'installazione di software non autorizzato sui sistemi della Struttura.

Risposta:

ASL 1

- I backup eseguiti su supporti rimovibili, rimossi dopo la creazione e conservati in ambiente sicuro, sia per quanto riguarda i sistemi ospitati presso il datacenter di Liguria Digitale, sia per quelli residuali ospitati presso il datacenter di Area 1;
- Si conferma. L'eventuale installazione di software non autorizzato viene comunque rilevata dagli agent xdr presenti a bordo delle postazioni e notificata al SOC di Liguria Digitale, e nel caso di procede alla disinstallazione.
- L'elenco dei fornitori di servizi critici IT con l'evidenza del servizio erogato era già stato indicato nella sezione D del documento "Cyber Risk Insurance Aon Proposal Form" (si confermano).

ASL 4

- Confermo che l'accesso ai sistemi (incluse le postazioni di lavoro) con profili amministrativi è consentito unicamente agli amministratori di sistema, debitamente formati e formalmente nominati

ASL 5

- La MFA è in distribuzione per quanto riguarda la posta elettronica ed in test per quanto riguarda gli accessi VPN su Firewall presente in ASL5. Per i fornitori esterni che accedono alla rete di ASL5 tramite accessi VPN gestiti su Firewall di Liguria Digitale è già attiva la VPN MFA.
- Sui sistemi è inibita la possibilità di installare qualsiasi tipo di software se non preventivamente autorizzato. Le deroghe (utenti con privilegi di amministrazione locale della PdL) sono censite e tracciate dall'outsourcer. L'outsourcer, nell'ottica di rafforzare

ulteriormente la protezione dell'infrastruttura Microsoft di Area 5 e di prevenire in modo più efficace le minacce informatiche, in particolare quelle finalizzate al furto delle credenziali la gestione dei sistemi con account privilegiati, utilizza uno standard di sicurezza basato sul Modello di Tiering (Microsoft Tiering Model) - separazione degli accessi amministrativi ai vari sistemi – la cui verifica sarà completata entro fine 2026.

- Il sistema di e-mail aziendale è Microsoft Office 365 (licenza E1). Per la protezione è attiva la funzionalità di Exchange Online Protection con le funzionalità della licenza E1.
- L'outsoucer ha implementato un doppio server (Windows update (WSUS)) uno per i Client e uno per i Server per la distribuzione delle patch di sicurezza. Le patch vengono installate nelle finestre di manutenzione concordate con Area 5.

LIGURIA SALUTE

- Si conferma che l'installazione di software sulle postazioni di lavoro è consentita esclusivamente agli utenti con ruolo "amministratore"

ASL 2

- Sì. Sono autorizzati alle installazioni sulle postazioni di lavoro (PdL) solo gli addetti IT, gli altri utenti di dominio (domain users) non hanno i privilegi necessari per effettuare installazioni sulle PdL.

GALLIERA

- Si viene impedita l'installazione di software non autorizzato sui sistemi della Struttura.

Quesito n. 51

Si chiede:

- elenco dei fornitori critici (critical dependencies) nel numero dai 10 ai 20 (sia IT sia non IT), con evidenza di: servizio erogato; criticità per il business; eventuale trattamento dati; dipendenza operativa; presenza di piani di continuità/disaster recovery; eventuali fornitori alternativi.

Risposta:

ASL 1

L'elenco dei fornitori di servizi critici IT con l'evidenza del servizio erogato era già stato indicato nella sezione D del documento "Cyber Risk Insurance Aon Proposal Form" (si confermano)

ASL 2

Elenco dei fornitori IT critici :

- *Microsoft (autenticazione, spazi cloud)*
- *Telecom-TIM (servizi di manutenzione hardware e sistemi di conservazione)*
- *Fastweb (connettività, telefonia fissa e mobile)*
- *Oracle (database)*
- *Liguria Digitale (Cloud IAAS, connettività, disaster recovery, SOC, applicativi)*
- *Elco (applicativi clinici)*
- *Dedalus (applicativi clinici)*
- *GPI (applicativi clinici)*

- Engineering (applicativi amministrativi)

- DedaNext (applicativi amministrativi)

NB: per alcuni software sanitari critici è previsto disaster recovery tramite i servizi messi a disposizione dal Cloud regionale IAAS di Liguria Digitale. Tutti i fornitori che trattano dati di cui l'Ente è titolare vengono nominati responsabili esterni del trattamento (ex art. 28 GDPR).

ASL 4

Fornitore	servizio	criticità	trattamento dati?	dipendenza operativa	presenza DR o BC	fornitori alternativi
Liguria Digitale	Datacenter, SOC, applicativi	alta	parziale	?	S	no
Vodafone	Connettività dati, fonia mobile	alta	no	?	N (l'architettura è ridondata ed eliminano SPOF)	
Fastweb	Connettività dati	alta	no	?	N (l'architettura è ridondata ed eliminano SPOF)	
TIM	servizi ICT	alta	no		N (l'architettura è ridondata ed eliminano SPOF)	
Ebit	Sistema PACS	alta	sì		N (l'architettura è ridondata ed eliminano SPOF)	
Dedalus	Sistemi applicativi sanitari	alta	sì		sono previste procedure per la continuità del servizio con uso del cartaceo o attività locali	no
Engineering	Sistemi applicativi finanziari	media	sì		N (l'architettura è ridondata ed eliminano SPOF)	
ADS	Sistemi applicativi HR	media	sì		N (l'architettura è ridondata ed eliminano SPOF)	
ITSVIL	Sistemi applicativi sanitari	media	sì		N (l'architettura è ridondata ed eliminano SPOF)	
GPI	Sistemi applicativi sanitari	media	sì		N (l'architettura è ridondata ed eliminano SPOF)	

ASL 5

Fornitore	Servizio	Criticità	Trattamento	Dipendenza	Piani di continuità	Fornitori Alternativi
Philips	PACS	alto	Nominati responsabili trattamento	Rete locale, rete elettrica	Nodi replicati	N/A
Esaote ebit	Cardiologia PACS	alta	Nominati responsabili trattamento	Rete locale, rete elettrica, linee connettività	Nodi replicati	N/A
Dedalus	LIS	alta	Nominati responsabili trattamento	Rete locale, rete elettrica	Nodi replicati, al momento operativo solo 1 nodo	N/A
ELCO	CCE, DSE, RIS	alta	Nominati responsabili trattamento	Linee connettività	Cloud PSR	N/A
Liguria Digitale	Anagrafe, COT	media	Nominati responsabili trattamento	Linee connettività	Cloud PSR	N/A
SINED	Nefrologia, Dialisi	alta	Nominati responsabili trattamento	Linee connettività	Cloud PSR	N/A
Liguria Digitale	Cloud, Server, PDL, Sicurezza	alta	Nominati responsabili trattamento	Linee connettività	Cloud PSR	N/A
Millenium	Cartella MMG	alta	Nominati responsabili trattamento	Linee connettività	Cloud PSR	N/A
Engineering	Contabilità e Magazzino, personae, anatomia patologica trasfusionale	alta	Nominati responsabili trattamento	Linee connettività	Cloud PSR	N/A
Topgate	Cartella ambulatoriale, screening	media	Nominati responsabili trattamento	Linee connettività	Cloud PSR	N/A

Quesito n. 58

Lotto 1: Relativamente alla statistica sinistri, richiediamo gentilmente di indicarci quanto segue:

o quali dei sinistri occorsi negli ultimi anni sono Furto e rapina di farmaci e medicinali, indicando il relativo importo nel caso di furto "combinato"

o conferma che i valori dei sinistri a riserva siano lordo franchigia

o indicazione del deducibile di polizza applicato ai seguenti sinistri: numeri 15083236, 15421989 e 15443043.

Risposta:

Confermiamo che i sinistri a riserva sono al lordo franchigia mentre i sinistri liquidati al netto sono:

Sinistro n. 15083236 – scoperto 20% minimo € 50.000.

Sinistro n. 15421989 – franchigia frontale € 1.000.

Sinistro n. 15443043 - franchigia frontale € 1.000.

Il furto di farmaci e medicinali è una casistica infrequente negli ultimi 5 anni.

Quesito n. 65

Con riferimento alla SEZIONE X - LIMITI – SCOPERTI – FRANCHIGIE, si chiede di confermare che quanto previsto per la garanzia “Differenziale storico-artistico” operi nei limiti di indennizzo indicati in tabella per le singole garanzie coinvolte dal sinistro.

Risposta:

Si rimanda al capitolato tecnico.

Quesito n. 66

Con riferimento alla SEZIONE X - LIMITI – SCOPERTI – FRANCHIGIE, garanzia Smottamento, cedimento e franamento del terreno si chiede conferma che lo scoperto del 10% con minimo non indennizzabile di € 10.000,00 operi per singola Ubicazione.

Risposta:

Come indicato nel capitolato tecnico lo scoperto 10% con il minimo €10.000 si applica per sinistro.

Quesito n. 67

Con riferimento alla SEZIONE X - LIMITI – SCOPERTI – FRANCHIGIE, si chiede conferma che i limiti di indennizzo e i relativi deducibili previsti per “beni elettronici” e “beni elettromedicali”, trovino applicazione esclusivamente per eventi non espressamente disciplinati alle singole garanzie. A titolo esemplificativo, si chiede di confermare che, in caso di allagamenti, restino operanti le

 AZIENDA TUTELA DELLA SALUTE LIGURIA	CENTRALE REGIONALE DI ACQUISTO PER LA SANITA' Tel.: 010 5488541 email: direzione.areals@atsliguria.it	 AREA LIGURIA SALUTE
--	---	--

condizioni specifiche previste per tale garanzia, e pertanto uno scoperto del 10%, con minimo di € 10.000 per singola ubicazione, nonché un limite di indennizzo pari a € 1.000.000 per sinistro e € 5.000.000 per periodo assicurativo, salvo eventuali diverse disposizioni introdotte in sede di Offerta Tecnica (OT).

15

Risposta:

Si rimanda al capitolato tecnico.

Quesito n. 68

Si chiede di confermare l'esclusione dalla copertura assicurativa dei seguenti beni: impianti per la produzione di energia da fonti rinnovabili, quali impianti eolici, fotovoltaici, solari termici e rispettive componenti. In caso di risposta negativa, si chiede di fornirne esplicita descrizione, ubicazione e valorizzazione e di indicare a quale partita tali beni siano assicurati.

Risposta:

si rimanda al capitolato tecnico alle definizioni di Beni Immobili e Beni Mobili.

Quesito n. 69

Si chiede conferma che i limiti di indennizzo previsti alla SEZIONE X si intendano cumulativi per tutti i Certificati d'assicurazione emessi in base alla presente Convenzione (secondo quanto riportato alla Sezione I – Convenzione) e che pertanto la Società non sarà tenuta ad indennizzare, per ogni sinistro e per ogni anno assicurativo, somme superiori a quelle indicate alle singole voci di garanzia per il complesso di tutti i contratti emessi in base alla Convenzione.

Risposta:

confermiamo che i limiti riportati nella tabella LSF sono da intendersi complessivi per tutti i certificati.

Quesito n. 70

Si chiede conferma che il limite di € 100.000.000,00 (eventualmente aumentabile da OT) rappresenti il massimo esborso, riferito al complesso di tutti i contratti emessi in base alla Convenzione, che la Società è tenuta a corrispondere all'Assicurato per tutti i sinistri che si verificassero nel corso della annualità assicurativa e che, pertanto, in nessun caso la Società sarà tenuta a corrispondere per singola annualità assicurativa - somma maggiore di tale importo.

Risposta:

Si conferma

 AZIENDA TUTELA DELLA SALUTE LIGURIA	CENTRALE REGIONALE DI ACQUISTO PER LA SANITA' Tel.: 010 5488541 email: direzione.areals@atsliguria.it	 AREA LIGURIA SALUTE
--	---	--

Quesito n. 71

Si chiede cortesemente se può essere riconosciuta all'operatore economico, in caso di aggiudicazione, la possibilità di sostituire il contenuto della clausola E) Esclusione Malattie Trasmissibili con il testo sotto riportato:

ESCLUSIONE MALATTIE TRASMISSIBILI

A parziale modifica delle condizioni di polizza si intendono esclusi dalle coperture assicurative qualsiasi perdita, danno, responsabilità, richiesta di indennizzo o risarcimento, costo o spesa di qualunque natura, direttamente o indirettamente causato da, contribuito, derivante o nascente da, o relativo a, una Malattia Trasmissibile o qualsiasi timore o minaccia (reale o percepita) di quest'ultima. Per Malattia Trasmissibile si intende qualunque patologia o malattia che possa essere trasmessa per mezzo di qualsiasi sostanza o agente da qualunque organismo a un altro organismo, ove:

- per sostanza o agente si intende, tra gli altri ed a titolo solo esemplificativo e non esaustivo, qualsiasi virus, batterio, parassita o altro organismo o qualsiasi sua variante, considerati viventi o meno, e
- il metodo di trasmissione, sia esso diretto o indiretto, include, a titolo solo esemplificativo e non esaustivo, la trasmissione per via aerea, la trasmissione attraverso liquidi corporei, la trasmissione da o verso qualsiasi superficie o oggetto solido, liquido o gassoso, o tra organismi, e
- la patologia o malattia, la sostanza o l'agente possano provocare o minacciare danni alla salute o al benessere della persona o possano causare o minacciare danni, deterioramento, perdita di valore, perdita di commerciabilità o perdita d'uso di beni materiali assicurati.

Ai fini della presente clausola si precisa che perdita, danno, reclamo, costo, spesa o altra somma, includono, a titolo esemplificativo, i costi di decontaminazione, pulizia, disinfezione, rimozione, monitoraggio o test, nonché i danni che derivano dagli atti e dalle misure per prevenire il contagio disposti dalle competenti Autorità anche in relazione alla chiusura o alla restrizione dell'attività.

La presente clausola si applica a tutte le garanzie della presente polizza, alle eventuali estensioni di copertura, coperture aggiuntive, alle eccezioni a qualsiasi esclusione e altre garanzie in copertura.

Tutti gli altri termini, condizioni ed esclusioni della presente polizza rimangono invariati.

Risposta:

Si conferma

Quesito n. 72

Si chiede cortesemente se può essere riconosciuta all'operatore economico, in caso di aggiudicazione, la possibilità di sostituire il contenuto della clausola F) Esclusione rischi Cyber con il testo sotto riportato:

CLAUSOLA CYBER RISK

È esclusa qualsiasi perdita, danno, responsabilità, sinistro, costo o spesa direttamente o indirettamente causati da, contribuiti da, risultanti da, derivanti da o in connessione con un Incidente Cyber che comporti la perdita, il danno, la distruzione, distorsione, cancellazione, non disponibilità, corruzione o alterazione dei Dati Elettronici o del/i Sistema/i Informatico/i.

Sono da intendersi comunque coperte le perdite materiali ed i danni ai beni assicurati nella polizza originale causati da un evento dovuto ad un rischio assicurato nella suddetta polizza, ivi inclusa l'interruzione dell'attività che ne derivi, anche se causata da un Incidente Cyber.

Definizioni

Nella definizione di "Incidente Cyber" sono compresi tutti i danni causati o conseguenti da:

- atti non autorizzati o dannosi indipendentemente dal tempo e dal luogo di loro compimento e dall'eventuale ricorso ad una minaccia od all'inganno;
- software intrusivi o malevoli;
- errori di programmazione o dell'operatore commessi dall'assicurato o da qualsiasi altra persona da esso autorizzata o incaricata;
- qualsiasi interruzione involontaria o non pianificata, totale o parziale, del sistema informatico dell'assicurato anche non direttamente causata da perdita o danno materiale di strumenti hardware;
- accesso, elaborazione, utilizzo o comunque operatività di qualsiasi Sistema informatico o di Dati elettronici effettuata da parte di qualsiasi persona o gruppo/i di persone;

Per "Sistema informatico" si intende l'insieme degli strumenti informatici hardware e software (calcolatori, software di base, apparati o sottosistemi elettronici, programmi, ecc.) anche nel caso siano tra loro interconnessi in rete, preposti ad una o più funzionalità o servizi di elaborazione incluso qualsiasi input, output o dispositivo di archiviazione elettronica dei dati associato, apparecchiatura di rete o struttura di backup.

Per "Dati elettronici" si intendono informazioni organizzate in complessi logicamente strutturati, elaborabili a mezzo di programmi.

Per "Software intrusivi o malevoli" si intende ad esempio la categoria dei virus informatici, atti ad interferire con le operazioni delle apparecchiature elettroniche al fine di danneggiare, distruggere o carpire informazioni, diffonderle indebitamente o criptarle al fine di estorcere denaro per la decrittazione, nonché diffondersi in altre apparecchiature elettroniche o Sistemi informatici allo scopo di arrecare danni, rallentarli o renderli inutilizzabili o causare altri problemi nel corso dell'esecuzione di programmi software.

Risposta:

Si conferma

Quesito n. 73

Si chiede cortesemente se può essere riconosciuta all'operatore economico, in caso di aggiudicazione, la possibilità di sostituire il contenuto della clausola G) Esclusione sanzioni con il testo sotto riportato: "In ogni caso la Società non fornirà copertura assicurativa e non sarà tenuta a pagare alcun indennizzo, né comunque alcuna somma in base alla presente assicurazione, nei casi in cui tale copertura o pagamento possa esporre la Società, o qualsiasi suo dipendente, o collaboratore, a sanzioni, o possa comportare violazione di divieti o restrizioni, secondo quanto previsto da risoluzioni delle Nazioni Unite in materia di embarghi e sanzioni economiche o commerciali, o da leggi o regolamenti dell'Unione Europea, della Svizzera, del Regno Unito o degli Stati Uniti d'America."

Risposta:

Si conferma

**CENTRALE REGIONALE DI ACQUISTO PER LA
SANITA'**

Responsabile Unico del Progetto
Dott. Giorgio Sacco

Documento informatico firmato digitalmente ai sensi
del testo unico D.P.R. 28 dicembre 2000, n. 445, del
D.Lgs. 7 marzo 2005, n.82 e norme collegate