ISTITUTO ZOOPROFILATTICO SPERIMENTALE
DELLA LOMBARDIA E DELL'EMILIA ROMAGNA
"BRUNO UBERTINI"
(ENTE SANITARIO DI DIRITTO PUBBLICO)
Sede Legale: Via Bianchi, 9 – 25124 Brescia
Tel 03022901 – Fax 0302425251 – Email info@izsler.it
C.F. - P.IVA 00284840170 N. REA CCIAA di Brescia 88834

Definizione Capitolato d'Oneri e Specifiche Tecniche Generali relative all'acquisizione di apparecchiature, servizi e/o sistemi da integrare con i Sistemi Informativi dell'IZSLER

Documento:	Documento di specifiche
Emittente:	Sistemi Informativi

Informazioni sul Documento	
Codice Doc. – Revisione – Data rilascio:	Capitolati-SIST Rev. SI ST 0201 del
WordProcessor: Codice richiesta:	

Autorizzazioni dell'attuale versione	
Funzioni	***Responsabili***
Autore	***Gianluca Archetti, Domenico Nilo MAZZA, Alessandro Morari, Riccardo Possenti***
Controllo	***Domenico Nilo Mazza***
Autorizzazione	

Nota Aggiungere alla sottostante tabella le righe necessarie allo scopo

Versioni			
Versione	Data	Autori	Modifiche
1.0	18/2/2018	Archetti, Mazza, Morari, Possenti	Prima Versione
2.0	30/11/2023	Archetti, De Franceschi Mazza, Morari, Possenti	Aggiornata struttura e contenuti

Note
Il presente documento è di proprietà esclusiva dell'IZSLER "Bruno Ubertini" di Brescia che se ne riserva tutti i diritti. Ogni riproduzione o diffusione anche parziale e con qualsiasi mezzo è da ritenersi vietata se non autorizzata per iscritto.

INDICE

1. Generalità

1.1 Scopo

Scopo del presente documento è quello di riassumere le regole da seguire per la definizione di un qualsiasi capitolato o documento di specifiche tecniche che preveda l'interconnessione dell'apparecchiatura, servizio e/o sistema oggetto della fornitura, a qualsiasi titolo acquisita, al Sistema Informativo Aziendale, comprese le sue infrastrutture, dell'IZSLER "Bruno Ubertini" di Brescia, in seguito indicato più semplicemente come IZSLER o Istituto.
Sono altresì ricompresi i servizi acquisiti dall'IZSLER in modalità outsourcing o "in service", ovunque le informazioni siano comunque correlate in qualche modo alle attività dell'IZSLER e gestite con strumenti informatici.
Le stesse caratteristiche dovranno essere soddisfatte da apparati proposti in donazione o acquisiti a qualunque altro titolo, la cui messa in rete, integrazione con il Sistema Informativo Aziendale (Sistemi Informativi) ed utilizzo nell'IZSLER sono subordinati al rispetto di quanto qui indicato.
Le regole qui esposte devono essere applicate anche ad apparecchiature, servizi e/o sistemi già presenti in occasioni di rinnovi contrattuali e/o estensioni e/o integrazioni della fornitura in essere, al fine di allineare alle politiche aziendali l'intero parco installato.
Sono quindi definite ed illustrate le regole che devono essere seguite in modo generale e non specifico per i singoli ambiti di applicazione, in modo da rappresentare un riferimento generico applicabile ad ogni area di interesse ed utilizzabile come allegato ad altri capitolati ai quali fare riferimento.
I destinatari del presente documento sono:

1. gli incaricati dell'estensione del Capitolato d'Oneri e delle Specifiche Tecniche, per i quali rappresenta la base per tale ambito,
2. gli incaricati della procedura di acquisizione, che devono verificarne la corretta applicazione,
3. i referenti dei potenziali fornitori, che si devono attenere alle regole descritte nel presente documento.

Non sono qui descritte le singole componenti richiamate per le quali si rimanda alla documentazione relativa.

1.2 Campo di applicazione

Il presente documento si applica ogni qual volta deve essere definito il Capitolato d'Oneri o un documento di Specifiche Tecniche relativo alla fornitura di un sistema/apparecchiatura/servizio che deve essere interfacciato con il Sistema Informativo Aziendale dell'IZSLER o in occasione di un'acquisizione a qualunque titolo, anche temporanea, di un'apparecchiatura da interconnettere al Sistema Informativo a qualsiasi titolo ed in qualunque modo in uso presso l'IZSLER di Brescia.
La sua applicazione è quindi da considerarsi diretta ed automatica, estensiva e senza limitazioni o deroghe: tutte le forniture dovranno prevedere quanto qui richiesto, senza alcun onere aggiuntivo per l'IZSLER.
Si ribadisce che le regole qui esposte devono essere applicate anche ad apparecchiature, servizi e/o sistemi già presenti in occasioni di rinnovi contrattuali e/o estensioni e/o integrazioni della fornitura in essere, al fine di allineare alle politiche aziendali l'intero parco installato.
Le attività oggetto del presente documento hanno sede presso le sedi dell'IZSLER "Bruno Ubertini" di Brescia nelle sue diverse sedi territoriali e possono essere parzialmente localizzate presso le sedi dei fornitori previo accordo con il Responsabile Unico del Procedimento (RUP), il Direttore di Esecuzione del Contratto (DEC) ed il Responsabile dei Sistemi Informativi.

1.3 Definizioni, acronimi e abbreviazioni

Sono qui riassunti per comodità di consultazione le abbreviazioni, gli acronimi e le definizioni adoperate nel resto del documento che si è ritenuto utile dettagliare.

Termine	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale
AD	Dominio Microsoft Active Directory
AGID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e s.m.i.)
CIE	Carta di Identità Elettronica
DEC	Direttore di Esecuzione del Contratto
GDPR	General Data Protection Regulation- Regolamento UE 2016/679
IZS	Istituto Zooprofilattico Sperimentale
IZSLER	Istituto Zooprofilattico Sperimentale Lombardia Emilia Romagna "Bruno Ubertini" di
PdL	Postazioni di Lavoro
QoS	Quality of Service
RDP	Rapporto di Prova
RUP	Responsabile Unico del Procedimento
SI	Sistemi Informativi
SIA	Sistema Informativo Aziendale
SPID	Sistema Pubblico Identità Digitale

1.4 Aspetti Generali

Le indicazioni presenti nel documento fanno prioritariamente riferimento al Piano Triennale per l'informatica nella Pubblica Amministrazione (in seguito riferito anche come Piano Triennale o Piano, vedi **Errore. L'origine riferimento non è stata trovata.**) redatto da AGID ed in generale alle linee guida di settore emesse oltre che da AGID stessa, dall'ACN e dal Garante per la Protezione dei Dati Personali

Qualsiasi apparato informatico e/o periferica associata che verrà installato presso l'IZSLER, dovrà avere caratteristiche e prevedere modalità di collegamento ed operative che dovranno essere concordate con i Sistemi Informativi e sottoposte alla loro preventiva approvazione, in assenza della quale il collegamento in rete non sarà consentito.

Eventuali apparati installati senza autorizzazione potranno essere disconnessi, disattivati e presi in custodia dal personale dei Sistemi Informativi senza necessità di alcuna autorizzazione da parte di terzi al fine di tutelare il corretto funzionamento e la sicurezza del Sistema Informativo Aziendale.

L'installazione di PdL (Postazioni di Lavoro), server e altre attrezzature informatiche fornite dall'azienda appaltatrice dovrà essere preventivamente concordata con i Sistemi Informativi: le modalità di collegamento saranno concordate in base alla dotazione tecnologica di cui dispone la sede interessata ed in base agli scopi funzionali dell'apparecchiatura.

Nello specifico:

1. Le caratteristiche delle postazioni in termini di dotazioni Hardware e Software dovranno essere concordate con i Sistemi Informativi e sottoposte alla loro preventiva approvazione, in assenza della quale il collegamento in rete non sarà consentito.
2. In caso di collegamento diretto alla rete dell'Istituto, le postazioni saranno gestite dal dominio aziendale (Active Directory Microsoft), e dovranno sottostare alle regole di sicurezza imposte relativamente agli accessi, alle policy di gestione, alla protezione antivirus/antimalware e agli aggiornamenti del sistema operativo e di tutte le applicazioni e moduli installati, da

considerarsi obbligatori come previsto dalle misure minime di sicurezza ICT previste da AGID ed ACN.

3. In nessun caso sarà possibile pilotare o accedere da remoto ad altre postazioni/PdL: tutte le operazioni e/o funzioni devono essere eseguite con strumenti, funzioni ed applicazioni proprie del programma stesso.
4. In caso di collegamento a rete virtuale dedicata, la postazione può essere gestita in modo indipendente dal fornitore, sia dal punto di vista degli accessi che della protezione antivirus e del sistema, ma deve comunque essere garantito l'aggiornamento del sistema e di tutte le sue componenti, e la manutenzione secondo quanto previsto dalla normativa in vigore. In questo caso è possibile da parte del fornitore chiedere di effettuare l'accesso da remoto al solo scopo di pilotare la postazione di lavoro per effettuare assistenza e manutenzione, ma non sarà possibile accedere al di fuori della VLAN assegnata, dei privilegi e delle funzioni abilitate.

Nel richiedere l'autorizzazione l'aggiudicatario si impegna a fornire tutte le informazioni necessarie ad una corretta valutazione delle attività da svolgere.
Non è ammesso l'utilizzo di Basi di Dati il cui accesso non preveda il rispetto di protocolli di sicurezza con la verifica ed il log degli accessi tramite utente e password e che non rispettino le indicazioni e le norme in materia di Privacy in vigore.

A carattere generale, viene inoltre richiamato il rispetto dei Principi guida presenti nel Piano Triennale per l'informatica della Pubblica Amministrazione di AgID (Agenzia per l'Italia Digitale) e riportati di seguito:

- *Digital & mobile first;*
- *Digital identity only;*
- *Cloud first;*
- *Dati pubblici un bene comune;*
- *Interoperabile by design;*
- *Sicurezza e privacy by design;*
- *User-centric, data driven e agile;*
- *Once only;*
- *Transfrontaliero by design;*
- *Codice aperto.*

1.5 Riferimenti

Sono qui raccolti i documenti di riferimento di primo livello citati nel presente documento.

[1] Piano Triennale per l'informatica nella Pubblica Amministrazione, AGID, aggiornamento 2022-2024, https://www.agid.gov.it/it/agenzia/piano-triennale

[2] Codice dell'Amministrazione Digitale (CAD), AGID, https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale

2. Sicurezza e Privacy

In tema di sicurezza delle informazioni l'aggiudicatario e/o fornitore deve adeguare la propria fornitura ed il proprio comportamento a quelle che sono tutte le normative e le disposizioni, sia interne che di ordine generale, che interessano tale ambito, a partire dal D. Lgs 101/2018, dal GDPR (General Data Protection Regulation- Regolamento UE 2016/679), anche in riferimento alla compliance rispetto alla region di permanenza dei dati, e loro successive modificazioni ed integrazioni. Si precisa infatti che l'aggiudicatario/fornitore, nel corso dell'intera durata del contratto, dovrà garantire pieno rispetto anche delle norme, dei provvedimenti e delle prassi in materia di data protection che dovessero intervenire nel tempo.

L'aggiudicatario/fornitore deve assicurare il pieno rispetto di tutte le normative in vigore sul trattamento dei dati personali ed in particolar modo di quelli sensibili, dimostrando che sono resi operativi tutti gli strumenti atti a tale scopo e dichiarando la propria disponibilità a provvedere ai futuri adeguamenti che la normativa, il Garante per la Protezione dei Dati Personali e/o l'IZSLER richiederanno.

Particolare attenzione dovrà essere adottata nella gestione di componenti e moduli di terze parti, verificando la presenza di raccolta e comunicazione di dati di tracciamento di qualsiasi tipo, che in nessun caso devono essere inviati al di fuori dei confini UE, come previsto dalle norme in vigore.

Occorre che la fornitura sia allineata alle policy previste da ACN, Garante della Privacy ed IZSLER in termini di sicurezza ed in particolare:

1. gestione e manutenzione dei sistemi;
2. costante, sistematica e completa gestione ed installazione di tutti gli aggiornamenti del Sistema Operativo e di ogni componente software installata nel sistema e/o necessaria al suo funzionamento, con particolare riferimento agli aggiornamenti diretti ed indiretti in tema di sicurezza e/o funzionali;
3. installazione, manutenzione ed aggiornamento degli antivirus, che se oggetto di fornitura, saranno a carico dell'aggiudicatario;
4. controllo degli accessi: l'IZSLER utilizza a tale scopo un Dominio Microsoft Active Directory, accessibile anche via protocollo standard LDAP, sul quale devono necessariamente essere censiti tutti gli utenti della rete e delle applicazioni; non sono ammesse utenze non nominative e dovrà essere fornita la lista degli utenti che accedono ai sistemi, nonché copia dei loro documenti di identità e Codice Fiscale;
5. gestione delle modalità di accesso alla rete aziendale;
6. applicativi web che anche se ad uso interno operano solo su connessioni sicure https/sftp, ecc…: il costo del relativo certificato digitale rilasciato da una Certification Authority, se non diversamente indicato, è a carico del fornitore;
7. ogni eventuale trasferimento di dati relativo all'utilizzo dell'applicazione e/o di un suo componente, anche di terze parti, dovrà essere tracciato e documentato, assicurando il pieno rispetto di quanto previsto dal GDPR e dal D. Lgs. 101/2018
8. deve essere prevista nativamente la possibilità di crittografare tutti i dati (file e DB) secondo procedure standard ed allo stato dell'arte.

Il sistema deve garantire la tracciatura completa di tutti gli eventi atti a ricostruire le operazioni intercorse quali, a titolo di esempio non esaustivo, accessi, operazioni, errori, ecc….

Eventuali VPN dovranno essere adeguatamente controllate e monitorate al fine di consentirne un utilizzo conforme alle disposizioni aziendali; gli accessi remoti potranno avvenire solo sulla base di credenziali nominali correttamente assegnate dai Sistemi Informativi e nell'esclusivo ambito dei contesti assegnati.

Le VPN, che rappresentano l'unico sistema di accesso da remoto ai sistemi, avranno un titolare responsabile, identificato nel richiedente o altra figura delegata che dovrà rilasciare copia del documento di identità e codice fiscale e che sarà opportunamente nominato responsabile del trattamento dei dati.
Saranno i Sistemi Informativi a definire le modalità di accesso esterno/remoto consentito e saranno autorizzate sole quelle che ad insindacabile giudizio dei Sistemi Informativi saranno ritenute adeguate in termini di affidabilità e sicurezza: è doveroso compito del fornitore adeguarsi a tutte le direttive aziendali senza alcun costo aggiuntivo e/o onere alcuno, pena l'impossibilità di accedere remotamente.
I Sistemi Informativi si riservano di poter interrompere in qualsiasi momento, anche senza preavviso, qualsiasi collegamento remoto qualora lo ritenessero opportuno e/o necessario senza altro obbligo che provvedere alla comunicazione, anche a posteriori, ai riferimenti comunicati in sede di attivazione: in nessun caso e per nessun motivo tale interruzione potrà essere motivo per qualsivoglia interruzione di servizi e/o forniture né potrà dare adito a richiesta di risarcimento o oneri aggiuntivi.
Nel caso di collegamento tramite rete virtuale, la postazione potrà esclusivamente accedere alla subnet predisposta: eventuali connessioni ad altre postazioni della rete dell'IZSLER o ad Internet, dovranno essere esplicitamente richieste (tramite apposita documentazione) essendo la VLAN predisposta protetta da firewall: le connessioni verso altre postazioni della rete dell'Istituto, non potranno in alcun modo prevedere l'utilizzo di software di controllo remoto (VNC, RDP, etc).
L'aggiudicatario si impegna a fornire un accesso amministrativo al sistema, riservato ai Sistemi Informativi e di loro uso esclusivo, accesso che per nessuna ragione potrà essere disabilitato se non su disposizione scritta del Dirigente Responsabile del Sistemi Informativi.
Nell'ambito della gestione della fornitura e per tutta la durata della stessa, per ogni attività derivante dagli adempimenti normativi in vigore, il fornitore si impegna fra l'altro a:

a. individuare i dipendenti o collaboratori che dispongono di accessi privilegiati a strumenti e sistemi e che perciò si configurano come amministratori di sistema, e di procedere verso di essi alla nomina ad amministratore di sistema, previa condivisione con l'ZSLER;
b. accettare ogni Nomina a Responsabile Esterno, ai sensi delle definizioni della richiamata normativa vigente, indispensabile per il trattamento di dati personali nel corso della esecuzione del contratto;
c. operare la nomina degli incaricati secondo le prescrizioni normative in vigore e fornire gli elenchi che saranno richiesti periodicamente da IZSLER in merito alle persone coinvolte come Amministratori di Sistema o incaricati.

Il fornitore si impegna a collaborare in ogni momento alle attività di Audit intraprese da o per conto di IZSLER, che verifichino puntualmente ogni aspetto relativo alla Qualità dei Processi, alla Sicurezza delle Informazioni ed alla Tutela della Privacy. A tal fine si impegna a mettere a disposizione le proprie risorse e a garantire l'accesso alle proprie sedi e la collaborazione fattiva del proprio personale. Si impegna a consentire l'effettuazione di analisi di sicurezza, da parte di IZSLER o Terze Parti fornitrici di servizi di Vulnerability o Risk Assessment, limitatamente alle componenti del Capitolato. Si impegna inoltre, per quanto di sua competenza, a collaborare fattivamente alla esecuzione delle suddette analisi, e a sanare eventuali elementi di vulnerabilità che dovessero emergere.
Inoltre, l'aggiudicatario/fornitore dovrà garantire e monitorare l'applicazione delle prescrizioni descritte anche da parte degli eventuali suoi sub-fornitori, anche attraverso attività di audit.

Come requisiti generali, l'aggiudicatario/fornitore dovrà:

- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite nell'ambito di tutte le attività ad esso affidate;
- Nell'ambito del trattamento dei dati e delle informazioni, ed in particolare nella comunicazione e trasmissione di informazioni, all'interno e all'esterno dell'organizzazione rispettare i principi di:
  - Least privilege;
  - Need-to-know;
  - Segregation of duties.

Inoltre, il Fornitore dovrà:

- Utilizzare i dati personali e le informazioni in modo lecito e secondo correttezza, per scopi legittimi e determinati, nel rispetto del principio di pertinenza e non eccedenza rispetto alle attività svolte;
- Utilizzare i dati personali e le informazioni solo ed esclusivamente per le attività connesse all'esecuzione di quanto richiesto contrattualmente;
- Non trattare i dati personali, ovvero le informazioni, diversi da quelli per i quali è stato espressamente autorizzato;
- Garantire il rispetto della riservatezza, dell'integrità e della disponibilità dei dati personali e delle informazioni adottando tutte le misure, fisiche nonché tecnologiche, di sicurezza idonee;
- Mantenere strettamente riservati i dati personali e le informazioni trattati nello svolgimento di quanto richiesto contrattualmente;
- Non copiare, duplicare, riprodurre o registrare, in qualsiasi forma e con qualsiasi mezzo, i dati e le informazioni, salvo nella misura strettamente necessaria per l'esecuzione dell'attività richiesta e sempre previa autorizzazione scritta da parte del Titolare; al termine delle attività richieste o comunque del contratto, restituire al referente del Titolare i dati e le informazioni oppure, se richiesto e applicabile, procedere alla loro distruzione, con modalità sicure e documentate, fornendone evidenza;
- Nel caso in cui l'attività di manutenzione debba essere svolta all'esterno del Titolare, garantire che i dati personali e le informazioni contenute nei prodotti non siano accessibili;
- Definire ed attuare delle procedure per il loro trattamento e memorizzazione dei dati e delle informazioni. Nello specifico il Fornitore dovrà adottare idonee procedure per la gestione, mantenimento e dismissione dei supporti di memorizzazione contenenti dati, ad esempio implementando metodi di sovrascrittura a più livelli o cancellazione sicura dei supporti. Tutte le attività di dismissione sicura dovranno essere registrate e conservate fornendo al Titolare tutte le evidenze di quanto svolto durante tutto l'arco del contratto;
- Garantire che il proprio personale (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.

È sempre vietata l'estrazione e il trasferimento di dati e/o di ogni altra informazione dalle basi dati e dai sistemi del Titolare, salvo espressa e preventiva autorizzazione scritta.

2.1 Accessi di rete

I cablaggi di rete ed i dispositivi che abilitano collegamenti verso l'esterno utilizzati per assistenza remota, monitoraggio o aggiornamenti automatici dei sistemi dovranno essere esclusivamente quelli forniti dai Sistemi Informativi dell'IZSLER.

Non sono ammesse installazioni di cablaggi e dispositivi di rete o comunicazione di terze parti e/o non approvati esplicitamente dal Responsabile dei Sistemi Informativi ed in nessun caso potranno essere interconnessi alla rete aziendale senza esplicita approvazione del responsabile dei Sistemi Informativi: l'eventuale loro presenza verrà considerata grave violazione delle politiche di sicurezza e comporterà l'immediato sequestro da parte del Responsabile Sistemi Informativi o suo Delegato con possibile denunzia all'Autorità preposta di PS per violazione delle norme sulla tutela dei dati Personali e Sensibili.
Anche le modalità di accesso alle LAN, sia via cavo che wireless/WiFi, sono esclusivamente quelle previste dall'IZSLER e non ne potranno essere accettate di differenti se non dopo valutazione ed accettazione esplicita dei Sistemi Informativi.
In ogni caso dovranno essere rispettate tutte le indicazioni in termini di configurazione, protezione, accessi ed in generale policy gestionali che verranno comunicate dai Sistemi Informativi al fornitore degli apparati, che provvederà alla configurazione prima della loro installazione e messa in esercizio.

2.2 Utenza Amministrativa e Gestione Profili Utente

In caso di soluzioni software e/o programmi applicativi di qualsiasi tipologia, dovrà essere fornita ai Sistemi Informativi un'utenza amministrativa dedicata, e non condivisa con il fornitore, per poter gestire completamente l'applicazione, che il personale dei Sistemi Informativi si impegna ad utilizzare secondo le modalità prescritte dal fornitore.
Lo stesso dovrà avvenire in caso di forniture di server e/o apparati di ogni tipo.
Per tutte le applicazioni complesse le utenze amministrative devono prevedere almeno due livelli funzionali o, in alternativa prevedere la possibilità di selezionare quali funzioni possono essere attribuite ai singoli utenti.
Viene inoltre ritenuta preferibile una soluzione che permetta di gestire gli utenti raggruppati per profili funzionali/operativi, in modo da semplificare e rendere più efficiente la gestione di classi differenziate di utenti senza dover intervenire sulle singole utenze.
La gestione dell'utente e della relativa password dovrà avvenire esclusivamente tramite Dominio Active Directory, accessibile anche tramite protocollo standard LDAP: utenze non nominative e/o non censite nel Dominio AD non sono ammesse.
Si ribadisce che la profilazione delle utenze avverrà esclusivamente sull'applicazione specifica: le informazioni fornite dal Dominio Active Directory saranno di supporto a tale funzione ma in ogni caso saranno univoche e non personalizzabili per singola applicazione.

2.3 Certificazione dei fornitori

Stante la criticità delle forniture oggetto del presente documento, è prerequisito inderogabile che il fornitore possegga tutte le competenze per garantire che l'attività possa essere pienamente realizzata senza possibili inconvenienti, interruzioni, ritardi o altre problematiche legate alle sue capacità.
E' pertanto necessario che le forniture avvengano esclusivamente tramite fornitori che detengano in corso di validità le complete certificazioni dei prodotti utilizzati nelle aree interessate delle attività che dovranno essere eseguite e ne dia piena evidenza, sulla quale l'IZSLER si riserva il diritto di effettuare verifiche.

2.4 Affidabilità delle applicazioni e backup dei dati

Tutte le applicazioni oggetto di forniture dovranno essere progettate e realizzate per garantire la massima disponibilità ed affidabilità.
Dovranno essere previste le procedure per l'implementazione di un sistema di Disaster Recovery ed essere disponibili tutte le funzioni atte a garantire la Business Continuity; l'Istituto si riserva la facoltà di scegliere che la soluzione venga integrata nel sistema di Disaster Recovery e Business Continuity già in uso in IZSLER, rispettando e integrando tali soluzioni.
Per ognuna delle applicazioni software, i sistemi ed i servizi dovranno essere rese disponibili procedure di Backup complete ed esaustive dei dati e, se possibile, delle configurazioni, nonché le modalità di restore, re- installazione e configurazione, comprensive dei pacchetti di installazione completi e della relativa manualistica.
La configurazione del backup delle informazioni previste è ad onere del fornitore del sistema e costituisce parte integrante della fornitura, così come il sistema di backup su nastro o altro sistema dedicato, ferma restando la possibilità dell'IZSLER di scegliere che lo stesso sia effettuato anche su altri sistemi utilizzando le soluzioni già in uso in IZSLER e in ogni caso rispettando le politiche di retention stabilite dall'Istituto.

2.5 Disponibilità dei sistemi, Disaster Recovery e Business Continuity

Tutte le forniture di sistemi complessi dovranno prevedere l'indicazione esplicita dei seguenti parametri relativi all'affidabilità e disponibilità degli stessi:

1. tempo medio fra i guasti (o mean time between failures: **MTBF**)
2. numero di cicli medio fra due guasti (mean cycles between failures: **MCBF**)
3. tempo medio per il ripristino del funzionamento (Mean Time To Restore/Repair: **MTTR**)

Per ogni valore specificato dovranno essere indicati i parametri ed i contesti di riferimento al fine di garantire la loro corretta valutazione.
Analogamente dovranno essere specificati i valori di:

a. **Recovery Time Objective (RTO):** tempo necessario per il pieno recupero dell'operatività del sistema
b. **Recovery Point Objective (RPO)** al fine di definire i punti di sincronizzazione delle attività e lo stato di un sistema ai quali è possibile ricondurre lo stesso in seguito ad un malfunzionamento.

Questi valori rappresenteranno un importante elemento di valutazione tecnico qualitativa delle soluzioni proposte, unitamente al livello degli SLA definiti sia in termine di servizio offerto che di tempi di soluzione delle problematiche che dovessero insorgere (vedi capitolo 5.9).

3. Interoperabilità

3.1 Integrazioni Speciali con Sistemi Istituzionali

Tutte le applicazioni, i servizi ed i sistemi oggetto di fornitura devono garantire la piena e completa integrazione, a pieno carico del fornitore e senza oneri per l'IZSLER, con tutti i sistemi istituzionali tesi a garantire il rispetto di normative locali, nazionali, europee o altri di riferimento.
A titolo di esempio non esaustivo si citano i seguenti sistemi in uso presso l'IZSLER e la PA in generale:

1. identificazione degli utenti esterni tramite SPID (Sistema Pubblico di Identità Digitale) e CIE (Carta di Identità Elettronica) per l'accesso alle funzioni messe a disposizione dall'IZSLER verso la propria utenza (https://www.spid.gov.it/);
2. pagamenti elettronici tramite le modalità e le funzioni previste da Pago PA di AGID (http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/pagamenti-elettronici);
3. l'integrazione, ove necessaria, con le Anagrafi Nazionali e Regionali degli Enti Proposti, quali ad esempio quelle gestite nell'ambito del portale dei Sistemi Informativi Veterinari
4. flussi di dati, a qualsiasi titolo realizzati, previsti in specifici contesti operativi.

Tutte le applicazioni, servizi e sistemi che conducono alla produzione di documenti di tipo sanitario, ad esempio Rapporti di Prova (RdP), prescrizioni, ecc…, devono prevedere la gestione documentale piena ed integrata con i sistemi in uso presso l'IZSLER (in aderenza ad i principi e le disposizioni previste dal CAD, Codice dell'Amministrazione Digitale, D.Lgs. 7 marzo 2005, n. 82 e s.m.i.), compresa la Firma Digitale e l'apposizione della Marca Temporale, ove prevista, e garantire l'assoluta tracciabilità dell'intero processo produttivo e delle operazioni effettuate da ogni utente che vi accede.

3.2 Integrazioni

L'apparecchiatura, il servizio e/o il sistema oggetto della fornitura dovrà essere pienamente integrato all'interno del Sistema Informativo in uso presso l'IZSLER secondo le specifiche fornite dal Sistemi Informativi: i costi di integrazione sono a completo e totale carico dell'aggiudicatario e rappresentano parte integrante della fornitura.
Eventuali costi aggiuntivi dovuti ad adeguamenti tecnologici dell'infrastruttura aziendale necessari per il collegamento dei sistemi oggetto di fornitura sono a totale carico dell'aggiudicatario e nessun onere potrà essere addebitato a qualsiasi titolo alla Stazione Appaltante.
A livello di controllo accessi gli utenti che potranno avere accesso all'applicazione saranno tutti e soli quelli censiti tramite il Dominio Microsoft Active Directory presente in Istituto, al quale i sistemi si dovranno interconnettere per la gestione delle utenze.
A nessun titolo e per nessuna ragione saranno ammesse utenze differenti.
A titolo di esempio non esaustivo sono indicati alcune esempi di integrazioni che si potrebbero rendere necessari (tale elenco non è da considerarsi esaustivo):

1. Anagrafi Centralizzate aziendale.
2. Middleware di integrazione aziendale.
3. Dominio Microsoft Active Directory.
4. Repository sanitario aziendale.
5. Sistema di Firma Digitale.
6. Sistema di Conservazione Legale Sostitutiva.

7. Order Entry Aziendale.
8. Applicazioni specifiche (ove necessario).
9. Sistema Informativo Veterinario Nazionale (VetInfo, https://www.vetinfo.sanita.it/).
10. Sistemi in uso presso la PA Centrale e Locale (per le regioni Lombardia ed Emilia Romagna), quali a titolo di esempio non esaustivo:
    - 10.1. l'identificazione degli utenti (SPID/CIE)
    - 10.2. pagamenti elettronici (Pago PA)
    - 10.3. gestione flussi dati e documentali
    - 10.4. ecc…
11. Ogni altro sistema che presenta collegamenti logico/funzionali con quello oggetto di fornitura.

L'integrazione deve avvenire sulla base delle specifiche in uso presso l'IZSLER e le Linee Guida definite in sede nazionale e delle regioni di interesse.
La piena e completa integrazione è parte integrante della fornitura e ne costituisce prerequisito indispensabile per la sua accettazione e non può prevedere alcun onere aggiuntivo per l'IZSLER: in nessun caso il fornitore/aggiudicatario potrà prevedere ciò con componenti accessorie e/o esterne che richiedano interventi a titolo oneroso, di qualsiasi natura, per l'IZSLER.

4. Architettura hardware e software

4.1 Architettura del software

In quest'area è necessario prioritariamente indicare che ogni pacchetto software, indipendentemente dal suo utilizzo, deve necessariamente rispettare i principi guida ed ogni altra indicazione prevista da AGID nel Piano Triennale (vedi [1]) nonché rispettare l'articolato previsto da CAD (Codice dell'amministrazione Digitale, vedi [2]): il contenuto di tali norme è da considerarsi qui integralmente e completamente richiamato.
Il software deve prevedere che l'interazione da parte dell'utente avvenga sulla postazione in cui sta fisicamente operando: non sarà possibile pilotare postazioni situate all'interno dell'IZSLER dall'esterno, ma sarà compito del software gestire le opportune fasi di lettura, scrittura e presentazione dei dati tramite opportuni protocolli di scambio e interfacce dedicate a tale scopo.
Archivi che gestiscono la memorizzazione di dati storici o che contengono informazioni necessarie al funzionamento dell'intero sistema devono essere residenti su supporti di memorizzazione dedicati a tale scopo: l'ubicazione deve necessariamente essere presso la sala server aziendale o su risorse cloud gestite da IZSLER e l'accesso essere regolato secondo le policy in uso presso l'IZSLER.
Tutte le informazioni devono essere gestite in modalità storicizzata, ossia deve sempre essere possibile risalire allo stato del sistema ad un determinato momento attivando livelli ulteriori di log qualora si rendesse necessaria un'analisi ulteriore dello stato e del comportamento del sistema.
Tutti gli accessi alle informazioni dovranno essere controllati, gestiti e memorizzati conformemente alle indicazioni normative sulla privacy, le linee guida regionali ed aziendali in tale ambito.
I server applicativi dovranno rispondere ai requisiti stabiliti dall'IZSLER a seconda del livello di complessità e criticità del sistema e definiti nel paragrafo seguente: eventuali costi aggiuntivi derivanti da tale implementazione sono a carico dell'aggiudicatario.
Si tenga presente che l'implementazione di particolari sistemi dovrà prima prevedere la valutazione delle funzionalità offerte con la possibilità di scegliere la soluzione tecnica ottimale, riservando la possibilità di trasferire informazioni agli strati software di livello superiore anziché gestire internamente l'intera interfaccia; tale richiesta è determinata dall'esigenza di minimizzare il numero di sistemi e di passaggi per l'utente durante l'intero flusso di lavoro.
Infine, per quello che riguarda ogni aspetto documentale e di comunicazione gestito dal Software, si fa presente che dovranno essere tenuti in considerazione tutti gli aspetti previsti nell'ambito del CAD, Codice dell'Amministrazione Digitale.
Per quello che riguarda le singole componenti Software oggetto della fornitura, dovrà essere garantita la piena operatività dell'intero sistema per tutta la durata del contratto.
E' facoltà del fornitore procedere al rinnovamento tecnologico del parco installato nel corso del periodo di validità, operazione che dovrà avvenire garantendo la piena continuità di servizio, in assenza di oneri per l'IZSLER e senza interruzioni operative.
In particolare si pone l'attenzione sulle possibili componenti che possano uscire dal supporto del produttore nel corso della fornitura: in questo caso, qualsiasi sia la componente oggetto di tale evenienza (compresi Sistema Operativo, Driver di Periferiche, sottosistemi e librerie SW ed ogni elemento, modulo o componente anche accessorio presente), il fornitore è tenuto a procedere all'adeguamento dell'intero sistema e di tutte le componenti interessate o influenzate dallo stesso a suo totale carico, garantendo la piena e completa funzionalità operativa e senza alcun tipo di onere per l'IZSLER.

4.2 Reportistica ed estrazione dati

Al fine di garantire la piena disponibilità dei dati prodotti, il sistema oggetto di fornitura dovrà garantire le seguenti funzioni:

1. Piano per la piena disponibilità ed estrazione (anche in background/automatico) di tutti i dati memorizzati sotto forma di DB relazionale pienamente documentato o di tabelle estese liberamente fruibili dagli utenti.
2. Reportistica completa e modificabile in almeno due formati (PDF ed excel/doc) con pieno accesso a tutti i dati ed operazioni di aggregazione.
3. Modulo di estrazione capace di funzionare in background/automatico con tracciatura degli esiti.
4. Interfaccia di accesso al DB dall'esterno dell'applicazione.
5. Interfaccia per la definizione di query di estrazione
6. Rendicontazione completa ed esaustiva di tutti gli accessi al pacchetto, comprensiva dei tentativi falliti e le relative motivazioni.

Tali funzioni dovranno essere separatamente configurabili per diverse tipologie di utenti e non richiedere necessariamente tutte un'utenza amministrativa.

4.3 Architettura Server e sistemi Hardware

L'aggiudicatario si impegna a fornire tutte le componenti previste dall'architettura server impiegata per il progetto, ciò non di meno si evidenzia che tutte le componenti hardware, sistema operativo, installazione, licenze RDBMS e tutte le altre licenze che fossero necessarie, oltre che la manutenzione di ciascuna di esse, saranno a carico dell'aggiudicatario.
Tutti i sistemi forniti e le relative componenti dovranno essere allineati allo stato dell'arte al momento dell'installazione ed in nessun caso potranno essere presi in considerazione apparati per i quali ne sia stata annunciata l'uscita di produzione (fase-out).
E' facoltà del fornitore procedere al rinnovamento tecnologico del parco installato nel corso del periodo di validità, operazione che dovrà avvenire garantendo la piena continuità di servizio, in assenza di oneri per l'IZSLER e senza interruzioni operative, salvo diversamente concordato in modo formale; il rinnovo tecnologico sarà considerato obbligatorio nel caso di adeguamenti imposti dalla normativa.

Tutti i server e le relative applicazioni dovranno essere progettati per operare in un contesto di Business Continuity e Disaster Recovery prevedendo le opportune forme di clusterizzazione e ridondanza delle componenti; tutti gli elementi critici dovranno prevedere parti di scorta calda e la sostituibilità a caldo (a titolo di esempio non esaustivo: dischi, alimentatori, ventole, ecc…).
La configurazione del sistema dovrà essere tale da garantire inoltre il massimo livello di prestazione nelle proprie funzioni e nell'accesso ai dati, e dovrà essere dimensionata per garantire il mantenimento on line delle informazioni per un periodo almeno doppio rispetto alla durata del contratto.
Dovranno inoltre essere definite ed implementate le politiche di Backup dei dati e delle configurazioni dell'intero sistema in modo da consentire il pieno e completo ripristino del sistema senza perdita di dati: il sistema di Backup, compresa la sua configurazione, è parte integrante della fornitura ed è a totale carico dell'aggiudicatario.
Il sistema dovrà essere protetto con una soluzione antivirus/antimalware costantemente aggiornata, il sistema stesso dovrà essere allineato con i rilasci di sicurezza come previsto dalla normativa in vigore; la responsabilità dell'aggiornamento della fornitura è a totale carico del fornitore.

Sarà inoltre considerato elemento preferenziale la possibilità di ospitare i sistemi server su macchine virtuali di almeno due differenti fornitori, quali ad esempio Microsoft o VMWARE, a condizione che tale possibilità sia certificata o garantita a totale onere del fornitore.
I sistemi server dovranno essere dotati di un proprio gruppo di continuità gestito (UPS) via software ed in grado di garantire un'operatività minima di 15 minuti, di concludere le operazioni in corso e procedere all'ordinato spegnimento della macchina e dei sistemi su di essa residenti, comunicando lo stato dell'alimentazione, gli eventi occorsi, l'avvenuta chiusura di procedura di spegnimento e l'eventuale riattivazione.
Tali sistemi di alimentazione di emergenza dovranno disporre nativamente di interfaccia LAN ed essere integrabili in un impianto di monitoraggio e controllo remoto come da specifiche fornite dai Sistemi Informativi.
IZSLER si riserva la facoltà di scegliere che la soluzione fornita venga realizzata utilizzando le proprie risorse elaborative, di storage, di antivirus/antimalware e di backup.

4.4 UPS

Oltre a quanto già previsto per i sistemi Server e ad integrazione di ciò, se richiesto dalla particolare criticità del sistema, anche le postazioni di lavoro (PdL) dovranno essere dotate di un proprio gruppo di continuità gestito via software ed accessibile via LAN, la cui scheda di interfaccia deve essere presente ed integrata sull'apparato, ed in grado di

1. garantire un'operatività minima di 15 minuti,
2. di concludere le operazioni in corso
3. di procedere all'ordinato spegnimento della macchina.

4.5 Architettura Cloud/ASP

Qualora il servizio offerto comprenda una componente implementata con un'architettura di tipo Cloud e/o ASP, sarà necessario che vengano correttamente definiti ed esplicitati i seguenti aspetti:

a. Garanzia del corretto adempimento di tutte le norme, direttive e linee guida in merito al rispetto della privacy e la protezione dei dati personali e sensibili
b. Integrazione con il sistema di Autenticazione Microsoft Active Directory presente in azienda e/o gestione delle credenziali degli utenti, che devono comunque rispettare i criteri generali espressi in questo documento e le norme e linee guida di riferimento
c. Modalità di gestione del backup dei dati e loro disponibilità per l'IZSLER su supporto fisico, che dovrà essere sempre garantito senza alcun onere per un numero minimo di richieste non inferiore a 4 per ogni anno di fornitura/contratto
d. Livelli di disponibilità del servizio, SLA garantiti e strumenti di monitoring del sistema a disposizione dell'IZSLER
e. Utilizzo di soli protocolli sicuri per l'accesso, la comunicazione o lo scambio di dati (quali ad esempio thhps, sftp, ecc…)
f. Banda richiesta per ogni utente connesso ed ogni altro parametro necessario a definire le caratteristiche che il sistema di connessione dovrà possedere
g. Altri parametri minimi richiesti dall'applicazione quali, a titolo di esempio non esaustivo, tempi di latenza e QoS (Quality of Service) e necessari per garantire una corretta fruizione dell'applicazione.
h. Tempi garantiti di risposta per le principali operazioni.

Nel caso di tali tipologie di fornitura/servizio l'aggiudicatario/fornitore si deve rendere disponibile ad effettuare autonomamente e sotto il controllo dei Sistemi Informativi eventuali test e verifiche sul corretto funzionamento del sistema in caso di segnalazione di anomalie di funzionamento senza oneri aggiuntivi per l'IZSLER.
Alla conclusione del servizio, il fornitore dovrà realizzare ogni aspetto necessario per il trasferimento delle risorse a IZSLER o al nuovo fornitore senza oneri aggiuntivi per l'Istituto.
Resta facoltà di IZSLER la decisione di implementare la soluzione sulle proprie risorse cloud e/o su architetture compatibili con esse.

5. Gestione della fornitura

5.1 Avvio della Fornitura e relazione con Sistemi Pregressi

Per ogni fornitura di apparecchiatura, servizio o sistema sarà onere e cura del fornitore subentrante assicurare la migrazione nel nuovo sistema di tutti i dati e le informazioni dal precedente impianto che assicurava le stesse funzioni al fine di garantire la piena continuità operativa e la corretta storicizzazione e confrontabilità dei dati, senza comportare alcun onere aggiuntivo per l'IZSLER.
In sede di offerta i proponenti dovranno esplicitamente prevedere questa fase indicando tempi, modi ed eventuali limitazioni presenti: queste ultime non potranno in nessun modo riguardale la profondità storica del dato o lo svolgimemto di tale attività ma solo ed esclusivamente essere limitate alle differenze strutturali degli applicativi relativamente alle informazioni gestite.
I Sistemi Informativi dell'IZSLER si impegnano a supportare ed agevolare tale attività, che sarà parte integrante ed imprescindibile della fornitura stessa, e sarà oggetto di valutazione e collaudo.

5.2 Sviluppi Software commissionati

In tutti i casi in cui la fornitura si riferisce, anche parzialmente, allo sviluppo di specifici pacchetti SW esplicitamente definiti da IZSLER tramite proprie specifiche tecnico/funzionali, l'Istituto Zooprofilattico detiene la piena e completa titolarità di ogni diritto sul software sviluppato.
I sorgenti ed ogni altro diritto derivante dallo sviluppo appartiene in via esclusiva all'IZSLER e nessun utilizzo di quanto sviluppato potrà essere utilizzato in assenza di esplicita richiesta formale e relativo consenso scritto da parte dell'Istituto.
Lo sviluppo dovrà avvenire con modalità, metodi e strumenti indicati dall'IZSLER: eventuali costi ed oneri relativi a licenze di strumenti e moduli o ogni altro elemento necessari per lo sviluppo sono a completo onere del fornitore, e saranno oggetto di fornitura e dovranno essere allineate alle ultime versioni disponibili al momento della chiusura del contratto di fornitura.
Per quello che riguarda il layout delle applicazioni ed il tema dell'accessibilità delle stesse, lo sviluppo dovrà avvenire coerentemente con quanto previsto da ACN ed AGID in queste tematiche e nel pieno rispetto delle linee guida emessi da tali enti o da altri del medesimo ambito.
Tutti i sistemi forniti dovranno essere allineati allo stato dell'arte al momento dell'installazione ed in nessun caso potranno essere prese in considerazioni strumenti, metodi o altro per i quali ne sia stata annunciata l'uscita di supporto.
L'aggiudicatario si impegna a consegnare come parte integrante della fornitura tutti codici sorgenti ed i moduli/strumenti ad essi collegati, completi di una documentazione esaustiva di tutte le componenti, su tutte le aree relative, quali, a titolo di esempio non esaustivo:

1. documentazione del SW sviluppato, interfacce e librerie utilizzato;
2. manuale utente;
3. amministrazione, installazione e manutenzione del sistema.

Infine si richiama quanto previsto dagli articoli 68 e 69 del Codice dell'Amministrazione Digitale, che disciplina le modalità con cui una Pubblica Amministrazione può acquisire software e sanciscono l'obbligo di rilasciare con licenza aperta il software da essa sviluppato o commissionato, per cui sarà obbligatorio per il fornitore della soluzione procedere alla sua pubblicazione completa come da linne guida in vigore al momento della pubblicazione (vedi https://developers.italia.it/it/riuso.html)

5.3 Capoprogetto e SAL

L'aggiudicatario si impegna a definire un gruppo di lavoro indicando all'inizio delle attività il responsabile della commessa (Capoprogetto) che sarà il referente unico dell'IZSLER per ogni aspetto inerente il progetto: egli potrà avvalersi delle figure professionali che riterrà opportuno coinvolgere: in tal caso ne dovrà essere data tempestiva comunicazione al/ai referenti dell'IZSLER.
Dovrà essere redatto un piano di lavoro che comprenda almeno tutte le fasi della commessa come descritte dal capitolato unitamente a tutti i momenti di verifica e rendicontazione (SAL Stato Avanzamento Lavori) che si ritengono necessari, compreso un Gantt aggiornato in formato compatibile con MS-Project.
Il Capoprogetto dovrà provvedere alla gestione di tutti gli aspetti connessi con la fornitura oggetto del presente capitolato e dovrà provvedere all'aggiornamento periodico dello Stato Avanzamento Lavori nei confronti del/dei referenti dell'IZSLER con intervalli non superiori alle 2 settimane.

5.4 Collaudi

Per ogni fornitura che preveda l'integrazione con i Sistemi Informativi sono previste le seguenti fasi di collaudo, da attuarsi secondo le procedure specifiche di ogni fornitura:

1. alla verifica e messa in funzione del sistema;
2. al collaudo di tutte le apparecchiature oggetto della fornitura;
3. alla piena e completa verifica funzionale in condizioni di esercizio simulando diversi cicli di funzionamento anche in condizioni di stress.

Il collaudo verificherà:

a. la corrispondenza tra le caratteristiche funzionali e tecniche dichiarate e quelle riscontrate;
b. l'avvenuta esecuzione delle sessioni di formazione per le diverse tipologie di utenti dell'Azienda;
c. l'interconnessione di tutte le componenti del sistema con la LAN aziendale e la piena raggiungibilità da essa;
d. la correttezza di funzionamento di tutti i sottosistemi e del sistema nel suo complesso.

Il collaudo avverrà sulla base di un piano di lavoro contenente modalità e tempistiche per ogni tipologia di test, i casi d'uso coperti dal test e le funzionalità impattate; sulla base di quanto definito nei singoli capitolati in considerazione delle caratteristiche dell'oggetto della fornitura, tale piano sarà redatto:

- dai referenti dei Sistemi Informativi congiuntamente al DEC ed ai referenti di tutti gli enti aziendali interessati, e condiviso con il Capoprogetto dell'Azienda Aggiudicataria e dovrà essere adeguatamente documentato in ogni sua fase;
- dal Fornitore. In tal caso, IZSLER potrà accettare il Piano o richiedere modifiche/integrazioni, che il Fornitore dovrà recepire e presentare nuovamente il Piano.

Il Collaudo è prerequisito necessario per l'entrata in esercizio dell'impianto e per poter procedere alla fatturazione delle attività, con la sola eccezione dei casi esplicitamente previsti nei documenti di gara: in ogni caso i Sistemi Informativi dell'IZSLER non forniranno il proprio assenso alla liquidazione fino al superamento del collaudo e della risoluzione delle prescrizioni in esso contenute.

5.5 Documentazione

Presso gli Uffici del Sistemi Informativi sono disponibili tutti i documenti che regolano le richieste per l'accesso alla rete aziendale da parte di utenti, aziende ed apparati, che dovranno essere restituiti

debitamente compilati in originale e firmati da un Legale Rappresentante dell'aggiudicatario onde ottenere gli accessi richiesti.
Sono parte integrante di ogni fornitura i set completi della documentazione utente ed amministrativa in formato elettronico: queste dovranno essere allineate alle consegne ed essere aggiornate almeno una volta all'anno con tutte le modifiche apportate.
Per ogni altra informazione in merito alla documentazione necessaria e/o disponibile, o esigenza di approfondimento che si rendesse necessaria si rimanda ai canali previsti dalle singole forniture.
Tutta la documentazione dovrà essere redatta in lingua italiana o in inglese: qualora il manuale utente non fosse disponibile in lingua italiana, dovrà comunque essere fornito un estratto contenente le funzioni principali redatto in lingua italiana da parte del fornitore.

5.6 Manualistica

Il fornitore si deve impegnare a consegnare copia cartacea ed elettronica di tutta la documentazione utente ed amministrativa del sistema oggetto di fornitura prima della messa in esercizio del sistema oggetto di fornitura, correttamente personalizzata per la propria installazione, comprensiva del dettaglio della configurazione adottata.
Tutti gli aggiornamenti previsti ed effettuati a qualsiasi titolo dovranno necessariamente prevedere anche l'adeguamento della documentazione fornita, che dovrà costantemente essere allineata allo stato del sistema in esercizio.
La documentazione dovrà essere fornita preferibilmente in lingua italiana o, in alternativa, in lingua inglese: non sono ammesse altre lingue in alcuna delle parti.

5.7 Certificazioni

Sulla base delle specifiche commesse, i Sistemi Informativi potranno procedere a richiedere specifiche certificazioni inerenti le attività oggetto del lavoro commissionato.
Anche quando non previste esplicitamente come requisito del Capitolato d'Oneri, le certificazioni pertinenti le attività richieste saranno considerate fattore preferenziale a parità di ogni altra condizione.
Saranno inoltre considerate fattore preferenziale al pari di migliorie della proposta, anche ove non esplicitamente richieste, il possesso di certificazioni ISO di ordine generale, esposte tramite il relativo certificato, quali quelle appartenenti alle famiglie:

1. ISO 9000
2. ISO 14000
3. ISO 20000
4. ISO 27000
5. ISO 31700

La valutazione delle certificazioni possedute, che dovranno essere allineate alle ultime versioni emesse, sarà oggetto di esame della commissione che ne valuterà impatto e rilievo sulla base delle specifiche richieste.

5.8 Assistenza e SLA

Per quello che riguarda l'assistenza del sistema, sulla base dell'importanza e criticità dello stesso, questi sono i livelli minimi richiesti di assistenza (SLA), qualora non siano diversamente definiti in sede di Capitolato Tecnico specifico della fornitura:

1. **Problema Bloccante**: intervento in 2/4 ore, soluzione e ripristino in 4/8 ore.

2. **Problema grave**: intervento in 8 ore lavorative e ripristino entro 16 ore lavorative

Problema non grave: intervento entro 3 giornate lavorative e ripristino nelle successive 2 giornate lavorative.Ogni attività manutentiva dovrà essere accompagnata da un rapporto che indichi tutte le informazioni dell'intervento eseguito quali, a titolo di esempio non esaustivo:

a. data e durata dell'intervento,
b. evento generante,
c. dati di chi ha segnalato l'anomalia,
d. operatori intervenuti,
e. operazioni effettuate,
f. avvenuta risoluzione della segnalazione e/o eventuali operazioni successive che si rendessero necessarie.

Sulla base della criticità dell'impianto potranno essere richieste forma di assistenza con orario esteso, anche nella forma H24 per 365 giorni/anno.

In sede di definizione del contratto potranno meglio essere definiti gli eventuali oneri legati alle singole operazioni di intervento che dovranno essere chiaramente definiti e dettagliati in sede di Capitolato e di offerta relativa comprensivi di tutte le potenziali voci richiamabili.

Eventuali interventi da remoto potranno essere consentiti nell'eventualità che l'aggiudicatario si allinei alle Policy di sicurezza in uso nell'IZSLER: anche in questo caso dovrà essere emesso un rapporto completo di intervento.

Tutte le attività di assistenza dovranno essere accompagnate da idonea reportistica, definita nel dettaglio con il Direttore di Esecuzione del contratto, che comprenda almeno le seguenti informazioni per il periodo definito nel contratto, tipicamente mensile:

1. Riepilogo delle attività svolte nelle diverse modalità di erogazione e dei tecnici coinvolti
2. Rispondenza delle attività agli SLA definiti nel contratto
3. Rapporto riepilogativo per ogni intervento effettuato a fronte di segnalazione di malfunzionamento comprensivo delle attività svolte e dei tecnici coinvolti

5.9 Penali

Accanto a quanto specificatamente indicato dal Capitolato per la singola procedura, ogni fornitura di componenti che interessa i Sistemi Informativi dovrà prevedere una sezione di Penali da attuarsi specificatamente per l'area di specifica competenza, situazione che deve essere definita anche in occasione di attivazione/rinnovo di contratti di manutenzione.

In particolare in caso di ritardo e/o irregolarità nella fornitura, nell'installazione, negli interventi di manutenzione, nel ripristino del sistema, nonché per qualsiasi inadempienza rispetto alle prescrizioni del capitolato, del presente documento o dell'offerta quando migliorativa e di maggior favore, non dovuti a forza maggiore, bensì imputabile a responsabilità della Ditta Aggiudicataria, dovrà essere prevista l'applicabilità, a giudizio insindacabile dell'IZSLER, di almeno le seguenti tipologie di penali pecuniarie sui ritardi nelle operazioni:

1. per ogni giorno solare nel completamento della fornitura;
2. per ogni ora/giorno nell'intervento da remoto oppure on site, misurata sui singoli episodi;
3. per ogni ora/giorno nel ripristino del sistema, misurata sui singoli episodi.

5.10 Conclusione della Fornitura

Al termine del periodo di fornitura ed alla dismissione dell'impianto il fornitore si impegna a supportare con piena e completa collaborazione, anche documentale, l'estrazione di tutti dati

applicativi ed operativi secondo un tracciato definito di comune accordo con l'IZSLER, affinché i dati relativi possano essere adeguatamente storicizzati e consultati su altro sistema aziendale.
Copia di tutte le informazioni ed i dati dovranno essere consegnati in forma tabellare al Sistemi Informativi unitamente alla documentazione, almeno in formato elettronico, per la loro interpretazione, lettura ed eventuale caricamento: per dimensioni di dati considerevoli potranno essere congiuntamente definiti caricamento dei dati su DBMS scelti dal Sistemi Informativi sulla base delle dotazioni disponibili.
In caso di avvicendamento fra fornitori o subentro del personale dell'IZSLER nella gestione della fornitura, è altresì onere del fornitore in uscita fornire tutta la necessaria assistenza ed affiancamento al fornitore entrante (o al personale dell'IZSLER qualora sia questo a subentrare) affinché possa avvenire un pieno e completo passaggio di consegne e garantire la piena continuità operativa.
In particolare, la fase di conclusione della fornitura prevede i seguenti aspetti:

- Fornitura del servizio e delle modalità di garanzia di continuità nella fase di trasferimento;
- Gestione del processo di trasferimento: ruoli, responsabilità, autorizzazioni e risorse da assegnare;
- Diritti di proprietà intellettuale: accordi necessari, licenze, codice (ove previsto), etc.;
- Due diligence: definizione della documentazione e dei contenuti da trasferire ad un altro Fornitore subentrante, nonché la definizione delle altre obbligazioni e penalità previste;
- Contratti e licenze;
- Sicurezza;
- Piano di comunicazione.

Il Fornitore si deve impegnare durante la fase finale, fino al termine del periodo contrattuale a soddisfare i seguenti requisiti generali:

- Non vi saranno impatti o interruzioni del servizio causate specificamente dalle attività di passaggio di consegne;
- Non vi saranno decadimenti dei livelli di servizio, specificamente imputabili al passaggio delle consegne e all'affiancamento del personale del Fornitore con quello subentrante;
- Dal punto di vista dell'utente finale, non vi saranno significativi cambiamenti, specificamente imputabili al passaggio delle consegne, che possano inficiare le attività operative.

Il passaggio di consegne e dei dati dovrà essere correttamente pianificato attraverso un apposito piano operativo e prevedere la redazione e consegna a cura del fornitore uscente, di tutta la documentazione ritenuta necessaria dall'IZSLER.
Tali fasi operative sono da considerarsi parte integrante della fornitura e non devono comportare alcun onere aggiuntivo per l'IZSLER.

A. Appendice: check list di integrazione.

A supporto delle attività di verifica della rispondenza della fornitura sono state definite delle check-list che sintetizzano le richieste verso i fornitori allo scopo di semplificarne le risposte.
Tali check-list non sostituiscono comunque l'adesione a quanto definito nell'intero documento.

1.1. Punti principali da considerare per l'integrazione di uno strumento alla rete.

Nel seguito della nota si indicherà genericamente con il termine sistema il PC di interfaccia e/o lo strumento che devono essere connessi alla LAN dell'IZSLER

1. Il sistema deve essere messo in Dominio Active Direscory, cambiando il nome della macchina in PC-inv (dove "PC" sta per computer desktop e "inv" è il n° di inventario del computer): in caso di numero di inventario non disponibile verrà assegnata una numerazione interna. Qualora il sistema sia attivato prima degli interventi di messa a Dominio AD, Antivirus, ecc... sarà necessaria una sessione congiunta con il fornitore di verifica della sua corretta operatività al termine di queste attività (la messa a Dominio) in modo da dare certezza del funzionamento dell'impianto o, nella peggiore delle ipotesi, riconfigurare il sistema fuori rete.
2. Sul sistema deve essere installato l'antivirus, in IZSLER si utilizza Sophos Endpoint Agent, ma il fornitore può offrire altro primario sistema di protezione, di classe professionale: in tal caso con aggiornamento a sue spese. Nel caso in cui l'antivirus sia installato successivamente all'attivazione del sistema, sarà comunque necessaria la scansione completa del sistema, senza esclusioni, in modo da assicurarsi che non siano già presenti infezioni; eventuali segnalazioni dell'antivirus relative alle directory da escludere saranno valutate con il fornitore; successivamente verranno applicate le esclusioni richieste.
3. Non sono ammesse utenze locali o di dominio generiche né privilegi di amministratore, che possono essere concessi limitatamente e su richiesta per consentire attività di installazione e/o manutenzione. I privilegi di amministratore potranno essere concessi al bisogno dall'assistenza IZSLER. Relativamente alla necessità di operare su una sessione di lavoro che potrebbe interessare più utenti anche su più giorni, è disponibile una modalità operativa specifica (chiamata UMS) che permette di gestire il sistema garantendo la continuità operativa, opzione da valutare congiuntamente a fornitore e reparto
4. Eventuali utenze locali presenti sul sistema vengono disabilitate automaticamente per policy aziendale
5. Gli aggiornamenti di sicurezza del Sistema Operativo (SO) sono obbligatori come da indicazioni del fornitore di questo (Microsoft o altri). L'avvio automatico a fronte di un aggiornamento di sistema dovrà essere disabilitato, prevedendo però un avviso per l'utente che il PC richiede il riavvio; tale avviso potrà essere ignorato solo un numero limitato di volte, dopo di che sarà necessario e potrà bloccare il funzionamento del pc stesso: occorre tener presente che la sequenza di riavvio sarà tanto più lunga quanto maggiore sarà il numero di avvisi ignorati ed eventuali altri aggiornamenti da installare scaricati dall'ultimo riavvio: su questa modalità operativa non c'è alcuna possibilità di intervenire.
6. L'eventuale firewall locale è aggiornato con le policy di dominio: occorre evitare sul firewall del sistema aperture generiche verso l'esterno, che potrebbero essere successivamente chiuse automaticamente dalle policies aziendali.
7. Occorre fornire le opportune indicazioni per la gestione del backup dei dati prodotti.
8. Qualora fosse necessario l'accesso remoto al sistema, questo è consentito tramite VPN con l'indicazione di un titolare della connessione del quale ci vanno forniti i documenti (d'identità

e CF) per la creazione dell'utenza relativa o, in alternativa, tramite Assistenza Rapida di Windows (tracciata via Firewall).

9. Le regole di cui sopra valgono per tutti i Sistemi Operativi, compresi i sistemi Linux o con altri Sistemi Operativi.

1.2. Punti principali da considerare per la gestione dei dati di uno strumento.

Per quello che riguarda le informazioni da acquisire relativamente alla richiesta di salvataggio in rete dei file/dati prodotti da uno strumento è necessario acquisire le seguenti informazioni minime:

a. dimensione dei file (min, media, max)
b. quanti sono i file e la loro tempistica di produzione
c. per quanto tempo devono essere conservati (mesi, anni,…)
d. chi deve accedervi (in Izsler o anche fuori)
e. eventuale migrazione degli stessi su Cloud
f. dimensione dei file da trasferire e/o leggere sul cloud (min, media, max)
g. frequenza di accesso dei file da trasferire e/o leggere sul cloud (quotidianamente/settimanalmente)
h. quale è il tasso di modifica dei file
i. qualora il dato dovesse essere modificato, indicare se è necessario mantenete più versioni dello stesso file o mantenete solo l'ultimo.

Le stesse informazioni devono essere acquisite in caso il fornitore proponga un proprio servizio di archiviazione, con in più le informazioni su

i. i sistemi di sicurezza adottati
ii. le politiche di backup
iii. la possibilità e le modalità di scarico dei dati salvati
iv. la locazione geografica dei dati salvati
v. l'eventuale accesso di terzi a tali dati