REGIONE DEL VENETO

Regione del Veneto

REGIONE DEL VENETO

PROCEDURA APERTA TELEMATICA, EX ART. 71 D.LGS. N. 36/2023, PER L'ACQUISIZIONE DI SERVIZI DI GESTIONE DELLE INFRASTRUTTURE IT E SICUREZZA INFORMATICA DELLA REGIONE DEL VENETO - GIUNTA REGIONALE

CUP: H77H25001220002

CODICE GARA: G02766

CAPITOLATO SPECIALE D'APPALTO

Indice

1. PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI GESTIONE DELLE INFRASTRUTTURE IT E SICUREZZA INFORMATICA – PREMESSA

Il presente capitolato disciplina i requisiti e le condizioni per la procedura aperta finalizzata all'affidamento dei servizi di Gestione delle Infrastrutture IT e Sicurezza informatica di Regione del Veneto, Giunta Regionale.

Le specifiche tecniche e i requisiti minimi elencati rappresentano gli standard che i fornitori dovranno garantire per la corretta erogazione dei servizi richiesti. L'oggetto della procedura è la fornitura dei SERVIZI DI GESTIONE DELLE INFRASTRUTTURE IT E SICUREZZA INFORMATICA articolati in: "Servizi conduzione operativa sistemi e sicurezza", "Servizi di supporto", "Servizi di gestione operativa", "Servizi di sicurezza aggiuntivi rispetto alla conduzione" e "Servizi di gestione licenze".

La documentazione di gara regola integralmente i termini e le condizioni che i soggetti aggiudicatari dovranno rispettare per l'erogazione dei servizi. La partecipazione alla presente procedura implica l'accettazione di tutte le condizioni descritte nel capitolato, e l'aggiudicatario sarà vincolato al rispetto dei requisiti qui descritti.

In caso di variazioni o aggiornamenti ai requisiti o alle modalità di esecuzione, prevarranno le disposizioni specifiche riportate in eventuali documenti integrativi, come indicato dal Responsabile Unico del Progetto.

1.1 Appendici

Sono parti integranti del presente Capitolato Tecnico le seguenti appendici:

- **Appendice 1 Indicatori di qualità:** contenente gli indicatori di qualità della fornitura e le penali previste per il mancato rispetto degli stessi;
- **Appendice 2 Profili Professionali:** contenente i requisiti professionali delle risorse da impiegare nella fornitura;
- **Appendice 3 Contesto Tecnologico e Applicativo:** contenente la descrizione del contesto infrastrutturale e applicativo dell'Amministrazione.

1.2 Acronimi e definizioni

Nel corpo del presente Capitolato Tecnico, con il termine:

ACRONIMI E DEFINIZIONI	DESCRIZIONE
AgID	Agenzia per l'Italia Digitale.
Amministrazione	Regione del Veneto come stazione appaltante.
Applicazione	Qualsiasi realizzazione software tesa a fornire all'Amministrazione un insieme di funzionalità strettamente collegate. Solitamente una applicazione è composta da uno o più moduli software e da un database a cui l'applicazione fa riferimento.
Baseline del sistema	Versione formalmente approvata degli elementi della configurazione del sistema, indipendentemente dal supporto di registrazione, formalmente descritta e fissata in un momento specifico del ciclo di vita del sistema.

Capitolato Speciale d'appalto	Capitolato Tecnico.
CAD	Codice dell'Amministrazione Digitale.
CERT	Computer Emergency Response Team
DATA CENTER	Centro Elaborazione Dati.
CMDB	Configuration Management Data Base.
CMS	Content management system.
CPU	Central Processing Unit.
CRM	Customer relationship management.
CT	Capitolato Tecnico.
DAS	Direct Attached Storage.
DBMS	Data Base Management System.
DEC	Direttore dell'Esecuzione del contratto di RV.
DR	Disaster Recovery.
ECM	Enterprise content management.
ETL	Extract, Transform, Load.
Fornitura	Complesso delle attività e dei servizi che la RV richiede.
FTE	Full Time Equivalent, ovvero 210 giorni annui a persona.
GG/PP	Giorno persona (tempo spesa a consumo).
GA	Servizio di gestione applicativa e basi dati.
HD1°livello	SPOC, single point of contact- assistenza di 1° livello.
HD2°livello	Servizio di Assistenza di 2° livello.
HW	Hardware.
ICT	Information & Communication Technology.
IMAC	Install, Move, Add, Change.

IPS	Intrusion Prevention System.
IPSec/VPN	Virtual Private Network realizzata tramite protocollo IPSec.
KPI	Key Performance Indicator.
LAN	Local Area Network.
NAS	Network Attached Storage.
MAD	Manutenzione adeguativa.
MAC	Manutenzione correttiva.
MEV	Manutenzione evolutiva.
OE	Offerta economica vincolante del Fornitore Aggiudicatario.
OT	Offerta tecnica vincolante del Fornitore Aggiudicatario.
PA	Pubblica Amministrazione.
PdL	PC desktop o notebook, a cui sono associate una o più periferiche.
QoS	Quality of Service.
RPO	Recovery Point Objective: parametro, normalmente espresso in ore o minuti, che rappresenta la quantità massima di perdita dati che si ritiene accettabile a seguito della ripartenza presso il sito alternativo, a seguito di un disastro. Pur essendo una quantità di dati, esso viene espresso mediante unità di tempo in quanto esprime il massimo ritardo della copia dati presente sul sito alternativo rispetto ai dati di produzione, dipendente dalla modalità adottata per la replica.
RTO	Recovery Time Objective: parametro, normalmente espresso in ore, che rappresenta il tempo massimo richiesto per la ripartenza dei servizi sulla infrastruttura tecnologica predisposta presso il sito remoto di DR.
RUAC	Responsabile Unico delle attività Contrattuali del Fornitore.
RUP	Responsabile Unico del Progetto della RV.
RV o RVE	Regione del Veneto, Direzione ICT e Agenda Digitale.
SAN	Storage Area Network.
SD	Service Desk.
SIEM	Security Information and Event Management.

SLA o LdS	Service Level Agreement/ Livelli di Servizio.
SOC	Security Operation Center.
SOS	Struttura Organizzativa Stabile.
SPC	Servizio Pubblico di Connettività.
SSL	Secure Socket Layer.at
SVI	Sviluppo SW.
SW	Software.
TT	Trouble Ticketing.
VPN	Virtual Private Network.
WAN	Wide Area Network.

Tabella 1 - Acronimi e definizioni

2. CONTESTO DELLA PROCEDURA APERTA

2.1 Contesto organizzativo

Direzione ICT, Agenda Digitale e SOS affidamento servizi e forniture ICT eroga servizi finalizzati alla cultura digitale, alle infrastrutture, all'interoperabilità e sicurezza informatica, al coordinamento, attuazione e monitoraggio dell'Agenda digitale del Veneto.

La Direzione è oggi organizzata in due Unità Organizzative ed un ufficio di Staff.

Ciascuna unità Organizzativa è articolata in uffici dedicati a tematiche specifiche, di cui di seguito sono elencate le principali competenze:

- **UO Sistemi informativi, servizi e tecnologie digitali**
  - Demand management e analisi dei fabbisogni informatici delle strutture regionali;
  - Pianificazione e progettazione dell'evoluzione del Sistema Informativo Regione Veneto (SIRV);
  - Progettazione e Sviluppo di applicazioni a supporto del SIRV;
  - Gestione e manutenzione applicazioni del SIRV;
  - Attività di collaborazione con strutture regionali;
  - Monitoraggio performance dei contratti e servizi ICT erogati agli utenti;
  - Definizione di standard tecnici per la convergenza Architetturale;
  - Gestione delle Operation del Datacenter e Cloud Management;
  - Gestione sicurezza informatica.
  - Conduzione sistemi (DATA CENTER) e gestione DR.
  - Pianificazione e budget, predisposizione documenti tecnici d'appalto per affidamenti sopra e sottosoglia comunitaria.
- **UO Strategia ICT, Agenda digitale e sistemi di comunicazione**
  - Supporto al Direttore nella Definizione delle Strategie ICT e Agenda Digitale;
  - Definizione dei principali documenti strategici regionali in ambito digitale, in particolare l'Agenda Digitale del Veneto;
  - Coordinamento, attuazione e monitoraggio dell'Agenda Digitale del Veneto;
  - Raccordo istituzionale con il livello nazionale ed europeo sui temi delle politiche digitali;
  - Ideazione e coordinamento progetti sperimentali in ambito di servizi digitali per il territorio (Pubblica amministrazione, imprese, Cittadini etc);
  - Banda Ultra Larga;
  - Piattaforme abilitanti e Servizi digitali per gli enti locali;
  - Diffusione cultura digitale per cittadini, imprese e pubblica amministrazione;
  - Gestione network e sistemi di telecomunicazione (telefonia, reti radio);
  - Gestione delle PDL
  - Formazione e-learning;
  - Audit e qualità dei servizi;
  - Assistenza Utenti e asset Management.

Ufficio di Staff a supporto della Direzione per attività relative a:

- Acquisti,
- Legale,
- Contabile.

Ai fini della fornitura in esame, sono stati individuati i seguenti ruoli in coerenza con la vigente normativa degli appalti:

- **Il Responsabile Unico del Progetto (RUP)** è nominato ai sensi dell'art. 15 del D.Lgs. 36/2023 per assicurare il completamento degli interventi pubblici nei termini e con le modalità previste dal presente capitolato.
- **Il Direttore dell'Esecuzione del Contratto (DEC)** è nominato ai sensi dell'art. 114 del D.Lgs. 36/2023, per assicurare il coordinamento, la direzione e il controllo tecnico-amministrativo dell'esecuzione dei contratti, in conformità ai documenti contrattuali e alle prescrizioni normative applicabili.

L'organizzazione interna delle UO prevede, inoltre, la nomina delle figure di Assistente al DEC, mediante assegnazione di ruoli dedicati a seguire le attività/servizi contrattuali a supporto del DEC.

Il personale del Fornitore impegnato nell'erogazione dei servizi previsti dalla presente procedura aperta, oltre a relazionarsi con il personale dell'Amministrazione, deve interagire e collaborare con i team impegnati nell'erogazione di servizi aggiudicati con altre procedure di gara, quali, a titolo esemplificativo e non esaustivo:

- Team impegnati nell'erogazione dei Servizi Applicativi;
- Responsabile del Monitoraggio contratti ICT e team di monitoraggio;
- eventuali altri gruppi identificati da RV;
- eventuali enti o soggetti che utilizzano i servizi PSR.

2.2 Contesto tecnologico ed applicativo

La descrizione del contesto tecnologico (infrastrutturale) e applicativo, su cui il Fornitore aggiudicatario della procedura aperta deve operare, è riportata nell'Appendice 3 al presente Capitolato Tecnico - Contesto Tecnologico e Applicativo. Quanto descritto rappresenta lo stato del contesto alla data, che potrebbe, comunque, essere soggetto ad evoluzioni prima dell'avvio del contratto derivante alla presente procedura o comunque evoluzioni anche nel corso della vigenza contrattuale. Il Fornitore dovrà in ogni caso garantire di erogare i servizi anche al mutare degli elementi componenti il contesto stesso, secondo le direttive definite da RV.

2.2.1 Polo Strategico Regionale (PSR)

La Regione del Veneto ha avviato un significativo rinnovamento delle proprie infrastrutture ICT, con l'obiettivo di consolidare e rafforzare il Polo Strategico Regionale (PSR), in linea con la "Strategia Cloud Italia" promossa dall'Agenzia per l'Italia Digitale (AgID). Il PSR rappresenta un'infrastruttura di riferimento per la Pubblica Amministrazione Veneta, offrendo servizi Infrastructure as a Service (IaaS) e Platform as a Service (PaaS) agli Enti sanitari, strumentali e territoriali. Questo modello di gestione consente di garantire un'infrastruttura sicura, efficiente e conforme agli standard nazionali di cybersicurezza e gestione del cloud pubblico.

Al fine di fornire una più chiara rappresentazione del contesto, si specifica che ad oggi è presente un team di governo delle attività legate al PSR incaricato di supportare la Regione del Veneto nella gestione dei Servizi Cloud e delle relative infrastrutture ICT.

In particolare, a titolo esemplificativo e non esaustivo, si elencano i principali ambiti di intervento della governance:

- Gestione della migrazione degli Enti: supervisione e coordinamento delle attività di transizione dei servizi gestiti dagli Enti Strumentali, Sanitari e Territoriali verso il PSR.
- Modello di contribuzione dei costi: definizione di un modello economico sostenibile e trasparente per la ripartizione dei costi tra gli Enti aderenti.
- Governance dell'onboarding degli Enti: gestione dell'intero processo di adesione, incluse le fasi di primo contatto,

condivisione della documentazione, supporto alla formalizzazione delle convenzioni, monitoraggio delle attività amministrative e rinnovo delle adesioni.

- Definizione dei processi di gestione: sviluppo e aggiornamento dei processi operativi relativi alla supply chain, procurement e management.
- Monitoraggio dei KPI dei servizi cloud: utilizzo di strumenti avanzati per il controllo delle performance dei servizi erogati dal PSR.
- Data Center Management (DCM): definizione di processi e procedure operative per la gestione del Data Center che ospita i servizi del PSR.
- Redazione e aggiornamento dei contenuti del Portale pubblico del PSR.
- Espansione dei servizi PSR: pianificazione e gestione dell'attivazione di nuovi servizi cloud e definizione dei relativi modelli di pricing.
- Compliance con i requisiti ACN: supporto per garantire l'adeguamento dell'infrastruttura e dei servizi cloud agli standard di sicurezza previsti dall'Agenzia per la Cybersicurezza Nazionale (ACN).
- Certificazione e conformità ISO 20000-1: valutazione delle procedure e individuazione delle azioni necessarie per ottenere la certificazione di qualità dei servizi cloud.
- Interfacciamento con ACN: gestione delle richieste di adeguamento delle infrastrutture e dei servizi cloud con l'Agenzia per la Cybersicurezza Nazionale.

2.3 Aspetti di innovazione e trasformazione digitale

La strategia della trasformazione digitale della Pubblica Amministrazione (PA), quindi perseguita da RV, contenuta nel *Piano triennale per l'informatica nella PA 2024-2026*, elaborato dall'Agenzia per l'Italia Digitale (AgID), prevede che ogni amministrazione definisca le proprie politiche interne sulla base dei seguenti principi:

- **digitale e mobile come prima opzione (digital & mobile first):** le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e fruibili su dispositivi mobili, considerando alternative solo in via residuale e motivata, attraverso la "riorganizzazione strutturale e gestionale" dell'ente ed anche con una "costante semplificazione e reingegnerizzazione dei processi";
- **cloud come prima opzione (cloud first):** le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano il paradigma cloud e utilizzano esclusivamente infrastrutture digitali adeguate e servizi cloud qualificati secondo i criteri fissati da ACN;
- **servizi inclusivi, accessibili e centrati sull'utente (user-centric):** le pubbliche amministrazioni devono progettare servizi pubblici che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo;
- **dati pubblici un bene comune (open data by design e by default):** il patrimonio informativo della Pubblica Amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- **concepito per la sicurezza e la protezione dei dati personali (data protection by design e by default):** i servizi pubblici devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- **once only:** le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite, devono dare accesso ai loro fascicoli digitali e devono rendere disponibili a livello transfrontaliero i servizi pubblici rilevanti;
- **sostenibilità digitale:** le pubbliche amministrazioni devono considerare l'intero ciclo di vita dei propri servizi e la relativa sostenibilità economica, territoriale, ambientale e sociale, anche ricorrendo a forme di

aggregazione;

- **sussidiarietà, proporzionalità e appropriatezza della digitalizzazione:** i processi di digitalizzazione dell'azione amministrativa coordinati e condivisi sono portati avanti secondo i principi di sussidiarietà, proporzionalità e appropriatezza della digitalizzazione, ovvero lo Stato deve intraprendere iniziative di digitalizzazione solo se sono più efficaci di quelle a livello regionale e locale, e in base alle esigenze espresse dalle amministrazioni stesse, limitandosi negli altri casi a quanto necessario per il coordinamento informatico dei dati, e al tempo stesso le singole amministrazioni devono garantire l'appropriatezza delle iniziative di digitalizzazione portate avanti autonomamente, cioè in forma non condivisa con altri enti al livello territoriale ottimale rispetto alle esigenze preminenti dell'azione amministrativa e degli utenti dei servizi pubblici.

La strategia evolutiva in ambito ICT di RV comprende sia gli obiettivi della Direzione stessa, sia interventi strumentali ad altre Aree tematiche della Regione del Veneto, che possono intervenire in maniera non preventivabile in qualsiasi momento durante la vigenza contrattuale.

Regione del Veneto ha, inoltre, alla data di stesura del presente documento, in fase di conclusione un percorso con AGID per essere identificata come Infrastruttura PA adeguata che prevede siano soddisfatti, tra gli altri, determinati requisiti di sicurezza per poter dare il via alla relativa procedura di qualificazione ed essere inseriti tra le «infrastrutture critiche» rilevanti per la sicurezza nazionale. Il percorso strategico adottato dalla Regione Veneto punta a un'infrastruttura di datacenter ibrida, basata su un mix di soluzioni on-premise e cloud pubblico. La strategia evolutiva mira, oltre alla gestione della infrastruttura per la Giunta Regionale, a mettere a disposizione soluzioni di cloud privato (Polo Strategico Regionale - PSR) per la pubblica amministrazione e le aziende sanitarie del territorio veneto.

La DGR 1331/2023 approva lo schema di Convenzione tra la Regione del Veneto e i soggetti individuati dalle precedenti delibere (DGR 532/2018 e DGR 826/2023) per l'adesione al Polo Strategico Regionale (PSR) e l'erogazione di servizi infrastrutturali cloud adeguati. Questa delibera si inserisce nel quadro normativo delineato dalla Strategia Cloud Italia e dal regolamento AgID (Determina 628/2021) e alle determinazioni ACN (n. 306 del 18 gennaio 2022 e Regolamento ACN n. 21007/24) per l'adeguamento delle infrastrutture digitali pubbliche, garantendo elevati standard di sicurezza, scalabilità e interoperabilità.

In linea con gli obiettivi dell'Agenda Digitale del Veneto 2025, il PSR funge da hub tecnologico per la migrazione e l'orchestrazione dei dati e servizi digitali, favorendo economie di scala e una gestione centralizzata conforme ai requisiti dell'Agenzia per la Cybersicurezza Nazionale (ACN). Questo approccio strategico consente di accelerare il processo di digitalizzazione, migliorando la resilienza dei sistemi informativi e l'accessibilità dei servizi pubblici, contribuendo così al raggiungimento di una governance digitale integrata e sostenibile per il territorio regionale.

RV persegue gli obiettivi di:

- garantire l'operatività e l'efficienza delle infrastrutture, assicurando la piena operatività e l'efficienza delle infrastrutture tecnologiche, con un focus sulla sostenibilità e l'ottimizzazione dei consumi energetici;
- disponibilità e prestazioni delle applicazioni, garantendo la disponibilità e le prestazioni delle applicazioni, integrando soluzioni di monitoraggio avanzate e IA per la manutenzione predittiva;
- garantire la sicurezza e l'integrità dei dati rafforzando le misure informatiche, formando i dipendenti sulle pratiche di cybersecurity per reagire rapidamente alle minacce, e aggiornando i piani di formazione in base a nuove tecnologie e rischi emergenti, sviluppando una cultura di sicurezza condivisa;
- allineamento tecnologico, mantenendo un costante allineamento con l'evoluzione tecnologica del mercato ICT, promuovendo l'adozione di tecnologie emergenti come l'IA e l'analisi avanzata dei dati.

3. OGGETTO DELLA FORNITURA

L'oggetto della fornitura riguarda i servizi di gestione, manutenzione e supporto specialistico per le infrastrutture hardware e software di base utilizzate da RV a supporto delle proprie attività informatizzate.

Si fa riferimento al complesso dei servizi e delle attività volti a:

- garantire la piena operatività delle infrastrutture tecnologiche;

- mantenerne la perfetta efficienza;
- garantire agli utenti la disponibilità e le prestazioni delle applicazioni installate sulle infrastrutture tecnologiche e l'integrità dei relativi dati;
- fornire il supporto necessario per garantire il costante allineamento con l'evoluzione tecnologica del mercato ICT e per definirne la crescita, in coerenza con gli obiettivi strategici dell'Amministrazione.

I servizi che costituiscono l'oggetto della presente procedura aperta e nei successivi capitoli descritti nel dettaglio sono di seguito riepilogati:

Servizi conduzione operativa dei sistemi e di gestione della sicurezza

- Conduzione operativa dei sistemi
- Monitoraggio H24
- Conduzione e gestione della Sicurezza
- Conduzione e Gestione della manutenzione Hardware dell'Infrastruttura

Servizi di supporto

- Supporto Specialistico
- Sistema di monitoraggio continuo e AI
- Supporto per i percorsi di certificazione ISO
- Supporto per compliance normativa NIS2
- Supporto per compliance Legge 90/2024
- Interventi fuori orario
- Supporto qualificazione e relativi adeguamenti infrastrutture critiche rilevanti per la sicurezza nazionale

Servizi di gestione operativa

- Service Desk (SPOC)
- Servizio Gestione Postazioni di Lavoro

Servizi sicurezza

- Servizio Vulnerability Assessment dell'Infrastruttura
- Servizio di Verifica delle Vulnerabilità delle Applicazioni WEB
- Servizio di Cyber Threat Intelligence (CTI)
- SOC - Security Operation Center

Servizi di gestione licenze

4. DURATA DEL CONTRATTO

Il Contratto spiega i suoi effetti dalla **data della sottoscrizione, ovvero dalla diversa data indicata in sede di sottoscrizione del contratto tra le parti**.

Pertanto, **dalla data di sottoscrizione del contratto sarà previsto quanto segue**:

- **Periodo di subentro/presa in carico**, non retribuito, della durata di 3 mesi, dalla data di avvio indicata dall'Amministrazione regionale nel contratto e prevista a partire dal 01/03/2026 salvo diversa indicazione.
- **Erogazione delle seguenti prestazioni:**
    - **IServizi di gestione licenze, per una durata complessiva di 48 mesi, saranno erogati** dalla data di avvio indicata dall'Amministrazione regionale nel contratto e prevista a partire dal 01/03/2026 salvo diversa indicazione**;**
    - **Gli ulteriori Servizi oggetto dell'Appalto, per una durata complessiva di 45 mesi, decorrono a partire dalla conclusione del predetto periodo di subentro/presa in carico e prevista a partire dalla data del 01/06/2025, salvo diversa indicazione.**

- **Trasferimento del know-how a fine fornitura**, il Fornitore deve garantire un supporto alla transizione per almeno 3 mesi, collaborando al trasferimento delle competenze verso l'Amministrazione o un nuovo Fornitore, secondo un Piano di Trasferimento approvato. (per il dettaglio si veda il par. 9.2.6 Piano di Trasferimento). Tale attività deve concludersi entro il termine del contratto.

5. DESCRIZIONE DEI SERVIZI

5.1 Servizi conduzione operativa sistemi e sicurezza

5.1.1 Conduzione operativa dei sistemi

Il servizio di conduzione operativa riguarda tutte le attività di gestione sistemistica necessarie per prendere in carico, condurre e mantenere sempre aggiornata e funzionante una infrastruttura hardware e software di base, utilizzata per l'erogazione di uno o più servizi informatici.

I servizi di conduzione operativa sono relativi a:

- I sistemi dell'infrastruttura on-premise presso il Data Center primario di Venezia, il Data Center secondario di BC-DR (Infocamere) di Padova ed il Data Center Secondario (VSIX) di Padova;
- I sistemi residuali della vecchia infrastruttura (Server Tower e Rack, NAS e Storage periferici) installati presso le sedi minori;
- I sistemi del modello di Data Center Multi-Cloud Ibrido Regionale infrastrutture, sia On-Premise che On-Cloud.

La descrizione dell'infrastruttura on-premise e dell'infrastruttura Multi-Cloud Ibrida Regionale di RV è riportata nell'Appendice 3 Contesto Tecnologico e Applicativo.

Le attività di conduzione operativa richieste presso il Data Center dell'Amministrazione di Venezia Vega devono essere erogate con presidio on site, con una distribuzione di risorse dedicate a garanzia di attività da svolgere direttamente a supporto.

Le attività di conduzione operativa per i siti di BC-DR di Padova devono essere effettuate prevalentementein modalità remota dal Centro Servizi messo a disposizione dal Fornitore e/o dal personale di presidio del sito primario, a meno di interventi on site necessari alla risoluzione di malfunzionamenti non gestibili remotamente. Le attività componenti il servizio, indicate a titolo esemplificativo e non esaustive e descritte nei seguenti paragrafi, sono:

- Gestione sistemi;
- Manutenzione sistemi;
- Gestione Applicativi e Basi Dati;
- Gestione sicurezza logica;
- Trouble ticketing;

Nel servizio sono previsti l'emissione e il mantenimento della documentazione delle procedure operative, processi e anche relativamente alle componenti dell'infrastruttura.

Gli orari e le modalità di erogazione del servizio sono specificati al § 8.1.

La progettazione del DR rientra nel Supporto Specialistico mentre la parte di implementazione e mantenimento è compresa all'interno dei canoni e delle attività già previste per i servizi di conduzione operativa dei sistemi e sicurezza.

5.1.2 Gestione Sistemi

La gestione dei sistemi include le attività necessarie a prendere in carico, condurre e mantenere sempre aggiornata e funzionante l'infrastruttura hardware e software utilizzata per l'erogazione di uno o più servizi informatici.

In tale contesto si definisce "sistema":

- L'insieme di più componenti hardware e software assimilabili ad un'unità elaborativa autonoma, a supporto

degli ambienti di collaudo ed esercizio di una o più applicazioni;

- I sistemi integrati che combinano potenza elaborativa, storage e software di sistema e degli ambienti elaborativi gestiti secondo il paradigma del cloud computing, realizzati mediante acquisizione di risorse elaborative da un cloud provider esterno o su infrastrutture hardware e software on-premise di RV.

Gli obiettivi della gestione sistemi sono:

- Garantire la disponibilità dei sistemi e l'esecuzione delle attività schedulate in coerenza con le specifiche indicate nel calendario di erogazione dei servizi all'utenza, sia interna che esterna;
- Assicurare un continuo controllo sullo stato dei sistemi e dei collegamenti, individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie;
- Assicurare la corretta produzione e distribuzione degli output;
- Prevenire, gestire e risolvere tutti i problemi che comportano interruzione o degrado del servizio all'utenza;
- Risolvere gli incidenti informatici relativi ai sistemi rilevati e segnalati dal monitoraggio infrastrutturale, in linea con i processi e le procedure vigenti;
- Risolvere gli incidenti informatici relativi ai sistemi rilevati e segnalati dal monitoraggio della sicurezza, in linea con i processi e le procedure vigenti;
- Ottimizzare l'utilizzo dello storage in termini di razionalizzazione degli accessi e garantire la disponibilità, la salvaguardia e l'integrità dei dati;
- Garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse hardware e software;
- Controllare l'impatto sulla tecnologia esistente e garantire l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni esistenti.

La gestione dei sistemi comprende:

- Definizione, realizzazione, schedulazione ed esecuzione delle procedure di gestione dei sistemi e dei collegamenti;
- Installazioni hardware comprensive di montaggio, movimentazione, patching, etichettatura, configurazioni software, dismissione e smaltimento; inoltre, si prevedono attività afferenti all'installazione hardware per POC Sicurezza;
- Configurazione, personalizzazione ed eventuale distribuzione presso sistemi periferici in relazione ad aggiornamenti di configurazioni esistenti;
- Operazioni di routine per il funzionamento dei sistemi (accensione e spegnimento, produzione di stampe, start-up dei collegamenti, ecc.);
- Monitoraggio infrastrutturale in modalità remota mediante gli strumenti del centro servizi;
- Monitoraggio della sicurezza in modalità remota mediante gli strumenti;
- Monitoraggio puntuale da remoto delle performance end-to-end delle applicazioni e dei servizi erogati (DB, front end, ecc.) con individuazione delle eventuali cause e delle attività di risoluzione, prevedendo anche il coinvolgimento del Fornitore dei Servizi Applicativi;
- Monitoraggio specifico delle performance dei Database;
- Esecuzione degli interventi di aggiornamento del software, ad esempio applicazione di patch (comprese le patch di sicurezza) e aggiornamento dei firmware sulla base delle politiche del produttore, oppure attraverso il coordinamento degli stessi se effettuati da terzi;
- Supporto all'analisi e alla definizione delle componenti infrastrutturali necessarie al corretto funzionamento delle nuove applicazioni software, con attenzione anche agli aspetti di sicurezza;
- Supporto all'Amministrazione e a Fornitori di sviluppo applicativo per l'esecuzione delle attività di test di integrazione, di performance (carico, durata, spike e stress) e di sicurezza (statica e dinamica);

- Supporto alla definizione degli spazi di allocazione dello storage, dimensionamento e relativa attività di configurazione e gestione;
- Supporto alla verifica dell'ottimizzazione delle risorse con cadenza trimestrale (es. dismissione di vm spente, snapshot obsolete, ecc.)
- Tuning e miglioramento delle prestazioni dei sistemi;
- Capacity management delle infrastrutture informatiche volto non solo all'analisi predittiva del futuro utilizzo delle risorse, ma anche al supporto all'Amministrazione nella pianificazione delle esigenze di approvvigionamento;
- Esecuzione di test di fail-over per i sistemi configurati in "high availability" ai diversi livelli dell'infrastruttura informatica;
- Gestione dei sistemi di Access Management e Identity Management e delle attività di:
    - Rilascio e/o modifica delle credenziali di accesso, sospensione/cessazione delle stesse, profilazione e loro monitoraggio periodico, gestione delle password policy;
    - Gestione degli account privilegiati: gestione delle password e dell'audit con particolare attenzione al mantenimento di un loro inventario, alla separazione dei compiti per ogni account rispettando il principio dei privilegi minimi, nonché la tracciatura e il monitoraggio delle loro attività.
- Gestione della componente di integrazione con i sistemi di gestione dell'identità digitale (SPID);
- Gestione dei backup e restore dei dati di sistema: è responsabilità del Fornitore definire la pianificazione delle attività di backup, al fine di ottimizzare la finestra temporale a disposizione, previa approvazione, da parte dell'Amministrazione, del piano prodotto; si specifica che l'attività è estesa anche ai backup dei vari servizi cloud che RVE utilizza;
- Gestione dello Storage (inteso anche come storage presso provider di servizi cloud che RVE utilizza/utilizzerà oltre allo storage presso i propri DC), a titolo esemplificativo e non esaustivo si prevedono le seguenti attività:
    - Controllo dell'utilizzo dei dischi e delle Virtual Tape Library (VTL), per assicurare la disponibilità di spazio;
    - Gestione dello spazio sui dischi e le VTL;
    - Riorganizzazione degli archivi, per assicurarne la massima efficienza;
    - Creazione, gestione e ripristino dei cataloghi utente;
    - Classificazione dei tipi di dati e delle applicazioni che li utilizzano;
    - Ottimizzazione dell'utilizzo dello storage;
    - Definizione delle politiche di gestione VTL4;
    - Analisi conoscitiva dell'utilizzo dello storage e produzione costante di reportistica;
    - Bonifica dei dati obsoleti;
    - Configurazione degli switch per le necessità di nuovi collegamenti (zoning, ecc.) ed inizializzazione dei dischi.
- Gestione delle attività di conduzione operativa dei nodi di backup (es. Rubrik o similari) attraverso la console di prodotto;
- Gestione delle attività di conduzione operativa dei nodi iperconvergenti (es. Nutanix o similari) attraverso la console di prodotto;
- Gestione delle attività di deploy per il Continuous Deploy/Continuous Integration garantendo una contemporaneità di almeno 6 deploy di progettualità applicative e/o infrastrutturali (attività da eseguire, in ogni caso, in parallelo alle normali attività di conduzione, come ad esempio di patching, o di aggiornamento

Firewall, ecc.);

- Gestione delle attività di logging attraverso la configurazione, raccolta, correlazione, consultazione, storicizzazione nel sistema di Log collecting secondo la normativa vigente in materia;
- Gestione operativa delle piattaforme di Business Intelligence (Qlik Sense, SAS Business Intelligence, SAP Business Objects Business Intelligence) che comprende le seguenti attività:
    - Monitoraggio, manutenzione e aggiornamento delle piattaforme Qlik Sense, SAS Business Intelligence e SAP Business Objects Business Intelligence per garantire continuità operativa e prestazioni ottimali;
    - Gestione di processi ETL (Extract, Transform, Load): pianificazione, implementazione e ottimizzazione dei flussi di estrazione, trasformazione e caricamento dati, integrando diverse fonti dati aziendali per supportare il processo decisionale;
    - Amministrazione dei Datalake: configurazione, gestione e ottimizzazione di datalake per la centralizzazione e la gestione dei dati non strutturati e semi-strutturati.
- Gestione operativa di tutti i sistemi server fisici e dei sistemi virtualizzati indicati nell'Appendice 3 Contesto Tecnologico e Applicativo;
- Gestione della Porta di Dominio (PDD), mantenendo il sistema conforme alla qualificazione a suo tempo ottenuta e, a fronte delle esigenze dell'Amministrazione, supportando la stessa nella eventuale evoluzione a nuove modalità di colloquio su SPC e nella configurazione del sistema per attivare le comunicazioni con Enti esterni. A titolo informativo e non esaustivo, si riportano le principali attività incluse nella gestione della PDD:
    - Esercizio e aggiornamento della piattaforma PDD (sistemi HW e SW) in relazione alle esigenze dei servizi applicativi;
    - Manutenzione della piattaforma PDD (sistemi HW e SW);
    - Monitoraggio della operatività della PDD;
    - Gestione/conservazione del log per 24 mesi;
    - Supervisione delle funzionalità "tracciatura" e "diagnostici";
- Gestione del sistema di interoperabilità e della Dorsale di Integrazione di RV;
- Gestione del sistema VAM (Veneto API Manager), che comprende le seguenti attività:
    - Esercizio e aggiornamento della piattaforma VAM dal punto di vista infrastrutturale in relazione alle esigenze applicative;
    - Manutenzione della piattaforma VAM stessa;
    - Monitoraggio della sua operatività;
    - Gestione e conservazione dei log.
- Distribuzione remota di ogni tipologia di software di sistema o applicativo sulle postazioni utente sia Desktop che notebook con verifica dello stato di aggiornamento delle PdL gestite, attivando gli interventi eventualmente necessari per la corretta operatività e minimizzando l'impatto sull'erogazione dei normali servizi informatici e sull'operatività degli utenti;
- Gestione e manutenzione della piattaforma di Virtual Desktop Infrastructure (VDI) attualmente erogata mediante infrastruttura Citrix o mediante prodotto offerto per il medesimo scopo dal Fornitore. Si specifica che si intende anche l'aggiornamento dell'ambiente VDI coerentemente con l'aggiornamento del Sistema operativo e applicativi delle PDL;
- Gestione del sistema di IT Asset Management e ITSM in termini di configurazione, raccolta, correlazione, consultazione, storicizzazione dei dati nel sistema del CMDB e definizione e integrazione di processi automatizzati di ITSM mediante gli strumenti indicati al § 5.5.4. Il Fornitore deve svolgere le attività:

- Di identificazione e classificazione degli elementi di configurazione relativi all'hardware e software di base, controllandone lo stato, le modifiche, il livello di aggiornamento, le interdipendenze, gestendo le condizioni di utilizzo, garantendone la rintracciabilità e l'adeguatezza, attraverso le procedure definite nell'ambito del processo di IT Asset & Configuration Management;
- Aggiornamento costante e comprensivo della riconciliazione (manuale o automatica) del sistema di asset management, con le informazioni inerenti ai sistemi oggetto del servizio;
- Con particolare focus sul CMDB, il Fornitore è obbligato a fornire strumenti utili a RVE per il monitoraggio del CMDB, definendone insieme a RV le specifiche tecniche qualora queste non siano ancora state stabilite, oppure adottando quelle già esistenti, nel caso in cui siano state precedentemente definite;
- Si prevede infine la possibilità da parte di RVE di effettuare degli audit volti alla verifica che il CMDB sia correttamente gestito; cadenza e modalità verranno comunicate a seguito dell'avvio del servizio. A titolo esemplificativo e non esaustivo, si prevede che suddetti audit avranno l'obiettivo di:
  - Verificare la conformità a specifiche policy aziendali o normative;
  - Garantire la qualità dei dati contenuti nel CMDB;
  - Assicurare l'aggiornamento continuo delle informazioni;
  - Individuare eventuali anomalie e/o inefficienze e le relative azioni correttive.

- Costante collaborazione con il Fornitore o dei Fornitori dei Servizi Applicativi al fine di identificare cause di eventuali deterioramenti delle performance dei servizi;
- Presidio del data center: dovrà essere prevista almeno una risorsa per il presidio dei DC (Primario (LYBRA), Secondario (VSIX), Secondario (Infocamere)), reperibile anche fuori dall'orario di lavoro, dedicata ad attività, a titolo esemplificativo e non esaustivo, di:
  - Imputazione dei dati all'interno del Software EcoStruxure Data Center Expert di Schneider;
  - Accoglienza visitatori;
  - Gestione Timesheet;
  - Presentazione procedure;
  - Gestione logistica materiale;
  - Gestione magazzino;
  - Verifica che i lavori siano svolti in conformità delle procedure di sicurezza;
  - Attività connesse.

  Si sottolinea che per figura assegnata non si intende una persona esclusivamente assegnata a suddette attività; in ottica di efficientamento, le risorse dedicate alla gestione dell'infrastruttura hardware dovranno alternarsi in modo tale da assicurare che il presidio sia costantemente garantito.

  Si prevede quindi che tali risorse vantino una conoscenza approfondita dell'infrastruttura a loro assegnata, tale da garantire adeguato supporto in caso di richiesta di informazioni o espletamento di interventi, come anticipato, anche in caso di attività fuori dall'orario lavorativo; infine, si prevede che, durante l'orario di reperibilità, in caso di necessità, la persona incaricata dovrà raggiungere fisicamente i data center indicati entro un massimo di un'ora dalla chiamata. Qualora la residenza dell'incaricato si trovi a una distanza superiore a 50 km dai data center, è prevista una tolleranza di 15 minuti.

Per quanto concerne la Business Continuity, il sito primario ed i due secondari hanno un collegamento ad alta velocità e bassa latenza in layer 2 con utilizzo del DNS Global Load Balancer di Oplon Networks per il bilanciamento. Per

garantire la Business Continuity, il Fornitore deve tenere in considerazione le configurazioni allo stato dell'arte ad ogni change dei sistemi, inoltre devono essere previsti i test di fail-over da eseguire con periodicità predefinita e redigere le procedure operative identificando adeguatamente e dettagliatamente le operazioni eseguite automaticamente dai sistemi e le operazioni che invece richiedono un intervento di "switch" manuale.

Il Disaster Recovery è situato presso il Data Center di Padova e garantisce la continuità operativa di alcuni servizi, a fronte di guasti particolarmente significativi che ne impediscono la fruizione dal sito primario per periodi non brevi. Pertanto, il Fornitore deve provvedere al ripristino dei servizi richiesti, utilizzando le medesime procedure di DR nel rispetto degli stessi requisiti di DR (RTO e RPO).

L'intera architettura e le procedure di ripristino devono essere progettate al fine di rispettare i livelli di servizio definiti da RV, espressi in termini di Recovery Time Objective (RTO) e Recovery Point Objective (RPO) e previsti nel piano di DR.

La gestione dei sistemi deve comprendere, pertanto, anche le attività di gestione della soluzione di DR, sia in condizioni ordinarie che di emergenza.

In particolare, al Fornitore è richiesto di:

- Definire un piano di DR per la gestione dell'emergenza (o comunque acquisire, aggiornare o implementare l'eventuale piano già definito e in essere per RVE), i cui contenuti devono essere definiti con RV in fase di avvio della fornitura. Il piano di DR deve essere sottoposto ad approvazione di RV prima di renderlo operativo;
- Adeguare il sito di DR allineandolo alle evoluzioni del sito primario (eventuali investimenti in infrastruttura saranno a carico di RV);
- Provvedere alla replica dei dati di produzione nel rispetto dei requisiti di RPO specificati;
- Mantenere allineato l'ambiente di recovery con quello di produzione;
- Provvedere alla gestione e all'aggiornamento delle procedure, degli script e/o dei meccanismi automatici di schedulazione/orchestrazione di task di ripartenza dei servizi sul sito DR;
- Verifica periodica dell'efficienza delle procedure di gestione delle emergenze;
- Gestire l'esecuzione dei test periodici di DR, in modalità continuativa, effettuandoli in modalità isolata e sicura per i servizi del sito primario;
- Provvedere in caso di dichiarazione dello stato di emergenza (disastro) da parte di RV, se necessario, all'allocazione di risorse da impegnare on site sul sito di DR per le attività di ripristino di quanto necessario alla ripartenza delle applicazioni, nel rispetto in particolare del requisito di RTO specificato;
- Eseguire, nei tempi concordati, il piano di rientro dal sito di DR.

5.1.2.1 Gestione Certificati digitali

I certificati digitali sono strumenti essenziali per garantire la sicurezza e l'autenticità delle comunicazioni e delle transazioni online, soprattutto nella Pubblica Amministrazione, in quanto permettono di verificare l'identità di un soggetto (persona fisica, ente, server) e di proteggere le informazioni scambiate. Inoltre, è obbligatorio comunicare agli enti pubblici competenti (ad es. l'Agenzia delle Entrate, Sogei e altri enti istituzionali) l'emissione di nuovi certificati o il rinnovo di quelli esistenti, per garantire la continuità operativa e la conformità ai requisiti normativi.

In Regione del Veneto sono attivi due scenari distinti per la gestione dei certificati digitali:

1. *Gestione dei certificati dalla Regione del Veneto verso Enti Esterni*
2. *Gestione dei certificati dagli Enti Esterni verso la Regione del Veneto*

Il fornitore dovrà costituire il Centro Competenza Certificati (abbr. CCC) di Regione Veneto. Di seguito si riportano le principali attività in carico al CCC nell'ambito dei due processi.

Gestione dei Certificati da Regione a Ente Esterno

Fase di Verifica dell'Esigenza e Richiesta nuovo certificato o Rinnovo*:*

- Il CCC deve monitorare le scadenze dei certificati attraverso uno strumento di controllo (si veda par. 6.1.2.2 - Piattaforma di Service Management)
- Nel caso di scadenza prossima di un certificato o nel caso di richieste di nuova emissione inviate dai PM RV Applicativi Il CCC provvede a richiedere il rinnovo all'Ente competente responsabile dell'Autorità di Certificazione.
- Il CCC ingaggia il team Operation che genera, se necessaria, la Certificate Signing Request (CSR)i, e provvede all'invio della richiesta di nuovo certificato.

Fase Gestione Fornitura e Distribuzione Certificato:

- Il CCC richiede ai referenti di Regione Veneto di inviare la richiesta (acquisto) all'Ente esterno che ha l'Autorità di Certificazione il CSR. Una volta ricevuto il certificato da quest'ultimo, il CCC apre un ticket in SysAid (tipo Change) per richiedere al Team Operation la presa in carico delle attività previste nella fase successiva (fase Gestione Change);
- Il CCC è inoltre responsabile della registrazione del certificato nell'inventario predisposto e della gestione dello scadenziario dei certificati in uso.

Fase Gestione Change:

- Il CCC effettua il backup del vecchio certificato e installa il nuovo certificato su server o client, aggiornando se necessario i dati sull'inventario per la gestione degli stessi.
- Il CCC deve coinvolgere e gestire i soggetti esterni intesi come utilizzatori del servizio del quale si sta cambiando il certificato.
- Il CCC deve verificare che l'installazione sia andata a buon fine (ad es. verificando lo stato del servizio o del dominio web) effettuando i test opportuni attraverso uno strumento di monitoraggio (si veda par.6.1.2.2 - Piattaforma di Service Management) e infine dovrà notificare l'esito dell'installazione attraverso la chiusura del ticket in SysAid e inviando una mail al Centro di competenza Certificati.

Fase Chiusura:

- Il Centro Competenza Certificati a seguito della verifica dello stato del Certificato comunica il buon esito del processo ai soggetti interessati PM RV applicativo e Fornitore, e infine invia la comunicazione via PEC all'Ente esterno.

Gestione dei Certificati Digitali da Ente Esterno a Regione del Veneto

Il processo di gestione dei certificati digitali tra un Ente Esterno e la Regione del Veneto si articola in 3 fasi principali, e le attività previste da parte del Fornitore rientrano nelle seguenti fasi:

Fase Sottoscrizione o aggiornamento dell'accordo/convenzione e ricezione del certificato digitale:

- L'Ente Esterno e la Regione del Veneto stipulano o aggiornano l'accordo/convenzione per la gestione dei certificati. Nella convenzione redatta dall'amministrazione verrà inserito quale referente tecnico un soggetto del CCC. Successivamente l'Ente Esterno invia il certificato digitale alla Segreteria ICT di RV che lo inoltra con il sistema di protocollo al gruppo regionale di sicurezza, il quale redireziona con mail al Centro Competenza Certificati. In questa fase non è richiesta alcuna attività in carico al Fornitore, tuttavia dovrà disporre un casella PEC dedicata.

Fase Distribuzione del certificato e Gestione del Change:

- Il CCC deve validare (es. verificare che il certificato sia valido e non corrotto) e comunicare ai soggetti interessati (PM applicativi,) e ingaggia il team operation per la change.
- Il Team Operation esegue il backup del vecchio certificato e installa il nuovo certificato sui sistemi della Regione del Veneto, e dopo l'installazione, effettua una verifica dello stato dei servizi per garantire che il certificato funzioni correttamente.
- Il Team Operation deve verificare che l'installazione sia andata a buon fine (ad es. verificando lo stato del servizio o del dominio web) e dovrà notificare l'esito dell'installazione inviando una mail al Centro di competenza Certificati.
- Il CCC effettua i test opportuni attraverso uno strumento di monitoraggio (si veda par. 6.1.2.2 - Piattaforma di Service Management) e comunica al team operation per confermare la chiusura della change. è inoltre responsabile della registrazione del certificato nell'inventario e della gestione dello scadenziario dei certificati in uso.
- Nel caso di chiarimenti con l'ente esterno e in particolare in casi di installazione congiunta il CCC deve prendere i contatti con i tecnici dell'ente esterno.

Fase Chiusura del processo

- Il Centro Competenza Certificati invia una comunicazione di esito ai soggetti interessati, confermando l'avvenuta installazione del certificato.

In fase di avvio del contratto RV definirà in dettaglio le attività del processo di gestione dei certificati digitali.

Si specifica che l'attività sopra descritte al par. 5.1.2.1 sono all'interno dei canoni e delle attività già previste per i servizi di conduzione operativa dei sistemi e sicurezza**.**

5.1.3 Manutenzione Sistemi

La manutenzione dei sistemi comprende le attività necessarie per mantenere continuamente allineati i sistemi alle più recenti innovazioni tecnologiche rilasciate dai vendor e necessarie per la corretta erogazione del servizio, nonché tutte le attività necessarie per ripristinare il funzionamento dei sistemi a fronte di errori.

Per le componenti hardware in garanzia, si prevede che le stesse siano spedite dal Fornitore al vendor (senza oneri aggiuntivi per RV) che ne seguirà il processo di sostituzione o riparazione; per i componenti non in garanzia, la manutenzione dei sistemi/componenti difettosi rientra nel servizio accessorio di manutenzione HW dell'infrastruttura.

Le attività di manutenzione dei sistemi possono essere di due tipi:

- **Manutenzione Preventiva**: attività di manutenzione atta a prevenire l'occorrenza di errori, malfunzioni e guasti;

- **Manutenzione Correttiva**: attività di manutenzione a seguito di malfunzionamenti o guasti.

Manutenzione Preventiva

L'attività è finalizzata a prevenire malfunzionamenti e/o degrado dei servizi nonché a ottimizzare il funzionamento dell'Infrastruttura ICT. Pertanto, il Fornitore ha la responsabilità di eseguire tutte le attività volte a individuare eventuali vulnerabilità, ad analizzare le performance dei sistemi e dei servizi erogati dall'Infrastruttura ICT attraverso la strumentazione in uso, a segnalare la necessità di implementare ulteriori politiche di backup e/o di monitoraggio, ad analizzare in modo continuativo i Log di sistema e di prodotto, a testare i meccanismi di affidabilità dei servizi erogati dall'Infrastruttura ICT.

Il Fornitore deve predisporre:

- Il Piano di Manutenzione Preventiva (ex-ante) di ogni componente dell'Infrastruttura ICT, da rendere disponibile a RV entro 20 giorni lavorativi dalla presa in carico della stessa e successivamente aggiornarlo su base semestrale e consegnato o messo a disposizione di RV;
- La Relazione di Manutenzione Preventiva (ex-post) e consegnarlo a RV entro 5 giorni lavorativi dal termine del trimestre di riferimento. A titolo esemplificativo e non esaustivo, nell'ambito delle attività, il Fornitore deve monitorare costantemente, in maniera continuativa e dare evidenza nella relazione trimestrale di:
    - Rilascio di aggiornamenti, di nuove versioni, service pack o correzioni (sistema operativo, SW di base, Middleware, software applicativo gestito e, ove applicabile, firmware) rilasciate dai produttori;
    - Compatibilità e impatto tecnologico degli aggiornamenti, delle nuove versioni o delle correzioni con l'ambiente di target;
    - Licenze software e certificati (server e applicativi) di proprietà dell'Amministrazione inserendo nei rapporti trimestrali le licenze e/o i certificati che entro il semestre successivo saranno in scadenza. Le stesse informazioni devono essere fornite anche su richiesta puntuale dell'Amministrazione;
    - Attività finalizzate ad elevare il grado di affidabilità dell'intera infrastruttura gestita, al miglioramento del funzionamento e all'aumento della sicurezza;
    - Previsioni di end of support (EoS) e di end of life (EoL) rilasciate dai produttori per i prodotti installati sull'infrastruttura, inserendo nella relazione trimestrale i prodotti software corredati dalle date di EoS ed EoL. Le stesse informazioni devono essere fornite anche su richiesta puntuale dell'Amministrazione;
    - Attività per minimizzare i tempi di fermo manutentivo, durante le operazioni programmate di aggiornamento tecnologico, adottando pianificazioni almeno semestrali.

I dati e le informazioni inserite nella Relazione di manutenzione preventiva (ex-post) devono essere resi disponibili all'Amministrazione in modalità "Live" per ogni trimestre di riferimento, ai fini della verifica e controllo puntuale dello stato delle attività di rilascio di aggiornamenti, delle scadenze delle licenze e/o dei certificati, delle previsioni di EoS e di EoL rilasciate dai produttori in scadenza, e in generale di tutte le attività che saranno di volta in volta inserite nel Piano di manutenzione preventiva semestrale. I dati e le informazioni devono essere resi fruibili attraverso la piattaforma di reportistica e SLA management del Fornitore per l'esecuzione delle attività di gestione dei sistemi.

Manutenzione Correttiva

L'attività è finalizzata a risolvere malfunzionamenti e/o degrado dei servizi e a ripristinare la corretta fruizione dei servizi. È responsabilità del Fornitore ripristinare il servizio nel minor tempo possibile e comunque nel tempo massimo definito, individuare le cause sottese al disservizio e proporne la soluzione definitiva, sfruttando tutte le competenze necessarie, anche laddove il disservizio riguardi tecnologie altamente specializzate o poco diffuse sul mercato (tecnologie "di nicchia").

Le attività da erogare, indicate a titolo esemplificativo e non esaustivo, sono:

- Gestire le richieste di intervento in modo efficace, per tutto l'iter operativo, fino alla soluzione del problema;
- Ridurre i tempi di fermo delle apparecchiature e dei sistemi, a fronte di malfunzionamenti o errori, entro i

termini stabiliti dagli SLA;

- Gestire il rapporto con fornitori terzi in caso di malfunzionamenti relativi a prodotti software per cui sia attiva una subscription o licenza che include la manutenzione, fino alla completa risoluzione;
- Effettuare la segnalazione a RV, in caso di malfunzionamento del software applicativo ad hoc e dare supporto per la parte di propria competenza al Fornitore terzo che ha in carico lo specifico SW nell'analisi e nella risoluzione del malfunzionamento;
- Gestire tramite l'aggiornamento e revisione del registro delle non conformità.

5.1.4 Gestione Applicativi e Basi Dati

La gestione applicativi e basi-dati comprende l'insieme di attività per la presa in carico e gestione di applicativi e delle relative basi dati.

In questo contesto viene definita "applicazione" una qualsiasi realizzazione software (ad-hoc, prodotto di mercato, in riuso da altre amministrazioni) tesa a fornire un insieme di funzionalità all'Amministrazione.

Per un dettaglio sulle applicazioni e le diverse tipologie di database incluse nel servizio si rimanda all'Appendice 3 Contesto tecnologico e applicativo.

Le attività richieste, a titolo esemplificativo e non esaustivo prevedono di:

- Prendere in carico l'applicativo e la relativa base-dati, curandone la loro corretta installazione in collaudo ed esercizio e l'ottimizzazione del workload, mediante:
    - Analisi preliminare dell'applicativo e della base dati;
    - Analisi delle Specifiche architetturali dell'applicativo e della base dati;
    - Preparazione degli ambienti di installazione (Staging, Collaudo, Produzione);
    - Installazione dell'applicativo e creazione/update della base dati;
    - Configurazione e ottimizzazione del workload;
    - Monitoraggio continuo delle prestazioni e gestione del workload.
- Gestire l'applicazione e le relative base-dati dal punto di vista operativo mediante:
    - Messa in esercizio dell'applicazione;
    - Dismissione dell'applicazione e delle base dati (dovranno seguire le linee guida AGID Conservazione delle basi dati, Aprile 2023 o successive);
    - Abilitazione degli utenti all'applicazione;
    - Riorganizzazioni e parametrizzazioni della base dati secondo le indicazioni fornite dal supporto del fornitore applicativo;
    - Analisi di occupazione spazio delle basi dati e interventi di tuning e di ottimizzazione delle performance;
    - Supporto al team applicativo per la definizione e ottimizzazione delle basi dati.
- Definizione e implementazione delle procedure relative alle repliche dei dati come indicate nel piano di DR;
- Supportare lo sviluppo applicativo per:
    - Disegno e modifica delle basi dati ai fini di un ottimale utilizzo;
    - Disegno e preparazione delle procedure da utilizzare in esercizio, ottimizzazione del workload;
    - Change e release management delle applicazioni;
    - Problem determination relativa a malfunzionamenti complessi o di interfaccia con il SW di base,

nonché con le connessioni di rete;

- Back-up/restore dei dati come indicato nel piano di DR;
- Raccolta degli indicatori dell'applicazione e relativa reportistica (la tipologia dei report sarà condivisa ad avvio fornitura);
- Raccolta e gestione delle segnalazioni di anomalia;
- Supporto dal punto di vista sistemistico degli aspetti tecnologici relativi allo sviluppo applicativo;
- Supporto dal punto di vista sistemistico degli aspetti tecnologici relativi alla privacy (pseudonimizzazione, cifratura e separazione dei dati personali da quelli comuni).

- Amministrare gli application server su cui le applicazioni sono installate (per la descrizione si rimanda all'Appendice 3 Contesto tecnologico e applicativo);
- Amministrare i DB server su cui i database sono installati (per la descrizione si rimanda all'Appendice 3 Contesto tecnologico e applicativo): si prevede che il Fornitore effettui l'amministrazione, ottimizzazione ed installazione dei database ospitati dai sistemi gestiti. A titolo esemplificativo ma non esaustivo si prevedono le seguenti attività:
  - Installazione e configurazione del database;
  - DB Administration (creazione tabelle, caricamento dati, ripristino degli indici, ottimizzazione dei DB, ecc.);
  - Aggiornamento dati statistici del catalogo del database;
  - Soluzione delle anomalie;
  - Installazione delle fix correttive e di sicurezza;
  - Installazione nuovi release;
  - Reporting periodico per evidenziare le frammentazioni dei database;
  - Analisi delle prestazioni delle singole sessioni applicative ed individuazione di possibili ottimizzazioni del codice;
- L'esecuzione di procedure di batch:
  - Batch applicativo, schedulato a seguito di richiesta effettuata dalle varie aree applicative;
  - Batch tecnico, che riguarda essenzialmente il salvataggio dei dati e la memorizzazione dei dati di sistema, utilizzati per la produzione di report statistici mensili;

  Il Fornitore ha la responsabilità del buon esito del batch tecnico per tutti i prodotti installati, compresi quelli di automazione. Inoltre, il Fornitore ha la responsabilità, a fronte di errori di esecuzione del batch applicativo, di fornire tempestivo supporto per verificare eventuali cause riconducibili all'infrastruttura.
- Gestire l'evoluzione dell'applicazione e della base-dati mediante:
  - Installazione di nuove versioni o aggiornamenti;
  - Tracciamento delle segnalazioni di anomalia con i relativi aggiornamenti/nuove versioni installate;

5.1.4.1 Adozione delle metodologie DevSecOps

L'attività di gestione applicativi e basi dati prevede l'adozione delle metodologie DevSecOps, ovvero l'insieme di pratiche che combinano lo sviluppo del software (Dev), la sicurezza (Sec) e le operazioni IT (Ops).

L'applicazione del DevSecOps prevede una stretta integrazione tra i gruppi di sviluppo, operation e i DevSecOps Engineer, e il team security con l'obiettivo di creare un flusso di lavoro ottimale per la gestione delle applicazioni. Si dà

priorità a strumenti e pratiche che automatizzano le attività più ripetitive, migliorano la qualità del codice e garantiscono rilasci stabili e tempestivi.

Tali attività comprendono:

- Il supporto tecnico ai gruppi di sviluppo per la gestione e manutenzione degli automatismi di rilascio degli applicativi;
- Supporto e analisi nelle fasi iniziali di condivisione della soluzione tecnica da rilasciare e migrazione delle applicazioni già esistenti nel parco applicativo di Regione del Veneto.

Tra le attività previste, spicca il supporto tecnico continuo per la gestione degli automatismi di rilascio. I DevOps Engineer collaborano con i gruppi di sviluppo per configurare e mantenere pipeline CI/CD (Continuous Integration/Continuous Deployment), utilizzando strumenti fondamentali come Bitbucket per il versionamento del codice, Bamboo per l'automazione dei processi e Nexus come repository degli artefatti.

Le pipeline di Continuous Integration devono prevedere un task di integrazione con SonarQube per l'analisi statica del codice sorgente per tutti i linguaggi supportati dal tool stesso.

Nelle fasi iniziali di ogni progetto, è previsto un momento di condivisione tecnica: i vari team si incontrano per discutere la soluzione proposta, identificare eventuali criticità e concordare tempistiche e milestone. Questo approccio collaborativo facilita la migrazione delle applicazioni esistenti verso architetture più moderne, come quelle containerizzate, mantenendo alta la compatibilità e la stabilità dei servizi.

Un altro aspetto importante è l'adozione di tecnologie di containerizzazione e orchestrazione. Grazie a Kubernetes, le applicazioni vengono erogate in ambienti containerizzati, migliorando la portabilità e la scalabilità. Strumenti come Kustomize e Argo CD vengono utilizzati per configurare e automatizzare i processi di deployment, garantendo un approccio modulare e facilmente adattabile alle diverse esigenze.

Per favorire l'adozione del DevSecOps all'interno dell'organizzazione, si organizzano regolarmente sessioni di formazione congiunta tra team di sviluppo e operation. In questi incontri si affrontano progressi, sfide e soluzioni, con un focus sulla promozione di una comunicazione aperta e trasparente. Inoltre, viene incentivato un continuo scambio di feedback per individuare e implementare miglioramenti. Si richiede al Fornitore di attenersi ai processi e alle responsabilità di seguito descritte.

Si rimanda all'Appendice 3 Contesto tecnologico e Applicativo per maggiori dettagli.

Per il dettaglio sulle figure professionali individuate, nello specifico i ruoli di DevOps Engineer incluse nel servizio, si rimanda all'Appendice 2 Profili Professionali.

Il processo di DevSecOps mira a integrare la sicurezza direttamente nel ciclo di sviluppo e distribuzione, garantendo la qualità del codice e riducendo vulnerabilità e difetti e a garantire una pipeline sicura e stabile, con un coinvolgimento attivo dei vari team per una gestione efficace della qualità del codice e della sicurezza. SonarQube viene utilizzato nella pipeline come strumento per l'analisi statica del codice, con responsabilità ben definite tra i vari team coinvolti, che di seguito viene descritta.

Team e Responsabilità

Team di Sviluppo (fuori dall'ambito di questo contratto) avrà la responsabilità di:

- Scrittura del codice e dell'integrazione delle best practice;
- Collaborare con gli altri team per risolvere vulnerabilità e difetti segnalati da SonarQube;
- Apportare le modifiche necessarie per soddisfare i Quality Gate (QG).

Team di Qualità e Sicurezza avrà la responsabilità di:

- Definizione dei Quality Gate, includendo metriche quali code coverage, maintainability e vulnerabilità;
- Revisione delle procedure e delle policy di sicurezza;
- Analisi delle vulnerabilità e dei bug ricorrenti, fornendo linee guida per la mitigazione;
- Utilizzo delle API di SonarQube per generare report di vulnerabilità.

Team Infrastrutturale e Sistemistico avrà la responsabilità di:

- Configurazione e manutenzione dell'infrastruttura necessaria per SonarQube, inclusi l'ambiente containerizzato e l'integrazione con Bamboo;
- Garantire l'accesso federato ai team di sviluppo;
- Monitoraggio continuo del sistema.

Nella seguente tabella vengono dettagliate le fasi progettuali previste e le attività di cui i team sono responsabili:

Fase	Dev	Ops	Sec
Fase 1: Documentazione a Supporto dell'Integrazione	Redazione della documentazione per l'utilizzo di SonarQube in relazione alla configurazione delle pipeline.	Documentazione relativa alla gestione della piattaforma SonarQube, come il monitoraggio e la manutenzione.	Indicazioni sulle policy di sicurezza da seguire e i requisiti di conformità.
Fase 2: Progetto Pilota	Supporto nell'integrazione iniziale con progetti selezionati e ottimizzazione del processo operativo di scansione.	Configurazione delle API di SonarQube per generare report automatizzati.	Validazione dei report di vulnerabilità generati tramite API, con analisi dei rischi.
Fase 3: Supporto per l'Integrazione dei Progetti	Collaborazione nell'adattare i progetti rimanenti per l'integrazione con SonarQube.	Pianificazione e coordinamento operativo per l'integrazione di SonarQube nei progetti rimanenti.	Supervisione della conformità di tutti i progetti alle regole di sicurezza definite.
Fase 4: Raccolta e Analisi di Errori e Vulnerabilità	Identificazione e classificazione degli errori relativi al codice sorgente.	Raccolta centralizzata dei dati di scansione per facilitare l'analisi.	Classificazione delle vulnerabilità più ricorrenti e aggiornamento delle regole di sicurezza.
Fase 5: Redazione del Report Generale	Contributo all'analisi dei bug organizzati per progetto.	Preparazione e consolidamento dei report con i dati raccolti.	Revisione dei Quality Gate definitivi e raccomandazioni per le azioni correttive.
Fase 6: Abilitazione dei Quality Gate Bloccanti	Aggiornamento del codice per soddisfare i Quality Gate bloccanti.	Configurazione dei blocchi nelle pipeline per applicare i Quality Gate.	Definizione e validazione delle regole bloccanti.
Fase 7: Monitoraggio Continuo	Monitoraggio della qualità del codice nei nuovi sviluppi.	Monitoraggio continuo delle pipeline e dei sistemi.	Verifica iterativa delle vulnerabilità per garantire il mantenimento della sicurezza.

Tabella 2 - Fasi progettuali previste

Al momento della stesura del presente documento, RVE è nella fase di avvio del progetto pilota. Tuttavia, non è al momento definito se l'avvio dei servizi ambito del presente Capitolato avverrà a progetto pilota terminato o in corso, oppure se verranno avviati altri progetti pilota.

5.1.5 Trouble Ticketing

Il servizio che si caratterizza come supporto di 2° livello infrastrutturale e riguarda la gestione e risoluzione di problematiche più complesse che non possono essere risolte dall'assistenza di primo livello, svolge le seguenti attività, a titolo esemplificativo:

- Ricezione e classificazione dei ticket:
  - Analisi dei ticket inoltrati dal primo livello per identificare la priorità e la gravità dell'incidente in base agli SLA (Service Level Agreement);
  - Aggiornamento dei ticket con ulteriori dettagli raccolti durante l'analisi preliminare;
  - Eventuale aggiornamento della priorità/impatto/criticità;
  - Eventuale riclassificazione degli incidenti o richieste;
  - Eventuale assegnazione a fornitori esterni, eventualmente responsabili di specifiche attività.
- Diagnosi tecnica approfondita:
  - Diagnosi e risoluzione delle segnalazioni/richieste dal primo livello, anche attraverso l'utilizzo delle informazioni presenti nella Knowledge base;
  - Consultazione dei log e dei report di monitoraggio;
  - Escalation a un livello successivo o a specialisti se necessario (ad esempio, al team di sviluppo o al Fornitore del sistema).
- Stesura e aggiornamento documentazione tramite:
  - Registrazione dettagliata della soluzione adottata nel sistema di ticketing per arricchire il knowledge base interno e/o consentire al primo livello di risolvere casi simili in autonomia in futuro.
- Proattività e miglioramento continuo:
  - Identificazione di trend ricorrenti nei problemi gestiti e collaborazione con altri team;
  - Proporre miglioramenti infrastrutturali;
  - Prevenire il ripetersi di problematiche analoghe.
- Reporting:
  - Produzione, condivisione e discussione con RV di report sull'andamento del servizio e sull'esecuzione di dettaglio delle attività sopra descritte e sui risultati da esse portati.

5.1.6 Ottimizzazione dell'infrastruttura

Regione del Veneto è impegnata a perseguire principi di sostenibilità ambientale e risparmio energetico e per questo aspetto ritiene che il governo efficiente e l'ottimizzazione dell'infrastruttura IT debba essere un elemento fondamentale del servizio richiesto con la procedura.

Come indicato brevemente nei paragrafi precedenti, il Fornitore dovrà quindi prevedere una conduzione operativa dei sistemi volta anche all'ottimizzazione dell'infrastruttura esistente.

In particolare, il Fornitore entro il primo anno di contratto dovrà dettagliare, sulla base di quanto proposto in sede di offerta tecnica, la pianificazione delle attività necessarie per la realizzazione di un progetto volto all'ottimizzazione dell'infrastruttura di RV.

Tale progetto, a seguito di approvazione da parte di RV, dovrà poi essere implementato nei 3 anni successivi di contratto.

Si precisa, inoltre, che la pianificazione è inclusa negli adempimenti del contratto e tale attività non dovrà avere alcun

onere aggiuntivo per RVE e non dovranno essere svolte dai Team di presidio (Team servizio di conduzione operativa dei sistemi e sicurezza, Team servizio PdL), mentre l'implementazione del progetto con l'obiettivo di ottimizzazione dell'infrastruttura rientrerà all'interno dei canoni e delle attività per i servizi di conduzione operativa dei sistemi e sicurezza.

5.1.7 Gestione Sicurezza Logica

Attraverso il servizio di gestione della sicurezza logica, il Fornitore adotta, implementa e gestisce tutte le contromisure di tipo tecnologico, volte alla difesa perimetrale e di contenuto del sistema informativo, in accordo con quanto stabilito da RV.

Tale servizio ha lo scopo di:

- Attuare la politica per la sicurezza dei flussi di rete in termini di tipo e/o contenuto del traffico;
- Monitorare e verificare l'efficacia delle misure di sicurezza adottate per i flussi di rete;
- Valutare e gestire il rischio associato alle minacce di tipo informatico;
- Utilizzare strumenti tecnologici e competenze per affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza.

Al Fornitore è richiesto di erogare le seguenti attività:

- Gestione dei dispositivi di sicurezza: l'attività consente di attuare la politica per la sicurezza sui dispositivi di difesa perimetrale di Regione del Veneto quali Firewall tradizionali e Next Generation Firewall (NGF) Fortinet, dei Web Application Firewall (WAF), delle VPN site-to-site e client-to-site, Bilanciatori (Application Delivery Controller ADC - Oplon), Proxy applicativi e di navigazione, sonde NDR, sistemi AntiDDos, garantendo e assicurando:
    - Interventi periodici programmati per il buon funzionamento dei sistemi e interventi volti al ripristino delle funzionalità dei dispositivi;
    - Interventi necessari a risolvere eventuali vulnerabilità o zero-day segnalati da CSIRT/ACN, che comportano analisi ed eventuale aggiornamento, o dai produttori stessi nel minor tempo possibile e non oltre i tempi previsti dalle normative di settore;
    - Installazione, configurazione e parametrizzazione dei dispositivi;
    - Interventi di ripristino in caso di malfunzionamenti HW per gli appliance fisici e di ripristino SW, sia per quelli fisici che per quelli virtuali;
    - Coordinamento e interfacciamento con la/le terze parti che ha/hanno in carico la gestione della rete;
    - Generazione di report standard e personalizzati prodotti dai software in uso RV corredati di statistiche e grafici ed esportabili in formato Excel o PDF, eventuali dettagli saranno concordati con RV;
    - Manutenzione delle componenti impegnate nell'erogazione del servizio, quali ad esempio aggiornamenti software, hotfix, operazioni di riavvio di specifici processi applicativi.
- Gestione del ciclo di vita delle utenze 'nominali' e 'applicative' configurate sui sistemi informatici; implementando un processo di verifica periodica (ogni 3 mesi) delle utenze attive, identificando anche gli account "dormienti", tramite l'analisi periodica dei log di accesso per individuare utenze non utilizzate da un determinato intervallo di tempo e/o individuando utenze inattive non ancora disattivate. Dovrà essere prodotto un report;

- Gestione degli apparati IDS (Intrusion Detection System) e IPS (Intrusion Prevention System): l'attività consiste nel gestire la configurazione degli apparati dell'Amministrazione ed eseguire gli aggiornamenti necessari (firme d'attacco, security patching update, ecc.);
- Content filtering: gestione delle configurazioni al fine di controllare l'ammissibilità dei contenuti in transito rispetto alle politiche di sicurezza, definite anche tramite la gestione di apparati di sicurezza specifici (es. soluzioni di sandboxing) in modo da ottimizzare l'uso delle risorse infrastrutturali, quali la capacità di banda verso Internet o il sistema di posta elettronica;
- Content security: l'attività provvede a una gestione efficace delle contromisure atte a contrastare la diffusione dei codici malevoli, quali virus o worm su sistemi client (postazione di lavoro) e server;
- Security Client and Server Hardening: l'attività provvede alla definizione, attuazione, gestione e controllo delle politiche di configurazione e di aggiornamento dei sistemi rilevanti per l'Amministrazione attraverso la determinazione e l'esecuzione di procedure specifiche;
- Rendere disponibile e aggiornata la documentazione sulla gestione e conduzione dei sistemi di sicurezza on-premise e cloud, nonché le descrizioni puntuali e verticali sui prodotti in essere (a titolo esemplificativo: sistema PAM, NDR ...) e nuovi che dovessero essere implementati (all'avvio del contratto, l'Amministrazione e il Fornitore concordano le informazioni che dovranno essere incluse nella documentazione relativa alla gestione e conduzione dei sistemi di sicurezza, sia on-premise che cloud).

Il Fornitore, entro due mesi dalla data di avvio dei servizi successiva al periodo di subentro/presa in carico deve fornire un rapporto dettagliato sullo "stato di salute" dei sistemi di RV presi in carico, evidenziando eventuali criticità e/o debolezze riscontrate sulla base di Penetration Test, Vulnerability Assessment e ulteriori test che ritiene opportuno. A seguito di tale attività, si prevede che il Fornitore condivida con RV un remediation plan con l'indicazione di tutte le contromisure necessarie da attuare, al fine di eliminare le vulnerabilità eventualmente rilevate, facendosi carico dell'espletamento delle contromisure di propria competenza. Si prevede che l'attività venga inclusa nel canone e che sia ripetuta con cadenza annuale. Inoltre, dovrà essere data evidenza all'Amministrazione tramite la presentazione di un report sull'esecuzione.

Il Fornitore deve dare supporto all'Amministrazione relativamente agli aspetti di sicurezza per l'adesione al Polo Strategico Nazionale (PSN) riguardo ai seguenti compiti:

- Garantire la realizzazione e il mantenimento dei livelli di sicurezza previsti per il dominio di competenza;
- Garantire che la politica di sicurezza presso l'Amministrazione sia conforme agli indirizzi e alle politiche di sicurezza definite nell'ambito di PSN;
- Effettuare un assessment per raccogliere, aggregare e predisporre nel formato richiesto le informazioni necessarie per verificare il livello di sicurezza del PSN;
- Fornire all'Amministrazione gli elementi necessari per la notifica al CERT di eventuali incidenti informatici;
- Proporre l'introduzione di ulteriori strumenti di sicurezza e relative figure professionali per la gestione, anche in corso di esecuzione del servizio;
- Prevedere l'introduzione, la gestione ed il monitoraggio di indicatori di qualità per misurare la sicurezza.

Il servizio di sicurezza logica dovrà prevedere, almeno, i seguenti requisiti minimi:

- Policy e strumenti di autenticazione sicura:
    - Autenticazione multifattoriale (MFA): richiedere almeno due fattori di autenticazione (password e token o impronta digitale);
    - Gestione sicura delle password: introduzione ed attuazione di politiche forti per la creazione, gestione e scadenza delle password, con l'uso di generatori di password sicure e il divieto di

riutilizzare password compromesse.

- Policy di autorizzazione e controllo degli accessi:
  - Controllo degli accessi basato sui ruoli (RBAC): assegnazione dei permessi in base ai ruoli aziendali e ai compiti specifici degli utenti;
  - Principio del minimo privilegio: gli utenti devono avere accesso solo alle risorse strettamente necessarie per svolgere le loro mansioni;
  - Segregazione dei compiti: separare le attività critiche per evitare che un singolo utente o processo abbia troppo controllo o potere.
- Sistemi di crittografia dei dati:
  - Gestione del Transport Layer Security (TLS): utilizzare protocolli sicuri come TLS/SSL per proteggere i dati durante la trasmissione (es. HTTPS) nel rispetto delle "Linee guida funzioni crittografiche - Transport Layer Security (TLS)" prodotte da ACN ed eventuali successive modificazioni;
  - Gestione della crittografia: protezione dei dati memorizzati utilizzando tecniche di cifratura (es. crittografia dei dischi o database crittografati), funzioni di hash, conservazione delle password nel rispetto delle "Linee guida funzioni crittografiche" prodotte da ACN ed eventuali successive modificazioni;
  - Gestione sicura delle chiavi crittografiche: implementare sistemi sicuri di gestione delle chiavi per evitare accessi non autorizzati mediante l'utilizzo di un modulo di sicurezza fisico (HSM Hardware Security Module). Tale gestione dovrà applicarsi sia in ambito PSR che in ambito Giunta Regionale e dovrà rispettare i requisiti imposti dal "Regolamento per le infrastrutture digitali e per i servizi cloud" di ACN (livello 1 e livello 2) ed eventuali successive modifiche. In particolar modo dovrà supportare anche un meccanismo di cifratura di tipo Bring Your Own Key (BYOK), ove applicabile, che consenta all'Amministrazione e ai vari Enti fruitori del servizio di generare autonomamente le proprie chiavi di cifratura. Rientrano nell'ambito di tale gestione, attraverso le adeguate competenze del personale tecnico, a titolo esemplificativo e non esaustivo:
    - Il mantenimento e/o l'aggiornamento della documentazione inerenti alle procedure di crittografia;
    - La verifica periodica di sistemi, politiche e processi di crittografia e gestione delle chiavi in risposta all'aumento dell'esposizione al rischio, valutato mediante audit da eseguire con cadenza almeno annuale o dopo qualsiasi evento di sicurezza;
    - L'applicazione di meccanismi di rotazione delle chiavi crittografiche secondo il periodo di validità delle stesse, tenendo conto di possibili rischi e requisiti normativi e legali.
- Attività proattive di protezione dalle minacce:
  - Software di sicurezza aggiornati: utilizzare antivirus, anti-malware e firewall costantemente aggiornati per rilevare e bloccare minacce;
  - Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS): monitorare il traffico di rete per identificare e bloccare attività sospette;
  - Protezione contro le vulnerabilità note: utilizzare strumenti di scansione delle vulnerabilità e aggiornare regolarmente i sistemi con patch di sicurezza.
- Attività di gestione dei log e monitoraggio:
  - Audit e log delle attività: registrare tutte le operazioni di accesso, modifiche e tentativi di violazione con strumenti di monitoraggio centralizzati;
  - Monitoraggio in tempo reale: utilizzare sistemi di monitoraggio attivi per individuare minacce o

anomalie in tempo reale;

- Analisi dei log: analizzare regolarmente i log di sicurezza per rilevare eventuali comportamenti anomali o minacce latenti.

- Gestione delle vulnerabilità e patch:
  - Gestione centralizzata delle patch: applicare regolarmente aggiornamenti e patch di sicurezza a sistemi operativi, applicazioni e firmware; si precisa che il Fornitore deve fornire anche gli strumenti di patch management che coprano tutte le esigenze espresse da Regione del Veneto;
  - Scansione delle vulnerabilità: eseguire test continuativi per identificare vulnerabilità nei sistemi, applicazioni e configurazioni; per la gestione del patch management, deve essere fornito un tool per gestire in modo efficace le attività e permettere, ai fini di audit, di verificare la bontà delle attività svolte;
  - Penetration test: condurre test di penetrazione periodici (si suggerisce almeno con cadenza mensile) per simulare attacchi e individuare debolezze sfruttabili.
- Piani di backup e ripristino:
  - Backup regolari: eseguire backup periodici dei dati critici in modo sicuro, sia on-site che off-site;
  - Cifratura dei backup: proteggere i dati di backup con tecniche di crittografia;
  - Procedure di disaster recovery: implementare piani di ripristino in caso di incidente (disaster recovery) per garantire la disponibilità dei dati e dei sistemi in caso di guasto o attacco.
- Controllo delle applicazioni:
  - Whitelist delle applicazioni: permettere l'esecuzione solo di applicazioni autorizzate per ridurre il rischio di eseguire software malevolo;
  - Verifica del codice: implementare procedure di revisione e verifica del codice per identificare potenziali vulnerabilità o backdoor nelle applicazioni interne;
  - Gestione aggiornamento applicazioni installate su PdL, evitando la permanenza di versioni obsolete e con conseguenti vulnerabilità;
  - Gestione degli asset e software attraverso l'integrazione con il prodotto di asset management come descritto nel paragrafo 5.4.2.2 - Inventario periodico degli asset.
- Formazione e consapevolezza del personale:
  - Formazione continua sulla sicurezza: educare i dipendenti su best practice di sicurezza, phishing, e altre minacce comuni;
  - Politiche di utilizzo accettabile: stabilire linee guida chiare per l'uso sicuro delle risorse aziendali e della rete;
  - Simulazioni di phishing: condurre test simulati di attacchi di phishing per verificare la preparazione del personale.
- Gestione delle identità:
  - Identity and Access Management (IAM): implementare soluzioni per la gestione centralizzata delle identità digitali e degli accessi degli utenti;
  - Single Sign-On (SSO): abilitare l'autenticazione unica per facilitare l'accesso sicuro a più applicazioni con un unico set di credenziali;
  - Revoca tempestiva degli accessi: assicurarsi che gli account di utenti non più attivi (dipendenti usciti o collaboratori temporanei) vengano disattivati immediatamente.
- Segmentazione della rete:

- Segmentazione e isolamento delle reti: separare i sistemi critici da quelli meno sicuri, utilizzando VLAN, firewall e zone demilitarizzate (DMZ);
- Protezione delle reti interne: implementare firewall interni e monitorare il traffico di rete per prevenire movimenti laterali di eventuali attaccanti.

- Gestione degli incidenti:
  - Piani di risposta agli incidenti: definire protocolli per rispondere rapidamente e in modo efficace a eventuali incidenti di sicurezza;
  - Team di gestione incidenti: disporre di un team dedicato o assegnato alla gestione delle emergenze e alla mitigazione dei rischi dopo un attacco;
  - Notifica delle violazioni: procedure chiare per la segnalazione interna ed esterna di violazioni di sicurezza (data breach), inclusa la notifica alle autorità competenti (secondo le normative della NIS2 e della Legge 90/2024).
- Politiche di accesso remoto sicuro:
  - VPN crittografate: utilizzare reti private virtuali (VPN) per proteggere l'accesso remoto alle risorse aziendali;
  - Autenticazione forte per l'accesso remoto: richiedere metodi di autenticazione robusti per gli utenti che si collegano da remoto, come MFA.
- Test e audit di sicurezza periodici:
  - Audit di sicurezza regolari: condurre verifiche periodiche delle politiche di sicurezza e della loro corretta implementazione;
  - Certificazioni di conformità: verificare che l'organizzazione aderisca a standard e normative di sicurezza, come ISO 27001, GDPR, o PCI-DSS.
- Politiche di accesso fisico ai sistemi critici:
  - Sicurezza fisica del datacenter: proteggere fisicamente server e dispositivi con accesso controllato (badge, telecamere, guardie) per evitare accessi non autorizzati;
  - Politiche di accesso alle workstation: garantire che i dispositivi fisici, come computer e laptop, siano protetti da accessi non autorizzati tramite blocco automatico e password.

Inoltre, il Fornitore deve dare supporto all'Amministrazione relativamente agli aspetti di sicurezza per l'adesione al Polo Strategico Nazionale (PSN) riguardo ai seguenti compiti:

- Garantire la realizzazione e il mantenimento dei livelli di sicurezza previsti per il dominio di competenza;
- Garantire che la politica di sicurezza presso l'Amministrazione sia conforme agli indirizzi e alle politiche di sicurezza definite nell'ambito di PSN;
- Effettuare un assessment per raccogliere, aggregare e predisporre nel formato richiesto le informazioni necessarie per verificare il livello di sicurezza del PSN;
- Fornire all'Amministrazione gli elementi necessari per la notifica al CERT di eventuali incidenti informatici;
- Proporre l'introduzione di ulteriori strumenti di sicurezza e relative figure professionali per la gestione, anche in corso di esecuzione del servizio;
- Prevedere l'introduzione, la gestione ed il monitoraggio di indicatori di qualità per misurare la sicurezza.

5.1.7.1 Soluzione per lo storage e gestione sicura delle password

Il Fornitore dovrà mettere a disposizione di RV, senza alcun costo aggiuntivo, una soluzione per lo storage e gestione sicura delle password a 360°, da fornire a tutto il personale, inclusiva di funzionalità atte a garantire sicurezza, praticità,

scalabilità e flessibilità, preferibilmente installato On-Premise presso i sistemi di RV. Tale soluzione dovrà essere in grado di gestire almeno 3.000 utenti, assicurando un'architettura scalabile in caso di necessità. Si specifica che la soluzione deve essere intesa come strumento di gestione a livello Enterprise di credenziali accesso utente.

Tale soluzione deve prevedere una gestione avanzata dei permessi, in ottica di definizione di specifiche autorizzazioni suddivise per gruppi, dipartimenti o singoli utenti. Inoltre, in ottica di gestione di circostanze straordinarie, tale sistema deve prevedere funzionalità di accesso delegato, utile per gestire situazioni di emergenza, permettendo quindi ad eventuali amministratori o utenti di fiducia di accedere agli account.

In termini di integrazione e compatibilità, si prevede che la soluzione si integri con gli strumenti attualmente in uso presso RV (i dettagli relativi agli strumenti in perimetro verranno forniti ad avvio del servizio), oltre a risultare compatibile con più sistemi operativi, a titolo esemplificativo e non esaustivo Windows, Mac e Linux. Inoltre, si prevede che la soluzione sia compatibile con dispositivi fissi (PC) e con dispositivi mobili (Tablet, Smartphone e SmartWatch) tramite la predisposizione di applicazioni dedicate, migliorando l'accessibilità e la gestione in mobilità. Infine, dev'essere assicurata compatibilità con i principali browser, in particolare Mozilla e Chrome, prevedendo quindi la possibilità di auto-completamento e di generazione di password random.

In termini di sicurezza, la soluzione deve prevedere metodi di autenticazione avanzati quali, a titolo esemplificativo e non esaustivo, MFA e autenticazione biometrica, oltre a qualsiasi altra soluzione ritenuta congrua a garantire un adeguato livello di sicurezza, facendo riferimento a best practice ed esperienze pregresse.

Per quanto riguarda la sicurezza delle password utilizzate, il sistema deve prevedere dei criteri specifici di impostazione delle password, quali a titolo esemplificativo: lunghezza minima, utilizzo di simboli e utilizzo di numeri. Inoltre, la soluzione proposta deve prevedere funzionalità di verifica delle password utilizzate, confrontando suddette credenziali con quelle esposte in violazioni pubbliche e, in caso di corrispondenza, produrre un alert indirizzato all'utente indicando la necessità di cambiare la password compromessa.

Infine, con l'obiettivo di garantire una valutazione dinamica del livello di sicurezza di suddette password si prevede la possibilità di condurre degli audit automatici, e produrre relativi report, volti alla verifica dell'adeguatezza delle password impostate dagli utenti con una cadenza che verrà stabilita ad avvio del servizio.

5.1.8 End Point Protection avanzato

Il Fornitore rende disponibile un servizio di End Point Protection avanzato in modalità As a Service, attraverso una piattaforma XDR che integri una protezione basata sull'AI, capace di integrarsi con il SIEM utilizzato dal servizio SOC regionale per garantire una gestione proattiva degli incidenti di sicurezza, erogato tramite il proprio centro servizi. In tal senso, si prevede che il Fornitore si occupi della gestione dei seguenti strumenti/attività:

- Piattaforma di Gestione:
  - Rendere disponibile, ovvero fornire, una piattaforma centralizzata per la gestione degli End Point (Server on-prem e in Cloud, workload nel cloud, container, Postazioni di Lavoro (PdL), Tablet e Smartphone degli utenti). I costi di licenza devono essere inclusi nel servizio di gestione licenze. Per maggiori dettagli si veda l'Appendice 3 Contesto Tecnologico e Applicativo.
  - La piattaforma deve supportare policy di sicurezza configurabili, con opzioni per personalizzare le impostazioni in base al tipo di dispositivo e alla sensibilità dei dati.
- Gestione del Servizio:
  - Supportare il gruppo di distribuzione software (SW distribution) nell'installazione degli agent su PdL, Server, tablet, smartphone e qualsiasi altro dispositivo in perimetro di suddetta distribuzione.
  - Garantire la manutenzione continua della piattaforma e degli agent, con aggiornamenti regolari di:
    - Patch di sicurezza;
    - Firme antimalware e altre definizioni.
  - Monitorare gli End Point in tempo reale, segnalando e gestendo le criticità rilevate.

- Effettuare azioni di remediation diretta sulle PdL infette tramite la console di amministrazione.
- Fornire reportistica dettagliata, su base trimestrale sull'andamento del servizio, incluso lo stato di protezione e la lista degli End Point in quarantena.

- Protezione Avanzata:
  - Oltre a garantire protezione contro malware, spyware, adware, ransomware e phishing, la piattaforma deve includere:
    - Protezione contro exploit zero-day;
    - File-less attack detection, rilevando minacce che non utilizzano file tradizionali;
    - Controllo del traffico web per prevenire accessi a siti pericolosi;
    - Gestione delle credenziali compromesse, prevenendo utilizzi non autorizzati.
- Integrazione:
  - La soluzione deve essere modulare e integrabile con un SIEM (Security Information and Event Management) e un SOC (Security Operation Center) per:
    - Raccogliere e correlare eventi di sicurezza;
    - Fornire visibilità centralizzata su tutte le minacce rilevate;
    - Abilitare risposte rapide e coordinate alle emergenze.
- Fase di Avvio del Servizio:
  - Effettuare un assessment iniziale del perimetro operativo, identificando rischi e criticità.
  - Implementare e rendere avviabile il servizio in accordo con le policy di protezione fornite dall'Amministrazione, ovvero fornire all'Amministrazione le configurazioni adeguate al contesto di RV e che seguano le best practice indicate dal produttore.
  - Definire e concordare con l'Amministrazione le modalità di aggiornamento (automatico o manuale) per PdL e Server.
- Ambiti di Protezione:
  - Protezione dei server localizzati presso i Data Center, con agent compatibili con ogni sistema operativo.
  - Protezione delle piattaforme applicative in ambienti cloud, con supporto per ambienti multicloud e ibridi.
  - Protezione delle Postazioni di Lavoro, con gestione delle periferiche (es. dispositivi USB) e delle policy di sicurezza.
  - Protezione Table e Smartphone.
- Reportistica Mensile:
  - Lista degli End Point installati, con stato di attivazione per PdL e Server.
  - Lista delle versioni degli agent installati.
  - Lista degli End Point in quarantena, con dettaglio delle azioni correttive previste o in corso.
  - Trend di sicurezza per rilevare eventuali aumenti o diminuzioni di criticità nel tempo.

5.1.9 Conduzione e gestione della manutenzione Hardware dell'Infrastruttura

Il servizio Conduzione e Gestione della manutenzione HW richiesto consiste nella riparazione dei guasti che possono verificarsi alle apparecchiature presenti nel Data Center primario di Venezia Vega e nei siti secondari VSIX e Infocamere di Padova, elencate nella lista riportata in Appendice 3 Contesto Tecnologico e Applicativo e nella esecuzione delle prove e dei controlli necessari per il ripristino delle apparecchiature alla normale funzionalità.

Le attività richieste al Fornitore si differenziano tra manutenzione:

- **Preventiva**: interventi periodici per evitare l'insorgere di malfunzionamenti. Si richiede un intervento on-site di manutenzione preventiva su tutte le apparecchiature HW da manutenere almeno ogni 15 giorni solari;
- **Correttiva**: azioni volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità attraverso attività di supporto on-site. In caso di **apparati fuori garanzia**, le attività richieste comprendono, a titolo esemplificativo e non esaustivo:
    - Eliminazione degli inconvenienti che hanno determinato la richiesta di intervento;
    - Controllo e ripristino delle normali condizioni di funzionamento;
    - Fornitura ed applicazione delle parti di ricambio della stessa marca, modello e tipo nuove di fabbrica per la manutenzione dell'esistente. Qualora la parte di ricambio necessaria per il ripristino delle funzionalità dell'apparecchiatura HW guasta non fosse più disponibile, il Fornitore deve comunicare a RV la necessità di acquistare la nuova apparecchiatura HW;
    - Aggiornamento della relativa documentazione;
    - Redazione del relativo "verbale di intervento".

È compito del Fornitore attivare gli interventi di manutenzione correttiva a seguito di segnalazioni del sistema di monitoraggio o dell'Amministrazione, attraverso il sistema di Trouble Ticketing. Il Fornitore deve comunicare tempestivamente al DEC tutti gli interventi di manutenzione correttiva aperti e la loro risoluzione, inclusa ogni eventuale problematica che si dovesse riscontrare.

Per gli **apparati in garanzia**, il Fornitore deve gestire il rapporto con terzi, facendosi carico di attivare il rapporto di garanzia, preventivamente interfacciandosi con il Referente di RV. Al Fornitore è richiesto, comunque, di dare supporto ai terzi nelle attività di competenza favorendo il buon esito e la tempestività di risoluzione dell'intervento. In tale ipotesi, valgono i livelli di servizio contrattualizzati con i terzi, senza responsabilità del Fornitore del presente CT. Alla scadenza dei singoli periodi di garanzia, le apparecchiature sono prese completamente in carico dal Fornitore che ne effettuerà la manutenzione diretta.

È, inoltre, in carico al Fornitore la:

- Gestione della movimentazione degli apparati (Server, rack ecc…) tra Data Center primario di Venezia Vega e Data Center di DR di Padova o all'interno di uno dei Data Center stessi, secondo necessità;
- Attività svolte in ottemperanza alla normativa indicata al § 9.6.2 di:
    - Data wiping (cancellazione) con specifici software proposti dal Fornitore e concordati con il Referente di RV;
    - De-magnetizzazione dei dischi tramite degaussing;
    - Distruzione fisica dei dischi;
    - Gestione della movimentazione dei dispositivi per la sicurezza.

In caso di restituzione dell'apparato a seguito di un guasto, è a carico del Fornitore il costo di restituzione, le spese di spedizione e di eventuali altri oneri logistici.

Nel caso in cui invece la parte di ricambio necessaria per il ripristino delle funzionalità dell'apparecchiatura HW guasta non fosse più disponibile o l'apparato stesso non fosse più manutenibile, il Fornitore deve comunicare a Regione del Veneto la necessità di acquistare la nuova apparecchiatura HW e l'acquisto della stessa sarà a carico dell'Amministrazione.

5.1.10 Attività di Formazione

All'interno dei servizi di Conduzione operativa sistemi e sicurezza, l'aggiudicatario dovrà programmare ed erogare un piano di formazione dedicato al personale tecnico e operativo di RVE con contenuti coerenti ai servizi ambito dell'appalto.

L'attività dovrà essere programmata con sufficiente anticipo ed erogata nel corso del contratto al personale tecnico e operativo di RVE coinvolto, e tale attività è ricompresa all'interno dei canoni e delle attività già previste per i servizi di conduzione operativa dei sistemi e sicurezza.

5.2 Servizio di conduzione operativa – attività monitoraggio H24

Il servizio di Monitoraggio H24 dei sistemi comprende un sottoinsieme di attività, a corredo delle attività indicate al paragrafo 5.1 - Servizi di conduzione operativa sistemi e sicurezza, di gestione finalizzate a garantire l'operatività dei sistemi del sito primario di Venezia Vega, del sito di DR di Padova e degli ambienti cloud, in modalità H24, compresi gli orari notturni e nei giorni di sabato (se non incluso nell'orario di presidio), domenica e festivi, quando non sono operativi gli altri servizi.

Principalmente il servizio di Monitoraggio H24 include il complesso delle attività volte alla ricezione delle segnalazioni dei malfunzionamenti, alla verifica e all'analisi degli allarmi generati dai sistemi e delle informazioni raccolte attraverso la strumentazione di monitoraggio, nonché le attività di risoluzione al I° livello e di escalation ai livelli superiori degli eventi occorsi. Inoltre, il servizio include attività di gestione e controllo H24 della schedulazione di procedure codificate.

Nel servizio di Monitoraggio H24 sono incluse tutte le attività di gestione che possono essere efficacemente svolte in modalità remota senza ricorrere alle risorse del Presidio operativo. Il servizio di Monitoraggio H24 è svolto attraverso la "service control room" presente nel Centro Servizi del Fornitore, ma è strettamente legato e complementare ai servizi di Presidio operativo: nella fascia oraria di copertura del Presidio operativo, infatti, i due servizi sono collegati tra loro per effettuare in modo integrato e complementare le attività di monitoraggio e gestione dei sistemi.

Il servizio di Monitoraggio H24 viene erogato mediante collegamento telematico alla rete dell'Amministrazione. Nell'ambito del servizio, il Fornitore dovrà mettere a disposizione di RV e quindi del servizio da esso erogato quanto segue:

- Numero telefonico dedicato attivo oltre le 18 fino alle 8; la richiesta di intervento dall'esterno dovrà essere censita dal team di monitoraggio sulla piattaforma SysAid per la verifica degli SLA. Il numero telefonico dedicato è anche per utenti esterni (ovvero utenti del PSR);
- Piattaforma di Monitoraggio dei sistemi e delle applicazioni per la rilevazione degli alert e dei parametri di funzionamento dei medesimi.

Il numero telefonico dedicato e l'utilizzo della piattaforma di monitoraggio sono inclusi nei costi del servizio e pertanto non comporta alcun onere aggiuntivo per RV; in particolare, è incluso nei costi del servizio l'eventuale installazione di componenti client (agent) da installare sui sistemi dell'Amministrazione. La piattaforma di monitoraggio dovrà consentire di tenere sotto controllo lo stato operativo dei sistemi e delle relative componenti e degli apparati di rete, rilevando automaticamente informazioni quali a titolo esemplificativo, ma non esaustivo, le seguenti:

- Stato dei diversi sistemi, sottosistemi, servizi ed apparati;
- Parametri critici per la funzionalità dei diversi sistemi, sottosistemi, servizi ed apparati, definendo dei valori di soglia che rilevano la prossimità di situazioni critiche. Ad esempio, tali parametri potranno riguardare eventi di tipo infrastrutturale quali:

- Disponibilità dei processi di sistema operativo, di rete, di networking, di database, ecc.;
- Allocazioni di spazio disco;
- Utilizzo della memoria;
- Utilizzo della CPU;
- Utilizzo delle interfacce di rete.

- Stato dei processi applicativi di particolare rilevanza, definiti Mission Critical (si rimanda all'Appendice 3 - Contesto tecnologico e applicativo, per l'elenco degli applicativi con criticità alta), fondamentali per la funzionalità dei servizi erogati, includendo eventi quali, ad esempio:
  - Disponibilità di processi applicativi;
  - Tempi di risposta delle transazioni;
  - Errori applicativi che prevedano la registrazione su file di log, dump, ecc.

Nell'ambito della piattaforma di monitoraggio, il Fornitore dovrà prevedere una soluzione per il monitoraggio end-to-end dei servizi applicativi erogati agli utenti finali, in modo da poterne facilmente verificare lo stato operativo e prestazionale.

Correlando tutte le informazioni provenienti dai vari sistemi che costituiscono l'ambiente di esercizio con quelle relative alle transazioni applicative, la soluzione dovrà dare evidenza dello stato operativo dei servizi applicativi erogati ed essere così di supporto alla rapida risoluzione dei problemi. In particolare, dovrà consentire di identificare automaticamente le componenti da controllare lungo la catena applicativa in caso di errore.

Oltre a monitorare la disponibilità dei servizi applicativi definiti Mission Critical e ad essere di supporto nella risoluzione dei problemi, la soluzione dovrà consentire di verificare e controllare le performance dei servizi erogati per verificarne l'aderenza ai livelli di servizio attesi.

L'attivazione della piattaforma di monitoraggio deve essere completata entro 4 mesi dalla data di avvio dei servizi successiva al periodo di subentro/presa in carico e consultabile dal personale di Regione e, su richiesta, i dati devono essere messi a disposizione di Regione estraendoli in formati csv, txt, xls, ovvero anche tramite ETL, rendendoli disponibili anche ad altri applicativi/piattaforme.

Monitoraggio H24 relativi ai servizi- PSR
Il monitoraggio H24, con supporto in lingua italiana 7 giorni su 7 (quindi anche fuori dall'orario d'ufficio), dovrà coprire sia l'infrastruttura di base, ovvero i sistemi che costituiscono ed abilitano l'erogazione dei servizi del Polo Strategico Regionale (PSR), sia le segnalazioni di incidente che potranno essere aperte dagli enti aderenti al PSR attraverso il Self-Service Portal (SSP) erogato attraverso la piattaforma tecnologica SysAid.

Con particolare riferimento a quest'ultima casistica, si sottolinea che a ciascuna tipologia di segnalazione di incidente è stata associata - oppure per nuove tipologie verrà associata - una categoria di SLA di intervento che dovrà essere rispettata dal Fornitore.

Quanto appena descritto e che viene richiesto al Fornitore è in linea e dovrà rimanere aggiornato rispetto ai requisiti del "Regolamento per le infrastrutture digitali e per i servizi cloud" emanato da ACN in Agosto 2024.

5.3 Servizi di supporto

I Servizi di supporto di cui RV intende avvalersi nella presente procedura aperta e di seguito descritti sono:

- Supporto Specialistico;
- Sistema di monitoraggio continuo e AI;
- Supporto per i percorsi di certificazione ISO;
- Supporto per compliance normativa NIS2 o altre normative e regolamenti che richiederanno un adeguamento alla compliance;

- Interventi fuori orario;

Il servizio di supporto potrà inoltre essere attivato per eventuali evoluzioni legislative in materia di Cyber Security.

5.3.1 Supporto Specialistico

Il servizio di supporto specialistico richiede l'attuazione di un processo strutturato e collaborativo tra Regione Veneto e il Fornitore. Questo processo include una serie di attività complesse che devono essere gestite con precisione per garantire che le esigenze di RV siano soddisfatte in modo efficiente.

Tale servizio rappresenta un elemento cruciale per garantire che le attività ad alto contenuto tecnologico siano eseguite correttamente, superando l'ambito delle normali operazioni di conduzione. Questo servizio è pensato per fornire assistenza tecnica avanzata sia a RV sia alle strutture operative del Fornitore, e include competenze specializzate che vanno oltre la semplice manutenzione ordinaria. La sua attuazione richiede l'impiego di risorse professionali altamente qualificate e l'integrazione di tecnologie all'avanguardia.

Si sottolinea che le giornate spese per suddetto servizio dovranno obbligatoriamente essere rendicontate nel SAL trimestrale.

Le attività di supporto specialistico includono, a titolo esemplificativo e non esaustivo le seguenti tematiche:

- Predisposizione, modifica e aggiornamento del Catalogo dei Servizi offerti da Regione Veneto nell'ambito del Progetto di convergenza Infrastrutturale;
- Definizione di criteri di accettazione dei servizi (SAC) in caso di nuovi servizi e/o evoluzione dei servizi esistenti;
- Definizione e miglioramento dei processi di service management o dei processi operativi in generale;
- Definizione e verifica delle politiche di sicurezza;
- Processi di capacity management dei sistemi ed evoluzione tecnologica degli stessi;
- Definizione di piani di disponibilità e continuità operativa delle infrastrutture.

Processo dettagliato per la gestione delle richieste

Il supporto specialistico consiste, pertanto, in attività richieste da RV al Fornitore su tematiche ad hoc di volta in volta concordate, di cui di seguito si evidenzia il processo articolato nei seguenti passi:

1. Emissione della richiesta da parte di RV

- **Descrizione della richiesta**: RV invia una richiesta al Fornitore con una descrizione sommaria dell'intervento richiesto. La richiesta deve contenere le informazioni essenziali, come l'ambito di intervento, l'output atteso, e il Referente del Servizio che si occuperà della gestione;
- **Ruolo coinvolto**: il **Referente del Servizio** di RV ha la responsabilità di inviare la richiesta e monitorare il processo.

2. Valutazione ed elaborazione della richiesta

- **Collaborazione**: il Fornitore esamina la richiesta e collabora con il Referente di RV per definire i dettagli dell'intervento. Il Fornitore può richiedere ulteriori informazioni per chiarire gli obiettivi.
- **Piano di Intervento**: entro 5 giorni lavorativi, il Fornitore prepara un Piano di Intervento che include:
    - Descrizione delle attività necessarie;
    - Suddivisione del lavoro per figura professionale;
    - Pianificazione temporale;
    - Output atteso.
- **Ruoli coinvolti**:

- **Project Manager (PM)** del Fornitore: gestisce la definizione del Piano di Intervento, coordinando il team tecnico;
- **Specialisti Tecnici**: collaborano con il PM per definire le risorse necessarie e gli strumenti da utilizzare;
- **Referente del Servizio RV**: fornisce input e feedback per garantire che la richiesta sia ben definita.

3. Approvazione del piano di intervento

- **Verifica**: l'Amministrazione verifica il Piano di Intervento proposto dal Fornitore, valutandone la fattibilità e la coerenza con gli obiettivi richiesti;
- **Feedback**: in caso di necessità, l'Amministrazione può chiedere revisioni o rifiutare il Piano;
- **Ruolo coinvolto**: **Responsabile della Governance di RV**, che valuta la proposta del Fornitore e approva o richiede modifiche.

4. Esecuzione della richiesta

- **Implementazione**: dopo l'approvazione, il team del Fornitore inizia l'esecuzione delle attività. Questo include l'utilizzo di strumenti e competenze specifiche per completare le attività richieste;
- **Coinvolgimento**: a seconda della complessità dell'intervento, possono essere coinvolti altri fornitori esterni;
- **Ruoli coinvolti**:
  - **Team Tecnico del Fornitore**: esegue le attività operative;
  - **Referente del Servizio RV**: supervisiona l'esecuzione e fornisce supporto quando necessario.

5. Validazione intermedia

- **Monitoraggio e feedback**: Durante l'esecuzione, il Fornitore può inviare aggiornamenti informali via e-mail per evitare disallineamenti rispetto alle aspettative. Eventuali problemi possono essere risolti in questa fase;
- **Ruoli coinvolti**: Il **Referente del Servizio RV** e il **PM del Fornitore** scambiano feedback e monitorano l'avanzamento del progetto.

6. Consegna dei risultati

- **Output**: Al termine dell'intervento, il Fornitore consegna l'output concordato all'Amministrazione. In caso di richieste più complesse, può essere prevista una sessione di verifica o test;
- **Ruoli coinvolti**: Il **Team Tecnico del Fornitore** fornisce i risultati finali, mentre il **Referente del Servizio RV** valuta l'output consegnato.

7. Validazione finale ed eventuali revisioni

- **Conformità**: RV verifica se l'output finale corrisponde a quanto richiesto. Se necessario, può richiedere revisioni o integrazioni;
- **Modifiche**: In caso di modifiche sostanziali, il Fornitore aggiorna il Piano delle Attività, che deve essere approvato formalmente prima di procedere;
- **Ruoli coinvolti**:
  - **Referente del Servizio RV**: verifica la conformità dell'output;
  - **PM del Fornitore**: si occupa di eventuali revisioni e della nuova approvazione del Piano.

In ottica di garantire un processo efficiente ed efficace di supporto specialistico, il Fornitore è tenuto a:

- **Integrare strumenti di monitoraggio automatico delle performance**, con l'uso di dashboard che forniscano metriche in tempo reale sull'avanzamento delle attività;

- **Implementare una piattaforma di collaborazione digitale** che permetta la gestione delle richieste, approvazioni e modifiche in modo strutturato, riducendo il rischio di disallineamenti;
- **Predisporre audit periodici di verifica** delle attività svolte, garantendo un continuo miglioramento e adattamento delle soluzioni alle esigenze tecnologiche e operative emergenti.

Tali miglioramenti rafforzerebbero la capacità di RV di monitorare in tempo reale l'andamento dei lavori e aumenterebbero la trasparenza nel processo di gestione delle risorse e delle competenze coinvolte.

5.3.2 Sistema di monitoraggio continuo e AI

In ottica di miglioramento dell'efficienza e di garanzia di trasparenza durante tutto il ciclo di vita del progetto, si richiede l'introduzione di un sistema di monitoraggio continuo che utilizzi metriche di performance condivise e definite con RV. Queste metriche potrebbero includere, a titolo esemplificativo e non esaustivo:

- **Tempi di esecuzione**;
- **Qualità del servizio** (misurata attraverso KPI);
- **Soddisfazione dell'Amministrazione**.

L'obiettivo è implementare la capacità di identificare tempestivamente eventuali criticità o ritardi, intervenendo così proattivamente, introducendo inoltre l'utilizzo di algoritmi di intelligenza artificiale efficientando in questo modo la gestione del supporto specialistico. A titolo esemplificativo e non esaustivo, l'AI potrebbe essere impiegata per:

- **Prevedere la domanda**: analizzando i dati storici, l'AI potrebbe suggerire quali ambiti potrebbero necessitare di supporto specialistico futuro;
- **Ottimizzare l'allocazione delle risorse**: gli algoritmi potrebbero suggerire come distribuire al meglio le risorse professionali in base alla complessità delle richieste;
- **Automatizzare l'analisi di dati operativi**: questo permetterebbe una visione più accurata delle performance e delle necessità di aggiornamento dei sistemi.

Il servizio prevede la produzione di un documento periodico, il Report di Monitoraggio e Previsione; l'Amministrazione deciderà la periodicità ad inizio contratto, che includerà le metriche di performance rilevate, i trend identificati e le previsioni generate dagli algoritmi di AI.

Il report conterrà un'analisi dettagliata delle eventuali criticità riscontrate e delle azioni correttive suggerite. Inoltre, saranno inclusi suggerimenti per il miglioramento continuo delle attività, basati sui risultati delle analisi storiche e previsionali.

5.3.3 Supporto per i percorsi di certificazione ISO

Il **servizio di supporto per le certificazioni ISO** ha l'obiettivo di assistere Regione del Veneto nel raggiungimento delle certificazioni necessarie per la gestione e la sicurezza dei suoi servizi IT e delle infrastrutture tecnologiche.

RV ha già ottenuto le seguenti certificazioni:

- **ISO 14001** (gestione ambientale);
- **ISO/IEC 9001:2015** Sistema di Gestione della Qualità (SGQ);
- **ISO/IEC 27001:2022** Sistema di Gestione per la Sicurezza delle Informazioni (SGSI);
- **ISO/IEC 27001:2013** Sistema di Gestione per la Sicurezza delle Informazioni (SGSI);
- **ISO/IEC 22301:2019** Sistema di Gestione della Continuità Operativa (SGCO).

Il Fornitore è tenuto ad assistere RV nel mantenimento delle certificazioni e nell'implementazione dei percorsi necessari per ottenere le seguenti certificazioni:

- **ISO 20000-1**: gestione dei servizi IT, che assicura che i servizi IT siano erogati in modo efficiente e conforme alle migliori pratiche internazionali.

Per altre eventuali informazioni circa le certificazioni (ad es. scope e relativi perimetri, si rimanda al sito https://www.regione.veneto.it/web/informatica-e-e-government/certificazioni-qualita-sicurezza)

Si sottolinea che il supporto al mantenimento ed adeguamento è inteso, a titolo esemplificativo e non esaustivo, nelle seguenti fattispecie:

- Aggiornamento della norma di certificazione;
- Supporto negli audit e nelle verifiche ispettive;
- Gestione della documentazione e delle procedure;
- Formazione e aggiornamento del personale;
- Monitoraggio e miglioramento continuo;
- Supporto tecnico e operativo.

Infine, si è evidenziato che l'infrastruttura di RV possiede un adeguamento di **livello 2**, mentre il cloud ha un attuale **livello 1** (con un piano per raggiungere il livello 2). Questa qualificazione indica il grado di maturità dell'infrastruttura e del cloud in termini di sicurezza e conformità agli standard internazionali.

Attività chiave del supporto per i percorsi di certificazione ISO

Il supporto fornito dal Fornitore si articola nelle seguenti attività, che coprono l'intero ciclo di certificazione, dalla pianificazione fino alla verifica finale con un Ente terzo:

1. **Impostazione del progetto di certificazione**: definizione degli obiettivi e delle fasi di lavoro per ottenere la certificazione, con chiara identificazione dei ruoli e delle responsabilità;
2. **Definizione del piano dei rischi e delle modalità di controllo**: analisi dei rischi connessi alla sicurezza, alla gestione IT e alla continuità operativa, con piani di mitigazione e monitoraggio continuo per garantire la conformità agli standard ISO;
3. **Identificazione dei gap organizzativi**: valutazione delle carenze strutturali e organizzative rispetto agli standard richiesti dalle ISO, con l'obiettivo di rendere l'organizzazione conforme alle norme. Questa attività include la definizione di tempi e costi per colmare i gap individuati;
4. **Stesura delle policy**: creazione e revisione delle policy di gestione, che definiscono ruoli, responsabilità e procedure per garantire il miglioramento continuo del sistema di gestione;
5. **Affiancamento del personale (training on the job)**: supporto pratico e formazione continua del personale coinvolto, per garantire che il team sia in grado di implementare e mantenere i requisiti delle certificazioni;
6. **Audit e test interni**: esecuzione regolare di verifiche interne e test per accertare che i controlli siano efficaci e che i piani di risposta agli incidenti siano pienamente operativi. Questo garantisce la continuità dei servizi e la conformità durante l'intero periodo del contratto;
7. **Supporto alla certificazione con un Ente terzo**: il Fornitore assiste RV nella ricerca e nel contatto con l'Ente terzo accreditato per ottenere la certificazione formale. Questo include la preparazione della documentazione e il supporto durante l'audit finale. I costi relativi al rapporto con l'Ente terzo sono a carico di RV;
8. **Supporto post-audit**: dopo l'audit da parte dell'Ente terzo, il Fornitore continua a supportare RV nelle eventuali azioni correttive e nei controlli successivi richiesti per mantenere la certificazione.

Si specifica che comunque, come indicato al par. 9.6, il Fornitore nell'erogazione dei propri servizi presso RV dovrà rispettare procedure, processi e strumenti indicati dalle normative e certificazioni di riferimento per RV.

5.3.4 Supporto per compliance normativa NIS2

RV desidera valutare la propria compliance alla direttiva Europea NIS 2, identificando eventuali scostamenti rispetto a quanto richiesto da suddetta normativa e intraprendendo quindi un percorso volto ad assicurare la completa aderenza dei propri sistemi alla NIS2.

A titolo esemplificativo e non esaustivo, si prevede che il Fornitore monitori i seguenti aspetti, in accordo con la Direttiva NIS2:

- Implementare politiche di sicurezza (inclusa redazione e aggiornamento di documentazione e processi) adeguate a prevenire e mitigare i rischi informatici;
- Assicurarsi che i fornitori operanti presso la supply chain di RV rispettino standard di sicurezza elevati, includendo requisiti specifici nei contratti;
- Mantenere registrazioni dettagliate delle attività di rete e dei sistemi informativi, riesaminandole regolarmente per individuare anomalie;
- Sviluppare procedure per la rilevazione, la segnalazione e la risposta efficace agli incidenti di sicurezza informatica;
- Predisporre piani per garantire l'operatività aziendale anche in situazioni di emergenza.

Di seguito si riportano, a titolo esemplificativo e non esaustivo, le principali aree di intervento che dovranno essere valutate e per le quali dovranno essere eventualmente proposti piani di intervento:

- Gestione del rischio;
- Incident Management;
- Continuità operativa;
- Sicurezza della catena di approvvigionamento;
- Formazione del personale.

Di seguito si riportano le principali attività richieste al Fornitore al fine di perseguire l'obiettivo di cui sopra, complete dei deliverable richiesti per ogni fase e con l'indicazione dei contenuti minimi per ogni deliverable:

1. **Assessment della compliance alla direttiva europea NIS 2:** questa attività si compone di diverse sotto attività legate alla pura attività di "Assessment", volte a raccogliere tutti gli elementi caratterizzanti l'organizzazione attuale, identificando eventuali criticità e punti di attenzione legati alla infrastruttura tecnica IT, ovvero gli scostamenti rispetto a quanto previsto dalla normativa.

Contenuti minimi deliverable:

- Analisi dettagliata dell'organizzazione attuale, incluse le infrastrutture tecniche IT, i processi organizzativi e le policy di sicurezza esistenti;
- Identificazione delle criticità e dei punti di attenzione rispetto ai requisiti della direttiva NIS 2;
- Impatti potenziali delle non conformità (tecnici, organizzativi, normativi);
- Elenco degli scostamenti riscontrati rispetto alla normativa, con una classificazione in base alla gravità e all'urgenza.

2. **Definizione degli interventi volti ad assicurare l'aderenza alla normativa:** l'attività prevede l'individuazione delle azioni correttive e delle misure tecniche, organizzative e procedurali necessarie per colmare gli scostamenti identificati durante l'assessment. Tali interventi includono, a titolo esemplificativo e non esaustivo:
    - Revisione delle policy di sicurezza informatica;
    - Proposta di adozione di strumenti tecnologici conformi ai requisiti della direttiva NIS 2;
    - Formazione del personale su eventuali nuovi standard e/o procedure aggiornate.

Contenuti minimi deliverable:

- Elenco dettagliato delle azioni correttive proposte per colmare gli scostamenti identificati;

- Indicazione delle priorità per ciascun intervento;
- Descrizione delle misure tecniche (es. implementazione di nuovi strumenti), organizzative (es. revisione delle policy), e procedurali (es. aggiornamento delle procedure operative);
- Indicazioni sulla necessità di formazione del personale e sui contenuti dei programmi formativi;
- Elenco delle attività formative previste (moduli, durata, destinatari);
- Obiettivi formativi specifici legati alla compliance NIS 2.

3. **Definizione del piano di azione e roadmap:** facendo riferimento agli interventi identificati, si prevede di procedere alla definizione di un piano di azione strutturato, articolato in una roadmap dettagliata che includa le priorità, le tempistiche e le risorse necessarie per l'attuazione degli interventi. La roadmap deve considerare sia le urgenze normative che gli obiettivi strategici aziendali, includendo milestone di verifica e revisioni periodiche. Ogni azione deve essere accompagnata da un piano di monitoraggio per valutarne l'efficacia e l'allineamento agli obiettivi, prevedendo eventualmente modifiche correttive in caso di variazioni di contesto o requisiti.

Contenuti minimi deliverable:

- Elenco delle azioni necessarie con descrizione dettagliata;
- Priorità assegnate alle azioni in base alla gravità delle non conformità e alle esigenze strategiche;
- Risorse umane, finanziarie e tecnologiche richieste per ciascuna azione;
- Modalità di monitoraggio per ogni azione (es. metriche di valutazione, KPI);
- Cronoprogramma delle attività, suddiviso in fasi e milestone chiave;
- Indicazione delle tempistiche e delle dipendenze tra le attività;
- Milestone per la verifica intermedia e finale dei risultati.

5.3.5 Supporto per compliance Legge 90/2024

In misura complementare con quanto previsto al paragrafo precedente per il supporto alla compliance NIS2, è richiesto un supporto per la compliance alla legge 90/2024 per Regione del Veneto (e non per altri enti regionali), ovvero a titolo esemplificativo e non esaustivo:

- Supporto alla definizione e adozione di misure e procedure per l'informazione verso ACN in caso di incidenti informativi;
- Supporto alle attività e compiti previsti per la struttura interna di cybersicurezza;
- Stesura e aggiornamento della documentazione prevista;
- Aggiornamento e presidio degli standard, linee guida e raccomandazioni emanati dal Centro nazionale di crittografia presso l'ACN.

5.3.6 Supporto qualificazione e relativi adeguamenti infrastrutture critiche rilevanti per la sicurezza nazionale

Regione del Veneto ha, inoltre, concluso un percorso con AgID per essere identificata come Polo Strategico Nazionale che prevede siano soddisfatti, tra gli altri, determinati requisiti di sicurezza per poter dare il via alla relativa procedura di qualificazione ed essere inseriti tra le «infrastrutture critiche» rilevanti per la sicurezza nazionale. La Regione ha acquistato le infrastrutture per la gestione del Data Center e la strategia evolutiva è indirizzata verso l'adozione del cloud privato per tutta la Regione.

Per garantire la conformità ai requisiti stabiliti, si prevede che il Fornitore supporti RV nelle attività propedeutiche al raggiungimento dell'obiettivo; di seguito si riportano le attività minime per le quali si richiede supporto:

- Assistenza nell'adozione delle misure tecniche e organizzative delineate nel "Manuale Tecnico sulle Misure di Sicurezza" del PSN, il quale descrive i trattamenti, le responsabilità e le misure adottate per garantire la riservatezza, l'integrità e la disponibilità dei dati;
- Garantire che le infrastrutture digitali e i servizi cloud siano conformi al Regolamento dell'Agenzia per la Cybersicurezza Nazionale (ACN), che definisce, a titolo esemplificativo e non esaustivo: capacità elaborativa, le misure e i requisiti per raggiungere i livelli minimi di sicurezza, …;
- Supporto tecnico nella migrazione dei dati e dei servizi verso l'infrastruttura del PSN, garantendo che il processo avvenga senza criticità e che siano rispettate la totalità delle modalità operative previste, come il "lift and shift";
- Offrire programmi di formazione per il personale tecnico di RV, in ottica di garantire una buona gestione delle nuove infrastrutture e dei servizi cloud adottati;
- Definire e, a valle dell'approvazione da parte di RV, implementare procedure per il monitoraggio costante delle infrastrutture e dei servizi, in linea con le best practice di Business Continuity e Disaster Recovery nazionali ed internazionali.

5.3.7 Servizi di supporto - Interventi fuori orario

Il servizio di intervento fuori orario comprende le attività di conduzione operativa on-site e/o di supporto specialistico svolte al di fuori del normale orario di lavoro, nei casi in cui RV richieda il prolungamento dell'orario di presidio per attività straordinarie programmate relativamente al Data Center primario (o relativamente ai servizi cloud di RVE non siti presso il DC), o interventi straordinari fuori orario on site sul sito di DR di Padova.

5.4 Servizi di gestione operativa

I servizi di gestione operativa/servizi infrastrutturali e sicurezza di cui RV intende avvalersi nella presente procedura aperta e di seguito descritti sono:

- Service Desk (SPOC);
- Servizio di Gestione delle Postazioni di Lavoro;

5.4.1 Service Desk (SPOC)

Le attività di system management devono essere strutturate in base ai processi di Service Management, pertanto, sulla base delle procedure adottate dall'Amministrazione e condivise con il Fornitore ad avvio contratto, il Fornitore deve adottare una modalità operativa che consenta di gestire incidenti e richieste degli utenti e fornire un'interfaccia per gli altri processi, quali Change, Problem, Configuration, Release, ecc., gestendo tutto il ciclo di vita dell'incident o della service request.

Il servizio di Service Desk, richiesto nella presente procedura aperta, si configura come punto di contatto (SPOC) per le richieste degli utenti interni di RV ed esterni (ad esempio cittadini fruitori dei servizi legati alla tematica dei Bandi e delle applicazioni quali MyPay, Imprese, Comuni, Enti convergenti ecc).

Si prevede di istituire uno SPOC con due numerazioni differenti:

- Numerazione servizi interni;
- Numerazione Enti convergenti, responsabile di fornire assistenza di primo livello, strutturando un sistema di contatti dedicati per garantire un supporto tempestivo ed efficace agli Enti collaboratori, coordinando le attività con il CERT per affrontare eventuali problematiche o incidenti.

I canali di contatto previsti per il servizio sono:

- Canale telefonico con numero verde dedicato. Il Fornitore deve dotarsi, senza oneri aggiuntivi per RV, di una linea telefonica in uscita da utilizzarsi nei casi in cui sia necessario contattare gli utenti;
- Un indirizzo e-mail dedicato;

- Chatbot;
- Portale web;
- Eventuali altre integrazioni (ad es. via API) con altre piattaforme.

RV ad avvio fornitura condivide con il Fornitore:

- L'elenco degli utenti VIP le cui richieste, a differenza di quelle degli utenti di tipo standard, devono essere trattate in via prioritaria;
- Le regole di catalogazione e assegnazione delle priorità dei ticket e i processi di interazione con i livelli del modello organizzativo. Al Fornitore è richiesto di consolidare le regole per iscritto e manutenere la documentazione in caso di variazioni.
- La modalità operativa da adottare in caso di quesiti di tipo amministrativo/legislativo per i quali sia necessario il coinvolgimento di personale interno atto a fornire la specifica risposta.

5.4.1.1 Modalità operativa di assistenza all'utenza di RV

La modalità operativa di assistenza all'utenza di RV è articolata secondo il seguente modello organizzativo:

- **Livello 1:** riceve ed acquisisce tutte le tipologie di richieste. Gli operatori di 1° livello svolgono attività informative e di supporto all'uso quotidiano dei servizi e delle applicazioni, eseguono le attività di prima analisi, categorizzazione, eventuale interazione con l'utente per reperire tutte le informazioni utili alla risoluzione della richiesta e/o smistamento mediante il corretto indirizzamento al secondo livello, ove non possibile la soluzione al 1° livello. La maggior parte dei ticket in carico al 1° livello prevede una risposta di tipo standard e/o predefinita.
- **Livello 2:** è rappresentato dai gruppi di esperti con maggiori competenze e conoscenze rispetto al 1° livello, per la diagnosi e risoluzione delle richieste. Il 2° livello è composto dalle risorse professionali dedicate ai Servizi previsti nella presente procedura aperta, oltre alle risorse appartenenti alla fornitura dei Servizi Applicativi e di rete. Il 2° livello viene attivato:
  - su segnalazione da parte del servizio di assistenza di 1° livello mediante il sistema di TT, qualora quest'ultimo non sia competente per la risoluzione della problematica segnalata;
  - dall'Amministrazione;
  - mediante apertura direttamente di un ticket al secondo livello.

  Gli operatori del 2° livello accedono al sistema di TT, per la visualizzazione delle richieste appartenenti all'ambito di propria pertinenza. Il 2° livello è responsabile della chiusura all'utente (Risoluzione) dei ticket di sua competenza ed è suddiviso nei seguenti gruppi:
  - 2° Livello Applicativo;
  - 2° livello Reti;
  - Supporto amministrativo di RV (personale specificamente identificato ad avvio fornitura);
  - 2° Livello per le Postazioni di Lavoro;
  - 2° Livello Sistemi (trouble ticketing) relativamente alle problematiche dei:
    - ✔ Servizi Base;
    - ✔ Servizi Accessori;
- **Livello 3:** è rappresentato da:
  - I soggetti di terze parti responsabili dei contratti di manutenzione HW in garanzia e SW di base per Sistemi, apparati TLC, Rete, Postazioni di lavoro, non inclusi nella presente procedura aperta e che provvedono alla riparazione di sistemi/componenti difettosi;

- Il Servizio di Manutenzione Correttiva delle applicazioni e il servizio di Gestione Applicativa che esegue interventi ad hoc sulle Basi Dati.

è attivato dai seguenti gruppi del 2° livello:

- 2° Livello per le Postazioni di Lavoro,
- 2° livello applicativo.

Il Fornitore deve utilizzare il sistema di Trouble Ticketing (TT) adottato da RV, fortemente integrato con altri sistemi; pertanto, le richieste di assistenza pervenute via mail, numero del call center, chatbot e eventuali altri canali, dovranno sempre essere censite nel sistema di TT, che sarà anche fonte per l'elaborazione delle statistiche sia per la valutazione dei livelli di servizio sia per la rendicontazione.

Il fornitore dovrà porre particolare attenzione alla gestione univoca (ovvero tramite 1 solo TT) di eventuali richieste gestite in più contatti, gestendo quindi la riapertura di eventuali TT già gestiti, ma per i quali l'utente riscontrasse difformità sul completamento della gestione

L'ambito per il quale il Service Desk di 1° livello fornisce supporto agli utenti, è costituito dalle tematiche inerenti:

- Segnalazioni relative ai servizi gestiti nella presente procedura aperta;
- Registrazioni relative ai servizi previsti nella procedura aperta "Servizi Applicativi", ossia interventi di MEV (manutenzione evolutiva), MAC (manutenzione correttiva), MAD (manutenzione adeguativa), PP (parametrizzazioni e personalizzazioni), GA (gestione applicativa), NEW (nuovi sviluppi), assegnategli dai diversi referenti di RV;
- Supporto all'uso delle funzionalità degli applicativi;
- Risposte all'utenza esterna su specifiche tematiche (Bandi);
- Segnalazioni relative a problemi di rete.

L'attività del Service Desk è volta a supportare gli utenti mediante attività di presa in carico delle segnalazioni, categorizzazione, assegnazione della priorità e soluzione della problematica, ove possibile, oppure instradando gli Incident e le Service Request ad uno dei 2° livelli specialistici, composti da figure professionali di tematica quando la soluzione della segnalazione non è possibile al 1° livello.

Al Service Desk è richiesto di tracciare, mediante l'apertura di ticket sul sistema di Trouble Ticketing (TT), qualsiasi richiesta pervenutagli attraverso i canali di contatto quali mail e telefonate.

La richiesta di assistenza pervenuta al Service Desk deve essere gestita e tracciata durante tutto il ciclo di vita, registrando anche i passaggi tra i tre livelli del servizio.

Per ridurre al minimo il pending discusso in altra sede, verrà introdotto un'attività di sollecito dei ticket sospesi, finalizzato a garantire un follow-up tempestivo delle richieste in attesa di risoluzione e a migliorare i tempi complessivi di gestione del servizio di supporto.

L'apertura dei ticket sul sistema avviene anche a seguito di incident rilevati dalle attività di monitoraggio, da instradare ai gruppi competenti per la risoluzione.

Al Fornitore è richiesto di erogare il servizio tramite il proprio il Centro Servizi, attivando, sin dall'avvio della fornitura, una VPN di collegamento ai sistemi di RV, mediante la quale gli operatori di 1° livello possano accedere in sola visualizzazione a tutti gli applicativi oggetto di supporto.

Al fine di garantire la qualità e l'efficienza del servizio, è richiesta la stabilità degli operatori del Service Desk, come definito in Appendice 1 Indicatori di Qualità. Gli operatori devono essere adeguatamente e costantemente formati sui nuovi applicativi e sugli aggiornamenti degli applicativi informatici inclusi nel perimetro del servizio, oltre che sulle tematiche previste nella presente procedura aperta attraverso la schedulazione periodica di incontri di formazione anche in relazione alle date di pubblicazione dei Bandi RV. L'assenza per qualsiasi motivo di personale specifico lato Fornitore non deve in alcun modo interferire con l'attività di gestione delle richieste, pertanto, dev'essere garantita l'intercambiabilità delle risorse, assicurando che ciascuna risorsa sia in grado di operare con competenze equivalenti e

conformi ai requisiti richiesti per l'attività.

Il servizio di assistenza di 1° livello deve garantire la gestione dei picchi di attività, ad esempio in concomitanza di rilasci di interventi particolarmente impattanti per l'utenza o a seguito della pubblicazione dei Bandi di RV. La pianificazione di tale gestione deve essere condivisa con RV almeno 4 giorni lavorativi prima degli eventi di picco previsti o comunque preventivamente concordato con RV.

La flessibilità nell'organizzazione del Fornitore deve essere garantita anche nei casi in cui RV, con adeguato anticipo di 4 giorni lavorativi o comunque preventivamente concordato con RV, richiede attività lavorative fuori dall'orario base esteso definito per il servizio di Service Desk (SPOC). Verrà attivata, in questo caso, anche la modalità di remunerazione extra-orario.

I contatti telefonici da Servizi Interni o Servizi del PSR possono avvenire, in orario esteso o in reperibilità Continuativa dalle 20 alle 08, solo esclusivamente attraverso il servizio SPOC.

La chiusura del ticket nei confronti dell'utente (Risoluzione) viene effettuata dal livello che ha in carico la segnalazione, anche se il ticket viene sempre reso visibile al 1° livello che, in qualità di SPOC deve sempre essere aggiornato sulle risoluzioni delle problematiche. La chiusura viene effettuata sul sistema di TT che registra sia la soluzione adottata, ai fini dell'aggiornamento della knowledge base, sia la risposta inviata automaticamente all'utente richiedente. Dopo 3 giorni dalla Risoluzione e in assenza di ulteriori segnalazioni da parte dell'utente, relative alla eventuale persistenza del problema, il sistema di TT effettua automaticamente la chiusura definitiva (Chiusura).

Reperibilità SPOC

Il servizio di reperibilità telefonica, erogato da personale del Service Desk al di fuori dell'orario base esteso, è attivo per garantire l'intervento del personale del Fornitore preposto del servizio di monitoraggio, in caso di problematiche non tempestivamente intercettate dai sistemi di monitoraggio stesso. Ciò al fine di contribuire a garantire la disponibilità dei servizi all'utenza per le applicazioni di tipo mission critical, elencate in Appendice 3 Contesto Tecnologico e Applicativo.

5.4.1.2 Strumenti a supporto del Trouble Ticketing

Nei paragrafi successivi si riportano gli strumenti previsti nel perimetro del servizio di Trouble Ticketing, ovvero:

- Portale Web
- SysAid
- Chatbot

Portale Web

Al Fornitore è richiesto di mettere a disposizione un Portale web che abbia almeno le seguenti componenti:

- **Repository FAQ** per fornire supporto agli utenti su tematiche ricorrenti;
- **Chatbot** integrato con il repository FAQ per rispondere automaticamente alle richieste degli utenti (si veda descrizione dettagliata di seguito);
- **Knowledge Database**, ad uso interno, contenente informazioni dettagliate, procedure operative, documentazione tecnica e linee guida utili al personale interno per la gestione efficiente dei processi;
- **Dashboard interna**, che fungerà da cruscotto di monitoraggio delle attività legate al Service Desk, fornendo indicatori chiave di performance (KPI) relativi alla gestione delle richieste di assistenza, all'efficienza della chatbot, ai tempi di risposta e alla classificazione delle problematiche più frequenti. La Dashboard dovrà essere arricchita con un sistema di alert che, in base a soglie convenute, segnala le situazioni a rischio. A partire da tali evidenze, comunque dovranno essere messe a punto azioni di prevenzione o contenimento da sottoporre alla Regione per una pronta risposta.

Al Fornitore è richiesto di organizzare e mantenere aggiornato un repository di FAQ da pubblicare a supporto

dell'utenza, che devono essere sempre approvate nei contenuti da RV prima della pubblicazione, il quale dovrà fungere da base dati per il chatbot.

Si prevede che il sistema integri un'interfaccia utente intuitiva dotata di intelligenza artificiale (IA) per migliorare l'accessibilità e l'efficacia delle informazioni, organizzando le FAQ in categorie e sottocategorie logiche, facilitando la ricerca e la navigazione da parte degli utenti, implementando un sistema di tagging e parole chiave che consenta sia al chatbot che agli utenti di individuare rapidamente le informazioni pertinenti.

In termini di metodologie di alimentazione del repository, dovranno essere garantiti aggiornamenti regolari, stabilendo procedure condivise con RV per l'aggiornamento continuo delle FAQ, assicurando che il chatbot disponga di informazioni sempre attuali. Inoltre, si prevede l'implementazione di un workflow di approvazione per le nuove voci o modifiche, garantendo l'accuratezza e la qualità delle informazioni.

Particolare attenzione è posta ai requisiti di accessibilità e usabilità: il repository FAQ, il portale web e il chatbot devono essere conformi ad almeno uno standard/linee guida di accessibilità e usabilità degli strumenti informatici, quali a titolo esemplificativo e non esaustivo:

- Web Content Accessibility Guidelines 2.0 (WCAG)/ ISO/IEC 40500:2012.
- EN 301 549;
- Linee Guida sull'accessibilità degli strumenti informatici emanate dall'AgID;
- Standard Regionali.

Infine, per garantire uno strumento costantemente in linea con le specificità e gli standard di RV, si richiede la raccolta di feedback dagli utenti sulle risposte ricevute, utilizzando queste informazioni per migliorare continuamente il repository, oltre all'analisi delle interazioni, monitorando le stesse per identificare aree di miglioramento e aggiornare le FAQ, la knowledge database e l'intero repository proattivamente da parte del Fornitore.

SysAid

SysAid è il sistema di Trouble Ticketing (TT) attualmente adottato in RV, caratterizzato da un elevato grado di integrazione con i processi aziendale. Qualora la piattaforma ITSM venisse sostituita su iniziativa del Fornitore, le licenze saranno a carico del Fornitore stesso e l'analisi e la progettazione sono incluse negli adempimenti del contratto e tale attività non dovrà avere alcun onere aggiuntivo per RVE e non dovranno essere svolte dai Team di presidio (Team servizio di conduzione operativa dei sistemi e sicurezza, Team servizio PdL). Qualora invece RV, una volta valutata la proposta ITSM, decidesse invece di confermare l'utilizzo della piattaforma, il fornitore sarà chiamato a potenziare lo strumento attraverso l'implementazione di funzionalità avanzate. In particolare, l'evoluzione dovrà concentrarsi sullo sviluppo di capacità che consentano un monitoraggio completo del ciclo di vita dei ticket, offrire strumenti per monitorare l'intero ciclo di vita dei ticket, garantendo che ogni fase sia documentata e facilmente accessibile ed che sia esportabile un tracciato di log delle variazioni, con particolare attenzione alla gestione del primo livello (SPOC)

IN alternativa qualora la piattaforma venisse sostituita su iniziativa di RV con una terza soluzione, il canone di licenze sarà adeguato come indicato al cap 7.

In un'ottica di gestione ottimale del ciclo di vita dei ticket e considerando l'evoluzione prevista con chatbot e portali a supporto del TT, è essenziale mantenere correlati i ticket censiti, pertanto eventuali solleciti ricevuti, sia tramite email che tramite il portale web, non si dovranno censire dei nuovi ticket ma essere tracciati con ticket aggiuntivi ma presentarsi all'utente come un unico ticket (padre), garantendo così una visione coerente e centralizzata delle richieste di assistenza. Durante il periodo contrattuale, qualora vi fosse un cambio del modello di licensing del prodotto in questione, il fornitore dovrà adattarsi al nuovo modello prevedendo un'analisi approfondita di come si intenda cambiare il modello adattando le quantità in modo da soddisfare comunque le necessità dell'Amministrazione assicurando che tale transizione avvenga senza alcun onere economico e operativo per l'Amministrazione.

Chatbot

Il Fornitore è tenuto a mettere a disposizione degli utenti di RV, senza costi aggiuntivi entro 6 mesi dalla data di ’avvio dei servizi successiva al periodo di subentro/presa in carico, un Chatbot dedicato al supporto degli utenti nella risoluzione di problematiche, con particolare focus sull’HD di I° livello, fortemente integrato con la Knowledge base ed il repository delle FAQ e caratterizzato dall’utilizzo dell’IA.

Questo strumento deve garantire risposte rapide e accurate, migliorando significativamente l'esperienza dell'utente e ottimizzando le operazioni di supporto. Di seguito viene fornita una descrizione dettagliata delle specifiche richieste per l’implementazione del chatbot, con la possibilità di integrare ulteriori funzionalità di valore aggiunto.

Il punto di ingresso per l’interazione utente-chatbot deve essere costituito da un'interfaccia dedicata e intuitiva, accessibile tramite diverse piattaforme come siti web aziendali, applicazioni mobili o strumenti di messaggistica istantanea. Questa interfaccia deve essere progettata per favorire un’interazione fluida e immediata, consentendo agli utenti di avviare conversazioni in modo naturale e senza barriere tecniche.

A supporto dell’esperienza conversazionale, il chatbot deve integrare algoritmi avanzati di Large Language Model (LLM), capaci di interpretare con precisione il linguaggio naturale utilizzato dagli utenti. Questi algoritmi devono essere in grado di estrarre l'intento della richiesta e analizzare il contesto specifico, anche in presenza di varianti linguistiche, ambiguità o espressioni colloquiali. L'obiettivo è garantire una comprensione profonda delle esigenze dell'utente per fornire risposte personalizzate e pertinenti.

Tramite l’integrazione con la knowledge base ed il repository delle FAQ, una volta compreso l'intento dell'utente, il chatbot effettua una ricerca all'interno della knowledge base e delle FAQ aziendali per individuare le informazioni più pertinenti e aggiornate relative alla richiesta, fornendo un feedback all’utenza utile alla risoluzione del problema o richiesta di informazioni. Tale feedback viene presentata all'utente attraverso l'interfaccia di chat, fornendo le informazioni richieste o indicando i passaggi necessari per la risoluzione della problematica.

Nel caso in cui la richiesta dell'utente risultasse non gestibile (assenza di riscontro nella knowledge base o nelle FAQ, richiesta estremamente complessa etc) e dopo aver posto domande aggiuntive all'utente per chiarire la richiesta e tentare una nuova ricerca nelle risorse disponibili, il chat può trasferire la conversazione a un operatore qualificato per una gestione più approfondita.

Al fine di garantire uno strumento efficace ed efficiente, si prevede l’integrazione del chatbot con meccanismi di machine learning e AI che gli permettono di:

- identificare nuove informazioni o soluzioni emerse durante le interazioni e aggiornare la knowledge base di conseguenza;
- analizzare le conversazioni passate per identificare aree di miglioramento nella comprensione e nella risposta alle richieste degli utenti.
- innescare un alert a fronte dell’apertura di un numero considerevole di ticket riguardo richieste di assistenza sulla stessa tematica.

Infine, al termine dell'interazione, si prevede che il chatbot richieda un feedback all'utente sulla qualità del supporto fornito, utilizzando queste informazioni per ulteriori miglioramenti del servizio.

Si prevede che al termine della fornitura, il Chatbot, ovvero tutto quello che viene configurato/realizzato per l’erogazione del servizio, rimanga di proprietà di RV.

5.4.2 Servizio Gestione Postazioni di Lavoro

Il servizio di gestione delle Postazioni di Lavoro (PDL) comprende le attività necessarie alla gestione dei PC, sia desktop che Notebook di RV e delle relative periferiche associate con attività di IMAC, inventario e aggiornamento degli asset, HD di 2° livello per gli interventi on site sulle PDL, manutenzione HW fuori garanzia e rapporto con Fornitore terzi per HW in garanzia, gestione dei dispositivi per le Videoconferenze e attività ad esse connesse, gestione della logistica e magazzino e servizi di gestione vari, come meglio esplicitato nei paragrafi successivi.

5.4.2.1 Caratteristiche generali del servizio

Nell’ambito della presente procedura aperta per PDL si intende l’insieme dei PC desktop e notebook a cui sono associate sia le relative periferiche, da catalogate in SysAid, quali video, docking cuffie, webcam, lettori usb, scanner,

speaker, storage esterni, sia gli elementi HW correlati come tastiere, mouse, printer da tavolo, plotter, proiettori o monitor o lavagne tv, o altri elementi come specificato nell'Appendice 3 Contesto Tecnologico e Applicativo.

Gli utenti serviti si distinguono tra VIP e STANDARD, per i quali sono previsti differenti tempi di evasione delle richieste e relativi SLA.

Per il dettaglio completo delle PDL, della distribuzione presso le sedi e la tipologia di utente servito si rimanda a quanto descritto in Appendice 3 Contesto Tecnologico e Applicativo.

È previsto l'utilizzo di un ambiente preposto per il preassemblaggio/configurazione del PdL il cui responsabile è il direttore della Direzione ICT, Agenda Digitale e SOS affidamento servizi e forniture ict, U.O. Sistemi informativi, servizi e tecnologie digitali.

Qualora, durante la vigenza del contratto, il Fornitore venga a conoscenza dell'imminente cessazione del supporto da parte del Produttore del sistema operativo relativo ad una o più PDL oggetto del servizio di gestione, è fatto obbligo al Fornitore di comunicare tempestivamente all'Amministrazione, documentando opportunamente (ossia dalla documentazione prodotta dovranno evincersi sia i prodotti sia la data in cui cesserà ufficialmente il supporto degli stessi da parte del produttore, oltre a qualsiasi altra informazione utile), la data in cui cesserà ufficialmente il suddetto supporto.

Gli interventi di IMAC vengono attivati mediante ticket aperti al 1° livello del Service Desk.

Tutte le apparecchiature e i relativi dispositivi accessori oggetto degli interventi di IMAC e di manutenzione HW devono essere sottoposti a collaudo, con firma del modulo di esito positivo da parte dell'utente destinatario della postazione e/o responsabile della stessa. In caso di esito negativo del collaudo il Fornitore deve, qualora non fosse possibile procedere alla riparazione contestuale del malfunzionamento, concordare con i Referenti RV la data di ripianificazione dell'intervento.

Il modulo di collaudo deve contenere almeno le seguenti informazioni:

- Luogo di intervento (provincia, edificio, stanza, …);
- Tipologia di PDL installata;
- Utente a cui è stata installata;
- Data di avvio e chiusura delle attività;
- Personale del Fornitore e Referente di RV;
- Esito del collaudo.

Si evidenzia che sono presenti dotazione residuali, che verranno censite al massimo entro la fine del periodo di affiancamento iniziale e per le quali si richiede al Fornitore di svolgere le seguenti attività:

- Provvedere al collegamento alla nuova PDL, come indicato al § 5.4.2.3 (Installazione di una PDL);
- Dismissione e Smaltimento come indicato al § 5.4.2.3 (Remove di una PDL)

Durante la presa in carico e l'attività di assessment degli asset verrà definito il numero preciso di asset dove è richiesto al Fornitore il servizio di gestione e manutenzione. La quantità indicata non potrà eccedere del 10% per ogni categoria, per il dettaglio si veda la tabella al cap. 4 Contesto tecnologico delle postazioni di lavoro di regione veneto nell'appendice 3 Contesto tecnologico e applicativo.

Il servizio di gestione delle postazioni di lavoro e degli asset collegati si compone delle seguenti macro- attività:

- Inventario periodico degli asset;
- IMAC;
- Manutenzione hardware PDL;
- Gestione logistica e magazzino;
- Gestione Desktop/Notebook da remoto;

- Gestione degli apparati per le Videoconferenze
- Altre attività di gestione.

5.4.2.2 Inventario periodico degli asset

L'attività di gestione dell'inventario degli asset ha l'obiettivo di rendere disponibile e mantenere aggiornata, durante tutta la durata della fornitura, una base informativa completa e dettagliata del parco macchine in servizio presso l'Amministrazione e gestite dal Fornitore. Tali informazioni devono evidenziare sia gli aspetti logistici e amministrativi, che quelli di configurazione hardware e software.

Il Fornitore deve effettuare un censimento iniziale di tutte le risorse da gestire nell'ambito del servizio, presenti nelle sedi dell'Amministrazione indicate in Appendice 3 Contesto Tecnologico e Applicativo, oltre che il censimento delle giacenze delle apparecchiature e degli altri beni materiali eventualmente presenti nel magazzino. Il censimento deve essere completato al massimo entro la fine del periodo di affiancamento iniziale, e l'esito deve essere consegnato secondo un formato concordato con l'Amministrazione.

L'inventario degli Asset gestiti (per tutte le sedi di RV) deve essere mantenuto aggiornato, a fronte degli interventi dei Servizi IMAC e Manutenzione e, in ogni caso, ripetuto almeno 1 volta ogni sei mesi.

Le informazioni sul ciclo di vita degli asset costituiscono la base per le attività di analisi sui dispositivi installati, per far in modo che sia possibile pianificare azioni e progetti di intervento e/o miglioramento degli apparati dell'Amministrazione.

Gli asset sono attualmente gestiti nel CMDB in uso presso RV (descritto nell'Appendice 3 Contesto Tecnologico e Applicativo).

È prevista la produzione di report riportante almeno le seguenti informazioni:

- Situazione degli asset gestiti con diversi livelli di aggregazione;
- Movimentazione degli asset, a vari livelli di aggregazione;
- Giacenze di magazzino.

Si richiede che il censimento per l'inventario delle PDL e dei software relativi venga effettuato tramite un'integrazione diretta con uno strumento di asset management, per garantire un monitoraggio automatico e continuo dell'inventario. Si prevede quindi di effettuare la raccolta e l'aggiornamento in tempo reale di informazioni su hardware, software e configurazioni, tramite agenti installati sulle postazioni di lavoro eliminando la necessità di interventi manuali e migliorando l'affidabilità del censimento.

Infine, si prevede di integrare il censimento con un sistema di gestione del ciclo di vita delle risorse (Lifecycle Management), che tracci le modifiche alle PDL e pianifichi attività di aggiornamento o sostituzione

Ad avvio della fornitura saranno concordati con l'Amministrazione i dettagli della reportistica e la frequenza di produzione.

5.4.2.3 IMAC

Le richieste di IMAC possono essere di due tipi:

- **Singola**: intervento IMAC relativo ad un singolo utente o singola PDL;
- **Massiva**: interventi IMAC afferenti a una pluralità di utenti o PDL di una o più sedi dell'Amministrazione indicate in Appendice 3 Contesto Tecnologico e Applicativo.

In caso di interventi massivi le attività di IMAC devono essere organizzate mediante la predisposizione del Piano di lavoro. Il Piano, il cui contenuto è oggetto di condivisione tra RV e Fornitore al momento della richiesta da parte di RV, deve, a titolo esemplificativo, trattare le seguenti informazioni essenziali:

- Cicli di consegna se previsti;
- Numero e tipologia di PDL oggetto del roll out per ciclo di consegna;
- Luogo di intervento;

- Tempi di avvio e conclusione del ciclo;
- Tempi di ritiro delle apparecchiature dismesse;
- Personale del Fornitore coinvolto;
- Procedure, documentate formalmente, da adottare per la cancellazione dei dati sulle postazioni da dismettere.

Tutte le attività di IMAC devono obbligatoriamente prevedere l'aggiornamento puntuale del sistema Asset Management.

Le attività del servizio IMAC, indicate a titolo esemplificativo e non esaustivo, sono:

Installazione nuova PDL

- Consegna dell'apparecchiatura all'utente finale;
- Assemblaggio dei singoli componenti;
- Sistemazione delle apparecchiature sugli appositi arredi;
- Collegamento dei singoli componenti alla rete elettrica e alla rete dati conformemente alle norme di sicurezza vigenti (D.Lgs. 9 aprile 2008, n. 81 e ss.mm.ii.);
- Configurazione in rete locale e geografica, utilizzando gli indirizzi IP e gli indirizzi di posta elettronica rilasciati dall'Amministrazione;
- Ripristino, secondo le procedure concordate con l'Amministrazione, di eventuali componenti software non standard e/o di archivi;
- In caso di installazione per sostituzione di una postazione, salvataggio e ripristino secondo le procedure definite dall'Amministrazione dei dati contenuti nella postazione di lavoro sostituita; Test di funzionalità e verifica del ripristino dei dati per l'accettazione dell'apparecchiatura da parte dell'utente o del responsabile della stessa secondo le procedure definite dall'Amministrazione;
- Test di funzionalità per l'accettazione dell'apparecchiatura da parte dell'utente o del referente dell'Amministrazione stessa;
- Recupero degli imballaggi e loro smaltimento secondo norme vigenti e trasporto dell'imballaggio a carico del Fornitore;
- Ove necessario, configurazione della stampante di rete, coordinandosi con il Fornitore del servizio di gestione delle stamparti di rete;
- L'attività di installazione, principalmente nel caso di nuova installazione, deve essere preceduta da quella di "site preparation", a carico dell'Amministrazione, che comprende varie azioni tra cui, per esempio, la corretta predisposizione dell'impianto rete e di quello elettrico;
- Se l'installazione avviene in sostituzione di una PdL preesistente, l'attività è preceduta dalla disinstallazione della stessa. La disinstallazione è a carico del Fornitore.

Remove - Disinstallazione di una PDL

- Cancellazione dei dati dall'apparecchiatura disinstallata attraverso l'uso di opportuni strumenti in grado di garantire la sicurezza dell'operazione e la privacy dei dati utente;
- Disattivazione delle funzionalità del sistema disinstallato con eventuale disconnessione dalla rete conformemente alle norme di sicurezza vigenti (D.Lgs. 9 aprile 2008, n.81 e ss.mm.ii.);
- Disassemblaggio dell'apparecchiatura disinstallata;
- Raccolta ordinata dei cavi delle apparecchiature disinstallate e posizionamento degli stessi all'interno dell'unità da trasferire al magazzino del Fornitore;
- Predisposizione al trasporto (compreso imballaggio) e ritiro delle apparecchiature disinstallate.

Move- Movimentazione PDL

A seguito di modifiche logistiche dell'utente (trasferimenti di sede/di stanza/di piano/ecc.), la movimentazione include almeno le seguenti attività:

- Disinstallazione dell'apparecchiatura e dei dispositivi aggiuntivi;
- Predisposizione al trasporto (compreso imballaggio) delle apparecchiature disinstallate;
- Trasporto delle apparecchiature da e per le sedi di movimentazione (incluso il magazzino);
- Installazione dell'apparecchiatura e dei dispositivi aggiuntivi e riconfigurazione secondo i parametri relativi alla nuova locazione;
- Test di funzionalità e verifica del ripristino dei dati per l'accettazione dell'apparecchiatura da parte dell'utente o del responsabile della stessa secondo le procedure definite dall'Amministrazione.

Add - Aggiunta ad una Pdl

L'intervento consiste nelle seguenti attività:

- Hardware – installazione di un nuovo dispositivo esterno (come hard disk, stampante, scanner, ecc.) ed il relativo driver appropriato su una postazione già operativa;
- Software – installazione di prodotti software su una postazione già operativa, inclusiva della personalizzazione di base secondo quanto previsto dalle procedure e dalle policy dell'Amministrazione.

L'attività prevede in entrambi i casi l'esecuzione di test di installazione per verificare il funzionamento delle componenti aggiunte, eventualmente sulla base di procedure fornite dall'Amministrazione.

Change - Modifica postazione di lavoro.

La modifica include almeno le seguenti attività:

- Installazione e configurazione di dispositivi aggiuntivi e del relativo software;
- Test di funzionalità e verifica dell'eventuale ripristino dei dati per l'accettazione dell'apparecchiatura da parte dell'utente o del responsabile della stessa secondo le procedure definite dall'Amministrazione;
- Installazione di upgrade hardware.

Di seguito RV condivide al Fornitore una stima dei volumi annui attesi di richieste IMAC:

- installazioni nuove: indicativamente 900 (incluso rollout);
- spostamenti (move): indicativamente 400;
- aggiunte di componenti (add): Indicativamente 300 per Hardware e 700 per il software.

5.4.2.4 Manutenzione hardware PDL

Su tutte le PDL oggetto del servizio, deve essere garantito il servizio di manutenzione HW, per il ripristino delle macchine in condizioni di efficienza a seguito di guasti o malfunzionamenti. Durante l'intero periodo contrattuale il Fornitore deve, pertanto, assicurare, senza oneri aggiuntivi per RV, la riparazione delle apparecchiature informatiche mal funzionanti e l'eventuale sostituzione dei componenti danneggiati.

Le attività richieste al Fornitore si differenziano in manutenzione:

- **Preventiva:** che consiste nell'effettuare controlli preventivi previsti dai produttori delle apparecchiature nelle loro specifiche tecniche. Tale attività può prevedere controlli e/o sostituzioni di componenti degli apparati, con modalità da concordare con i Referenti RV;
- **Correttiva:** che consiste nell'effettuare interventi di riparazione dei guasti e delle disfunzioni che dovessero verificarsi. La modalità di intervento si differenzia tra asset in garanzia e fuori.

Per gli **asset fuori garanzia**, l'eventuale sostituzione di parti di ricambio e/o di dispositivi accessori deve essere effettuata con parti/dispositivi/prodotti originali, al fine di rispettare le condizioni contrattuali e i LDS previsti. Più precisamente:

- è in carico a RV l'acquisto di nuovi asset in caso non sia possibile provvedere alla riparazione (PC desktop e/o notebook, scanner, plotter e altri beni accessori) e la fornitura del muletto in sostituzione;
- è in carico al Fornitore l'acquisto delle parti di ricambio degli asset oggetto del servizio. Nel caso di malfunzionamenti causati dall'impiego di componenti incompatibili con i sistemi in dotazione, il Fornitore è tenuto, a propria cura e spese, alla sostituzione e al ritiro delle componenti difettose.

Per gli **asset in garanzia**, il Fornitore è tenuto a gestire il rapporto con terzi, assumendosi la responsabilità di attivare la garanzia, previa interfaccia con il Referente di RV. Il Fornitore deve inoltre supportare i terzi nelle attività di loro competenza, facilitando il buon esito e garantendo la tempestività nella risoluzione degli interventi. Qualora necessario, il Fornitore dovrà intraprendere campagne di sollecito nei confronti dei terzi per assicurare il rispetto delle tempistiche e la corretta esecuzione degli interventi. In tale ipotesi, valgono i livelli di servizio contrattualizzati con i terzi, senza responsabilità del Fornitore. Alla scadenza dei singoli periodi di garanzia, le apparecchiature saranno prese completamente in carico dal Fornitore che ne effettuerà la manutenzione diretta.

In entrambi i casi (asset in garanzia e non), qualora non sia possibile ripristinare la piena operatività delle apparecchiature informatiche presso la postazione dell'utente, deve essere garantita la disinstallazione, l'imballaggio, il ritiro ed il trasporto delle apparecchiature in questione, a cura e spese del Fornitore. Inoltre, deve essere assicurata la sostituzione temporanea di quanto danneggiato con apparecchiature informatiche perfettamente funzionanti e con le medesime caratteristiche hardware e/o le funzionalità del Sistema Operativo presenti in quelle sostituite.

5.4.2.5 Gestione Desktop/Notebook da remoto

In caso di intervento da remoto su PdL Desktop/Notebook, l'Amministrazione si riserva di autorizzare il Fornitore ad effettuare l'intervento di diagnosi dei malfunzionamenti, prendendo visione dell'operatività della PdL, tramite il prodotto di assistenza remota messo a disposizione dall'Amministrazione stessa, indicato nell'Appendice 3 Contesto Tecnologico e Applicativo e comunque comunicato ad avvio fornitura e solo previa esplicita autorizzazione dell'utente, che deve essere presente durante la sessione di intervento (ad es. maschera di conferma da cliccare) e secondo le regole stabilite dall'Amministrazione.

Attualmente, la soluzione di assistenza remota adottata funziona esclusivamente all'interno della rete regionale, escludendo la possibilità di collegarsi a utenti in telelavoro o comunque fuori sede (smart working). Per garantire un supporto più efficace, il software di accesso remoto messo a disposizione da RV dovrà essere integrato con il sistema di Ticketing Tool (TT) o con il canale di comunicazione instaurato (il Fornitore ha la possibilità di utilizzare, a proprio onere, tool di gestione del canale comunicativo per gli utenti che lavorano in smart working). Inoltre, l'accesso dovrà essere di tipo presidiato, ovvero autorizzato dall'utente prima di ogni intervento.

A tutela del Service Desk e della sicurezza dell'Amministrazione, il sistema di assistenza remota dovrà garantire l'anonimato dell'operatore del call center lato utente, pur consentendo la registrazione delle attività eseguite.

In tal caso, in fase di avvio, RV identifica:

- Utenti abilitati all'utilizzo del prodotto in questione;
- Apparecchiature per le quali le attività possono essere effettuate con le modalità stabilite;
- Policy di accesso.

L'Amministrazione si riserva di modificare, nel corso della durata contrattuale, le regole di utilizzo di tale tipologia di interventi o di inibire gli interventi in questione, ove necessario, per esigenze di sicurezza dell'Amministrazione stessa.

5.4.2.6 Gestione dispositivi personali

Per garantire una gestione efficace della sicurezza dei dispositivi personali utilizzati per scopi lavorativi si prevede una stretta collaborazione tra il team impiegato nel servizio di Gestione delle Postazioni di Lavoro (PDL) ed il team di Sicurezza; con particolare riferimento al coinvolgimento di quest'ultimo nell'attività di predisposizione e diffusione di politiche dedicate ed attuazione delle stesse tramite attività di analisi monitoraggio dei dispositivi personali, quali a titolo esemplificativo e non esaustivo:

- Personal Computer;
- Tablet;

- Chiavette o Storage USB;
- hard disk esterni.

Si prevede quindi che il fornitore definisca e, a valle dell'approvazione di RV, implementi una politica BYOD (Bring Your Own Device) stabilendo le condizioni e le modalità con cui i dispositivi personali possono essere utilizzati per scopi lavorativi. Questa politica deve almeno delineare i controlli necessari, le responsabilità degli utenti e le misure di sicurezza da adottare, garantendo la protezione dei dati aziendali e la conformità alle normative vigenti e dovrà essere basata sulle best practice a livello internazionale.

Pertanto, il fornitore è tenuto ad effettuare un'analisi approfondita in merito alla sicurezza del device, secondo quanto stabilito all'interno della politica BYOD approvata, includendo l'identificazione di potenziali minacce come accessi non autorizzati, infezioni da malware e violazioni dei dati.

Sulla base di questa analisi, devono essere implementate misure tecniche e organizzative adeguate, come, a titolo esemplificativo e non esaustivo:

- crittografia dei dati;
- autenticazione a più fattori;
- uso di reti private virtuali (VPN);
- soluzioni Mobile Device Management (MDM).

Risulta essenziale quindi che il fornitore presidi il processo end-to-end, non limitandosi all'individuazione delle criticità ma, senza oneri aggiuntivi per RV, il fornitore è tenuto a presentare ed implementare le relative soluzioni per permetterne l'utilizzo, fornendo una chiara indicazione di almeno i seguenti aspetti: attività svolte, eventuali criticità riscontrate, distinzione tra rischi e minacce potenziali, eventuale grado di impatto, eventuali soluzioni per mettere in sicurezza il dispositivo e permetterne l'utilizzo, riscontro in merito all'applicazione delle soluzioni.

Il Fornitore è inoltre tenuto a svolgere un'attività di monitoraggio e aggiornamento continuo delle politiche BYOD, in considerazione della continua evoluzione dell'ambiente tecnologico e le relative minacce alla sicurezza, è fondamentale che l'Ufficio PDL e l'Ufficio Sicurezza collaborino per monitorare costantemente l'efficacia delle misure adottate e aggiornare le politiche e le procedure in base alle nuove esigenze e alle migliori pratiche emergenti.

Infine, si prevede che il fornitore svolga attività dirette alla formazione dei dipendenti sulla politica BYOD implementata.

5.4.2.7 Altre attività di gestione

Rientrano in questa categoria tutte le attività di gestione delle richieste avanzate dagli utenti, comprendendo, a titolo esemplificativo ma non esaustivo:

- Gestione delle utenze per la firma digitale, incluse impostazione e configurazione.
- Distribuzione e installazione on-site di materiali di consumo per le apparecchiature gestite dall'Amministrazione (es. personal computer portatili, accessori, ecc.).
- Verifica dei collegamenti e gestione delle videoconferenze attraverso i sistemi messi a disposizione dall'Amministrazione (Google Meet, Lifesize, Cisco WebEx, Microsoft Teams, ecc.).
- Gestione dei Terminalini di Presenza, le attività comprendono:
    - Verifica della raggiungibilità dei dispositivi;
    - Attività di messa in linea;
    - Sostituzione di apparati difettosi, ove necessario.
- Verifica di fattibilità per l'installazione fisica di nuovi asset (per gli asset gestiti dagli Affari Generali della Regione del Veneto, è richiesta l'autorizzazione preventiva degli enti competenti).

- Cablaggio degli asset e gestione delle connessioni di rete.
- Gestione delle verifiche di raggiungibilità degli apparati.
- Attività di posa e messa in linea, previa autorizzazione del Servizio Sedi.
- Eventuale rimozione e sostituzione di apparati difettosi.
- Configurazione hardware e software di tutte le componenti assegnate.
- Spostamento degli asset e delle loro componenti, ove necessario e/o richiesto.
- Collaudo e verifica finale delle attività svolte, con accettazione formale da parte della Regione del Veneto.
- Servizio di staging per PdL richieste in comodato d'uso, comprendente:
    - Formattazione e predisposizione delle postazioni di lavoro (PdL) prima della consegna agli utenti, anche nel caso di asset non soggetti a manutenzione;
    - Organizzazione della logistica interna per la gestione e la consegna degli apparati a Regione del Veneto, che provvederà alle pratiche amministrative.

  Sarà responsabile il Fornitore della preparazione/staging delle PdL nei rollout pianificati.
- Gestione e smaltimento sicuro dei supporti elettronici in caso di guasti o dismissione, in conformità alle normative vigenti (§ 9.6.2). Su richiesta della Regione del Veneto, il Fornitore dovrà:
    - Prelevare il supporto da smaltire;
    - Compilare una scheda di registrazione con le seguenti informazioni: tipo di supporto, numero di inventario, nominativo e firma di chi effettua il prelievo, firma del referente della Regione del Veneto;
    - Provvedere alla distruzione e allo smaltimento del supporto senza ulteriori oneri per l'Amministrazione. I dispositivi interessati includono, a titolo esemplificativo: hard disk (HDD/SSD), chiavette USB, memorie RAM, batterie per laptop, ecc.

5.4.2.8 Gestione logistica e magazzino

Al fine di adempiere alle attività di gestione delle attività di stoccaggio e movimentazione delle PDL come hardware afferenti ai Data Center si prevede che il fornitore gestisca due magazzini separati, come di seguito esplicitato. Si sottolinea che il numero massimo di PC e dispositivi hardware che possono essere fisicamente presenti presso le sedi di RV sarà concordato successivamente con il responsabile designato.

Magazzino per lo stoccaggio e le attività correlate:

Il Fornitore è tenuto a disporre di un proprio magazzino idoneo allo stoccaggio dei beni acquistati prima della consegna presso le sedi di RV. Tale magazzino deve essere organizzato per accogliere le PDL - ad oggi è stimata una capacità presso il magazzino del fornitore di un numero massimo di 900 PdL (pc e monitor per un totale di 1800 colli mentre per i componenti data center non è previsto lo stoccaggio presso il magazzino del fornitore) oltre a rack, server e altri dispositivi afferenti i DC, acquistati per conto di RV (o comunque da Enti o altri soggetti in convenzione presso il PSR di RV), in considerazione della necessità di garantire una corretta gestione degli spazi presso le sedi di RV. A tal fine, si prevede che il Fornitore si doti di locali idonei, provvisti di assicurazione e di tutte le misure necessarie per garantire un servizio efficiente e conforme agli accordi contrattuali, oltre ad implementare procedure per ridurre i rischi di danneggiamento, furto o smarrimento.

Il Fornitore deve farsi carico della gestione fisica dei beni presenti in magazzino, incluse le attività di trasporto e consegna dalle proprie strutture alle sedi di RV. È inoltre responsabile delle operazioni di disimballaggio, etichettatura e distribuzione del materiale previsto per le attività, nonché della gestione e dello smaltimento degli imballaggi.

La gestione del magazzino deve prevedere il censimento e la catalogazione dei beni presenti, con aggiornamenti costanti da rendere disponibili in caso di movimentazioni, ripetuti almeno una volta l'anno o su specifica richiesta di RV, utilizzando il sistema di Asset Management. Il Fornitore è inoltre tenuto a segnalare a RV il raggiungimento della soglia di riordino, definita preventivamente all'avvio del contratto.

Gestione del magazzino situato in Via Colombara a Mestre

Per il magazzino situato in Via Colombara a Mestre (ha una disponibilità di spazio per lo stoccaggio fino a 150 m^3), il Fornitore è responsabile della movimentazione degli apparati hardware, non limitandosi alle PDL ma, come per il punto precedente, includendo rack, server e altri dispositivi afferenti i DC. La richiesta copre tutte le attività di movimentazione tra sedi aziendali, all'interno delle stesse sedi, e verso/da il magazzino di Mestre. Inoltre, il Fornitore deve gestire l'intero processo logistico, dalla fase di ritiro degli apparati fino alla consegna all'utilizzatore finale, comprensive di operazioni di disimballaggio ed etichettatura. È inclusa anche la gestione dello smaltimento di hardware obsoleti o non più funzionanti, da effettuare nel rispetto delle normative ambientali e di sicurezza vigenti.

Si prevede inoltre che il Fornitore predisponga e fornisca imballaggi appropriati per il trasporto degli apparati, garantendo che questi siano adeguati a proteggere i dispositivi durante la movimentazione. Deve assicurare la sicurezza fisica e funzionale del magazzino, implementando procedure per ridurre i rischi di danneggiamento, furto o smarrimento. A tal riguardo, RV si riserva il diritto di effettuare audit di sicurezza per verificare la conformità delle soluzioni adottate.

In termini di garanzie, il Fornitore deve fornire adeguate fideiussioni finanziarie, le cui specifiche saranno definite in seguito.

Infine, la gestione del magazzino deve includere il censimento e la catalogazione costante dei beni, con aggiornamenti disponibili in caso di movimentazioni, ripetuti almeno una volta l'anno o su richiesta di RV, utilizzando il sistema di Asset Management. Anche in questo contesto, il Fornitore deve segnalare la soglia di riordino, stabilita all'inizio del contratto in accordo con RV.

5.4.3 Servizio Gestione Postazioni di Lavoro - Gestione Videoconferenze

Fatte salvo le specifiche operative per la gestione delle PdL indicate nei precedenti paragrafi, di seguito si riportano in modo sintetico e non esaustivo le attività connesse alla specifica gestione delle sale di Videoconferenze. Per il dettaglio sugli aspetti tecnici e l'ubicazione si rimanda all'Appendice 3 – Contesto Tecnologico.

Inoltre, si ribadisce che, devono essere mantenute le licenze per le videoconferenze e previsto un presidio fisso per la gestione operativa, il cui dettaglio sarà inserito nella tabella delle figure "Gestione PdL".

Il servizio e le licenze ambito del presente appalto saranno avviati a giugno 2027.

Responsabilità della figura da eseguire "da remoto":

- Circa 40-45 videoconferenze mensili programmate con calendario condiviso.
- Assistenza per l'attivazione e supporto durante la videoconferenza.
- Attivazione della registrazione e predisposizione del link per l'acquisizione.
- Acquisizione dell'elenco partecipanti, sia per lo streaming che per una riunione normale.
- Assistenza per l'utilizzo degli apparati e risoluzione di eventuali malfunzionamenti.
- A richiesta, moderazione della riunione.

In caso di nuove installazioni

- Consulenza operativa sulle tecnologie impiegate per le videoconferenze (VDC).
- Contestualizzazione da parte degli uffici competenti per la regolarità amministrativa.
- Movimentazione dell'apparato e prima configurazione funzionale.
- Verifica di fattibilità per l'installazione fisica (per gli asset gestiti dagli Affari Generali della Regione del Veneto, si richiede l'autorizzazione preventiva degli enti competenti).
- Cablaggio dell'asset.

- Gestione attraverso verifiche di raggiungibilità.
- Attività di posa e messa in linea, previa autorizzazione del Servizio Sedi.
- Eventuale rimozione e sostituzione di apparati difettosi.

5.5 Servizi di sicurezza aggiuntivi rispetto alla conduzione

RV intende avvalersi nella presente procedura aperta anche per l'approvvigionamento dei servizi di seguito descritti:

- Servizio di Continuos Vulnerability Assessment dell'Infrastruttura;
- Servizio di Verifica delle Vulnerabilità delle Applicazioni WEB
- Servizio di Threat Intelligence;
- SOC Security Operation Center;

5.5.1 Servizio di Continuous Vulnerability Assessment dell'Infrastruttura

Il Fornitore deve erogare un servizio di Vulnerability Assessment finalizzato a raccogliere le informazioni utili a verificare lo stato di sicurezza dell'infrastruttura IT di Regione Veneto e del PSR, allo scopo di identificare le eventuali vulnerabilità a cui sono esposti i servizi oggetto di analisi. Sono oggetto del monitoraggio sia i server che gli apparati di rete e di sicurezza (presso i DC di RVE già specificati e presso, comunque, i servizi CLOUD attivi o che saranno attivati). Gli eventuali accessi VPN forniti per eseguire le attività di Vulnerability Assessment infrastrutturali verranno configurati in modo tale da avere piena raggiungibilità per tutti i IP target di test.

Le scansioni dell'Infrastruttura devono essere eseguite in modalità continuativa anche al fine di adempiere ai vincoli indicati da ACN in merito all'adeguamento dei servizi cloud al livello 2.

Le scansioni VA devono coprire sia gli ambienti containerizzati sia sistemi fisici e virtuali tradizionali.

Nell'ambito del servizio, in presenza di IP interni all'infrastruttura, verrà fornito un accesso remoto (VPN).

All'occorrenza potranno essere richieste delle scansioni al di fuori della normale pianificazione. Il servizio ha lo scopo di accertare i seguenti aspetti:

- Vulnerabilità delle componenti software standard installate sugli apparati e sui server, con particolare riguardo alle vulnerabilità del sistema Operativo, dei Software di Middleware, dei DBMS e dei Firmware;
- Vulnerabilità delle componenti di sicurezza software installate sugli apparati e sui server;
- Vulnerabilità delle configurazioni di hardening che possono risultare incomplete o non corrette;
- Vulnerabilità dei livelli di protezione attivi, protocolli attivi, strumenti di protezione installati e attivi.

L'ambito iniziale di esecuzione è definito in Appendice 3 Contesto Tecnologico e Applicativo e potrà essere aggiornato ad inizio fornitura. In fase di avvio il Fornitore deve effettuare la classificazione degli asset in base al livello di rischio, e proporre all'Amministrazione la profilazione di rischio per l'eventuale prioritizzazione degli interventi legati alle vulnerabilità riscontrate durante l'esecuzione.

Il Fornitore deve:

- Effettuare le scansioni e i test periodici, in modalità continuativa, utili alla rilevazione delle vulnerabilità;
- Verificare i risultati delle scansioni e assegnare le priorità di intervento in base alla severità dei rischi di sicurezza rilevati, in accordo con le politiche di sicurezza dell'Amministrazione;
- Redigere e consegnare al gruppo di Conduzione Operativa e ai referenti di RV il report di vulnerability assessment;
- Il report deve contenere almeno le seguenti informazioni per ogni singolo server / apparato oggetto del servizio:

- Informazioni sullo storico delle scansioni eseguite;
- Vulnerabilità rilevate e relativo dettaglio:
- Classificazione della criticità delle Vulnerabilità;
- Classificazione delle vulnerabilità per tipologia, Porta e Protocollo;
- Identificativo delle Vulnerabilità ove disponibile secondo gli standard CVVS (Common Vulnerability Scoring System) e CVE (Common Vulnerabilities and Exposures);
- Risultati della scansione accompagnati dal Piano di rientro dalle vulnerabilità identificate;
- Proporre soluzioni di limitazione e controllo del rischio per vulnerabilità.

Ad inizio contratto, il Fornitore deve fornire una prima Relazione dettagliata sullo 'stato di salute' dei sistemi di RV presi in carico, evidenziando eventuali criticità e/o debolezze riscontrate sulla base di Penetration Test, Vulnerability Assessment e ulteriori test che ritiene opportuno. La relazione deve essere corredata da un remediation plan, con l'indicazione delle contromisure necessarie per eliminare le problematiche e le vulnerabilità eventualmente rilevate.

5.5.2 Servizio di Verifica delle Vulnerabilità delle Applicazioni WEB

Il Fornitore dovrà rendere disponibile un servizio di verifica e analisi dinamica delle vulnerabilità di sicurezza delle applicazioni WEB gestite da Regione del Veneto, sia per le applicazioni raggiungibili da rete pubblica che per quelle raggiungibili solo da rete interna (anche tramite mobile app). Il servizio ha la finalità di individuare ed evidenziare i seguenti aspetti critici di sicurezza

- Vulnerabilità legate alla Configurazione delle WEB Application con particolare riguardo alle directory e alle pagine web esposte all'accesso pubblico;
- Vulnerabilità legate ai meccanismi di Autenticazione che possano esporre le applicazioni ad accessi non autorizzati;
- Vulnerabilità legate ai meccanismi di Autorizzazione e Profilazione che potrebbero consentire ad utenti non autorizzati di ampliare i propri privilegi di utilizzo delle applicazioni;
- Vulnerabilità legate alla validazione e visualizzazione dei dati che potrebbero consentire di effettuare attività di code injection o che rendano accessibili informazioni non strettamente connesse al profilo autorizzativo dell'utente loggato.

Nell'ambito delle applicazioni non esposte su internet e quindi raggiungibili soltanto dall'interno dell'infrastruttura, verrà predisposto un accesso remoto (VPN).

A titolo di esempio si riportano di seguito alcune tipologie di vulnerabilità che devono essere oggetto di verifica:

- Accesso abusivo a funzionalità aggiuntive;
- Gestione non controllata degli input;
- Cross-Site Scripting;
- Cross-Site Request Forgery;
- Format String;
- Integer Overflows;
- LDAP Injection;
- Mail Command Injection;
- Null Byte Injection;
- Path Traversal;
- Remote File Inclusion;

- SSI Injection;
- SQL Injection;
- XPath Injection;
- XML Attribute Blowup;
- XML Bombing;
- XML External Entities;
- XML Injection;
- XQuery Injection.

Il servizio deve essere erogato dal Centro Servizi del Fornitore in modalità As a Service. Ove necessario, è consentita l'installazione presso i Data Center della Regione Veneto, delle componenti da utilizzare per la verifica delle applicazioni raggiungibili solo da rete intranet.

I costi di licenza, la manutenzione e i costi di subscription annuali delle piattaforme software utilizzate per l'erogazione del Servizio sono inclusi nei costi del servizio così come i costi di connettività che dovessero rendersi necessari per la verifica delle applicazioni su rete Intranet.

Le applicazioni WEB oggetto del servizio (si veda par. 7.5 Misurazione dei Servizi infrastrutturali e sicurezza nella tabella "Verifica Vulnerabilità delle applicazioni Web) dovranno essere sottoposte a scansione, al fine di poter individuare lo stato di sicurezza e lo stato di esposizione alle vulnerabilità. Alla singola applicazione potrà essere associato più di un Fully Qualified Domain Name (FQDN) Pubblico o Privato.

Previa condivisione col fornitore, RV si riserva la possibilità di richiedere scansioni specifiche al di fuori del dominio di intervento concordato.

Il Fornitore dovrà provvedere ad effettuare le seguenti attività:

- verificare i risultati delle scansioni collezionando le segnalazioni riscontrate;
- produrre la reportistica di sintesi e di dettaglio relativa alle scansioni effettuate;
- classificare le segnalazioni in base a priorità/severità dei rischi di sicurezza secondo quanto stabilito dalle policy dell'Amministrazione;
- suggerire il piano di intervento necessario ad eliminare le eventuali criticità;
- provvedere alle remediation in caso di criticità afferenti al perimetro in sua gestione.

Dovrà essere reso disponibile all'Amministrazione l'accesso alla console di management della piattaforma tecnologica utilizzata per il servizio.

Su base mensile, il Fornitore dovrà rendere disponibili dei report di riepilogo contenenti almeno le seguenti informazioni:

- Dettaglio delle scansioni effettuate nel periodo di riferimento;
- Confronto con le scansioni precedenti sulla stessa applicazione, al fine di monitorare eventuali miglioramenti o peggioramenti dello stato di sicurezza.
- Vulnerabilità rilevate e relativo dettaglio:
    - Classificazione della criticità delle Vulnerabilità rilevate;
    - Classificazione delle vulnerabilità per tipologia, Porta e Protocollo;
    - Identificativo delle Vulnerabilità ove disponibile secondo gli standard CVVS (Common Vulnerability Scoring System) e CVE (Common Vulnerabilities and Exposures, CVE;
    - Descrizione generale per la potenziale risoluzione della Vulnerabilità.

5.5.3 Servizio di Cyber Threat Intelligence (CTI)

Il Fornitore dovrà rendere disponibile un servizio di Cyber Threat Intelligence (inclusivo di tecnologia e prodotti sw necessari) adeguatamente strutturato per coprire tutti gli IP, i domini, gli indirizzi VIP e le applicazioni mobile afferenti al perimetro di Regione del Veneto, garantendo un monitoraggio efficace e continuo delle potenziali minacce. Il servizio dovrà essere funzionale a prevenire e mitigare attacchi informatici, potenziali o in corso, nei confronti dell'Amministrazione, al fine di limitare gli impatti sulle infrastrutture tecnologiche di rete e IT dell'Ente.

In particolare, il servizio dovrà assicurare la protezione sia degli ambienti Multicloud (GCP e PSN, AWS, Azure o eventuali altri che saranno attivati nel corso del contratto) sia degli ambienti On-Premise. Inoltre, dovrà essere dinamico e aggiornabile in base a mutate esigenze o all'inserimento di nuovi contesti operativi, garantendo così un adattamento costante all'evoluzione delle minacce e del perimetro tecnologico regionale.

Il servizio dovrebbe prevedere almeno le seguenti componenti:

- Early warning;
- Cyber Intelligence;
- Data Leakage;
- Data breach;
- VIP Protection;
- Fake App Monitoring.

I servizi di intelligence si devono basare su metodologia OSINT (OPEN Source Intelligence) che prevedono la verifica continuativa tramite fonti aperte di nuove vulnerabilità e/o di nuovi vettori di attacco che possano essere sfruttati per penetrare l'infrastruttura IT di RV.

Il servizio di Cyber Threat Intelligence, mediante il servizio di Early Warning dovrà permette di individuare le nuove vulnerabilità da fonti ufficiali, e preventivamente eventuali nuove vulnerabilità, di fatto non ancora ufficializzate, provenienti da fonti non ufficiali.

La componente di servizio di "Early Warning" ha i seguenti obiettivi:

- individuare preventivamente nuove vulnerabilità tramite fonti non ufficiali;
- raccogliere informazioni al fine di individuare i seguenti elementi:
    - presenza di operatori malevoli sulla rete ed identificazione delle potenziali finalità di attacco;
    - esecuzione di azioni malevoli in rete verso obiettivi simili a quelli dell'Amministrazione;
    - rilevazione preventiva di specifici "elementi" tecnologici malevoli (es: software, firmware), non ancora classificati, che possono potenzialmente sfruttare le vulnerabilità relative al contesto tecnologico dell'amministrazione.

La componente di servizio di "data breach monitoring", attraverso il monitoraggio delle reti internet (incluso dark e deep web), ha lo scopo di individuare:

- attività finalizzate a trattare in modo illecito o fraudolento il patrimonio informativo (dati / informazioni) gestito dalle infrastrutture IT dell'Amministrazione;
- attività di commercializzazione divulgazione e pubblicazione del patrimonio informativo gestito dall'Amministrazione.

Il servizio, erogato dal Fornitore presso il Centro Servizi, ha carattere continuativo e deve prevedere:

- Controllo continuo in tempo reale di fonti aperte alla ricerca di "elementi" di interesse per la sicurezza della Regione del Veneto citati o individuati all'interno di determinate aree della rete. A titolo di esempio si riportano alcuni elementi che sono tipicamente oggetto del monitoraggio:
    - Dati personali di operatori dell'Amministrazione (Specifiche identità o username);

- indirizzi di posta elettronica;
- documenti legati all'Amministrazione;
- informazioni collegate a specifiche applicazioni web o mobile;
- elenchi di IP Pubblici attestati sulle applicazioni dell'Amministrazione;
- Servername;
- web domains;
- e-mail domains;
- brand.

- Generazione di segnalazioni o allarmi, secondo una classificazione di rilevanza, sulla base dei risultati oggettivi derivanti dall'analisi delle informazioni provenienti dalle diverse fonti aperte;
- Produzione di reportistica.

L'ambito delle ricerche sarà concordato con il Fornitore secondo le necessità di RV. A titolo di esempio si riporta la lista degli elementi che potranno essere oggetto dei singoli interventi di Threat Intelligence:

- Applicazione/Progetto;
- Tipologia di servizio (servizio di "Early Warning" o data "Breach monitoring");
- Selezione delle fonti;
- Configurazione Domini e indirizzi IP;
- Configurazione Operatori ("Key People");
- Configurazione indirizzi posta elettronica;
- Nomi dei servizi esposti su rete pubblica o privata dall'amministrazione;
- Nomi di amministrazioni e/o enti controllati;
- Termini/frasi di specifico interesse.

Gli indirizzi IP potranno essere sia di tipo pubblico, raggiungibili da rete Internet, sia di tipo privato, raggiungibili esclusivamente dalla rete interna.

La Regione del Veneto fornirà l'elenco iniziale di VIP, domini e app da monitorare. Nel corso del contratto, potranno incorrere eventuali variazioni sia come conseguenza di input di Regione del Veneto sia su proposta del Fornitore.

Il Fornitore deve rendere disponibile i seguenti report al fine di rendicontare gli elementi di sintesi e di dettaglio dello stato di esecuzione del servizio.

- Executive Summary su base bimestrale: Report in formato digitale con dettagli di alto livello destinato all'amministrazione condiviso tramite portale della fornitura.
- Techhnical Report su base almeno mensile: Report con dettagli specifici degli eventi più rilevanti e le azioni mitiganti rilevate, destinato al personale operativo responsabile delle azioni di mitigation e resolution.
- Instant Report real time: destinato al personale ed al management dell'amministrazione con dettagli relativi alla segnalazione specifica relativa alla criticità rilevata.
- weekly bulletin: un bollettino che fornisce una panoramica sul mondo cyber sulla settimana passata.

Nel caso in cui vengano individuate possibili minacce, dovrà essere reso disponibile, nel minor tempo possibile, un report di incident che contenga almeno le seguenti informazioni:

- Ricerca (Threat Analysis) oggetto dell'Incident;
- Tipologia di dominio e di servizio impattato (servizio di "Early Warning" o data "Breach monitoring");

- Severità della minaccia rilevata;
- Timestamp relativa alla rilevazione;
- Lista e descrizione dettagliata degli “elementi” e delle informazioni raccolte;
- Sintesi e dettaglio dei risultati ottenuti dalle analisi effettuate;
- indicazioni di azioni suggerite o raccomandazioni da mettere in atto.

5.5.4 SOC - Security Operation Center

Regione Veneto ha deciso di attuare un modello di coordinamento e di servizio basato sui principi di risposta agli incidenti informatici integrando un HyperSOC (Security Operation Center) che possa monitorare la sicurezza informatica e gestire gli incidenti a livello regionale. Le nuove tecnologie dell’informazione e delle comunicazioni hanno progressivamente focalizzato le attività in ambito Cyber Security, ciò ha comportato un parallelo incremento delle vulnerabilità. La digitalizzazione dei servizi e delle informazioni ha inevitabilmente accresciuto l’esposizione al rischio: il pericolo di furto, manomissione e compromissione dei dati nello spazio cibernetico ha evidenziato la necessità di mettere in sicurezza le attività.

Il modello adottato da Regione Veneto ha l’obiettivo di potenziare la resilienza cyber dei sistemi informativi per garantire la messa in sicurezza dei dati e dei servizi dei cittadini ed è il punto di raccordo tra le pubbliche amministrazioni locali di riferimento, oltre ad eventuali altri Enti/Società che ne facciano richiesta.

La sicurezza informatica è diventata una priorità assoluta per proteggere dati sensibili, processi aziendali e la reputazione stessa delle organizzazioni. In questo scenario, il Security Operation Center, noto come SOC, aiuta a difendere le aziende da queste minacce digitali: identificare, prevenire e soprattutto mitigare in tempo reale le minacce.

Il compito principale del SOC è la sorveglianza costante dell’ambiente informatico aziendale. Il SOC monitora il flusso di dati, il traffico di rete, l’accesso ai sistemi e altre attività rilevanti. La sua missione è rilevare qualsiasi attività sospetta e rispondere prontamente per mitigare i rischi. In un mondo in cui i pericoli possono emergere da qualsiasi

Il SOC monitora attraverso differenti tecnologie il traffico di rete, gli accessi ai sistemi, le attività dei dispositivi, e molto altro ancora. Il suo obiettivo è rilevare in tempo reale qualsiasi attività sospetta o comportamenti che potrebbero indicare un potenziale attacco.

Il SOC è inoltre responsabile di analizzare le minacce e raccogliere informazioni cruciali che possono essere utilizzate per migliorare ulteriormente la sicurezza aziendale anche attraverso attività di Cyber Threat Intelligence (CTI). Le analisi post-incidente aiutano a comprendere come sono avvenuti gli attacchi e cosa può essere fatto per prevenirli in futuro.

Nel contesto di una conformità normativa sempre più rigorosa, il SOC gioca un ruolo importante nell’aiutare le aziende a rispettare le leggi e i regolamenti in materia di sicurezza informatica. Fornisce report dettagliati sulle attività di sicurezza, contribuendo a dimostrare la conformità con gli standard richiesti.

Al SOC sono collegati a una serie di strumenti e sistemi che rilevano attività sospette o segnali d’allarme nei vari componenti dell’infrastruttura aziendale. Questi includono sistemi di rilevamento delle intrusioni, strumenti di analisi del traffico di rete, sistemi di gestione delle minacce e molto altro. L’integrazione di queste tecnologie consente al SOC di avere una visione completa dell’ambiente informatico aziendale.

Servizi:

1. Analisi della sicurezza: Monitoraggio dei sistemi alla ricerca di attività sospette; indagare e intraprendere azioni correttive;
2. Implementazione e della gestione dei sistemi di sicurezza all’interno del SOC collaborando con le varie strutture IT. Assicurando che i che i sistemi siano configurati correttamente;
3. Threat intelligence: monitoraggio costante delle fonti di intelligence relative alle minacce (tattiche degli

aggressori e anche sugli Initial Access Broker (IaB);

4. Analisti degli incidenti: L'analisi delle violazioni (attraverso attività di Incident Response) e degli attacchi avvenuti per comprendere come sono avvenuti e come possono essere prevenuti in futuro;
5. Conformità verso requisiti normativi in materia di sicurezza informatica e di incidenti informatici e con report dettagliati alle autorità competenti quando necessario.

Il servizio SOC tramite l'utilizzo della soluzione SIEM proposta dal Fornitore nell'ambito del servizio (per il dimensionamento si faccia riferimento al cap 7) dovrà quindi anche:

- Gestire e automatizzare il processo di raccolta e orchestrazione dei log;
- Monitorare e gestire gli eventi e i dati raccolti analizzandoli e aggregandoli per identificare correlazioni;
- Evidenziare proattivamente eventi o comportamenti di interesse consentendo, ad esempio, di rilevare un accesso amministrativo al di fuori del normale orario di lavoro, quindi informazioni sull'host, sull'Id e altro ancora;
- Evidenziare preventivamente tramite logiche e algoritmi di ML e AI pattern di eventi che possano portare ad allarmi o eventi di sicurezza;
- Gestire e valutare falsi positivi / falsi allarmi e ridurne la numerosità.

Nell'ambito del servizio SOC richiesto, l'implementazione del sistema SIEM potrà avvenire a discrezione del fornitore con le seguenti modalità:

- installazione del sistema SIEM on-premise presso i data center della Regione del Veneto;
- installazione del sistema SIEM presso i data center del fornitore;
- installazione del sistema SIEM su infrastrutture di cloud privato.

Le tecniche utilizzate dai SOC per il monitoraggio e il rilevamento delle minacce, sono le seguenti:

Sistemi di Rilevamento delle Intrusioni (IDS/IPS)

I sistemi di rilevamento delle intrusioni (IDS) e i sistemi di prevenzione delle intrusioni (IPS) verificano minacce all'interno di un SOC. Gli IDS rilevano attività sospette o non autorizzate all'interno della rete aziendale, mentre gli IPS sono in grado di bloccare o mitigare immediatamente le intrusioni. Questi sistemi sono essenziali per identificare violazioni di sicurezza e attacchi informatici.

Analisi del Traffico di Rete

l'analisi del traffico di rete. Questo processo coinvolge la monitorizzazione costante del traffico dati all'interno della rete aziendale al fine di individuare pattern anomali o comportamenti sospetti. L'analisi del traffico di rete consente al SOC di individuare tentativi di attacco, attività di malware e altri comportamenti non autorizzate.

Sistemi di Cyber Threat Intelligence (CTI)

I sistemi di intelligence sulle minacce sono utilizzati per monitorare l'intero panorama delle minacce cibernetiche. Informazioni da fonti multiple, i feed di intelligence (white, gray e black). L'obiettivo è identificare in modo proattivo le minacce emergenti e le vulnerabilità che potrebbero essere sfruttate dagli aggressori. Vengono anche utilizzati sistemi passivi di analisi delle vulnerabilità con lo scopo di identificare in maniera precoce eventuali falle di sistema con lo scopo di mitigarle quanto prima.

Honeypots e Honeynets

Le honeypots e le honeynets sono utilizzate per attirare gli aggressori su sistemi creati ad arte per raccogliere informazioni sulle minacce. Le honeypots sono sistemi o risorse apparentemente vulnerabili ma in realtà progettate per catturare gli atti illeciti degli aggressori. Queste tecnologie consentono al SOC di studiare le tattiche dei criminali informatici e migliorare le proprie difese.

Monitoraggio degli Accessi e delle Credenziali

Il monitoraggio degli accessi e delle credenziali Questa attività implica la registrazione e l'analisi degli accessi ai sistemi

e alle risorse aziendali. Il SOC cerca di identificare comportamenti anomali, come tentativi di accesso non autorizzato o utilizzi non conforme delle credenziali.

Analisi delle Minacce

L'analisi delle minacce: indagare sulle minacce rilevate per comprendere la loro portata e il loro impatto potenziale. Il fornitore dovrà prendere in carico l'analisi delle mail (ordinarie e/o PEC) di potenziale phishing segnalate dagli utenti e l'attivazione delle opportune azioni di mitigazione del rischio secondo le best practice

Mitigazione delle Minacce

Le giuste misure per mitigare le minacce : esempio, se si tratta di un malware, il SOC potrebbe isolare un dispositivo infetto o spegnere addirittura una porzione di rete (come nel caso di un incidente ransomware) e quindi rimuovere il malware e ripristinare l'integrità del sistema. In caso di tentativi di accesso non autorizzato, potrebbe essere bloccato l'accesso ai sistemi del personale e potrebbero essere reimpostate le credenziali.

Report e Documentazione

Documentazione dettagliata di tutte le violazioni e delle relative azioni intraprese. Questa documentazione è preziosa per le indagini forensi, la conformità normativa e la revisione post-incidente. La precisione e *la completezza nella documentazione sono fondamentali per garantire la trasparenza e la capacità di rispondere a eventuali azioni legali.*

Prevenzione delle Violazioni Future

L'aggiornamento delle politiche di sicurezza, dei sistemi o l'implementazione di nuove misure di protezione.

gestione della comunicazione degli incidenti:

- **Rilevazione e Valutazione:** Il SOC rileva e valuta gli incidenti di sicurezza in modo tempestivo per determinare se un incidente rientra nell'ambito delle leggi sulla notifica.
- **Comunicazione alle Autorità:** Nel caso in cui un incidente rientri nelle categorie di notifica, comunicazione dell'incidente alle autorità preposte, rispettando i requisiti legali.

Tecniche di Protezione e Prevenzione

Per garantire la sicurezza informatica aziendale, il Security Operation Center (SOC) non si limita a monitorare, rilevare e rispondere alle minacce. È anche responsabile di mettere in atto misure di protezione e prevenzione per ridurre al minimo i rischi.

Patch Management, Hardening e Sviluppo Sicuro del Codice

Uno degli aspetti fondamentali per la protezione delle infrastrutture informatiche, sono *la terna magica di Patch Managemeng, Hardening e Sviluppo Sicuro del Codice*. Una mancata applicazione dei processi collegati, possono permettere ai criminali informatici di fare breccia all'interno di una infrastruttura ICT;

Firewall e Filtri Web

I firewall e i Next Generation Firewall (NGFW) sono strumenti chiave per il lavoro del SOC, per controllare e limitare il traffico di rete. Il SOC configura e gestisce questi dispositivi per impedire l'accesso a siti web dannosi o non autorizzati e per proteggere la rete aziendale da intrusioni non desiderate.;

Antivirus e Sicurezza degli Endpoint

I programmi antivirus e la sicurezza degli endpoint sono fondamentali per rilevare e bloccare malware e minacce informatiche. Questi strumenti monitorano costantemente i dispositivi endpoint, come computer e smartphone, per rilevare comportamenti sospetti o file dannosi;

Monitoraggio del Network e Analisi dei Log

I log sono essenziali per il lavoro del SOC sia per rilevare accessi abusivi ma anche in fase di incident response, per comprendere come è avvenuto in incidente informatico.

Gestione delle password e Multi Factor Authentication (MFA)

L'applicazione delle corrette politiche sulle password è fondamentale per una buona protezione dagli attacchi

informatici di una azienda, L'autenticazione "multi fattore" è una misura di sicurezza che richiede più di una forma di verifica dell'identità per accedere a un sistema.

Monitoraggio degli Accessi

Il monitoraggio costante degli accessi ai sistemi e alle risorse aziendali per rilevare attività sospette o tentativi di accesso non autorizzato.

Gestione delle Identità e degli Accessi (IAM)

La gestione delle identità e degli accessi per garantire che *solo le persone autorizzate possano accedere a determinate risorse aziendali.*

5.5.4.1 Servizio di Continuous Penetration Test

All'interno delle attività e servizi del SOC, il fornitore dovrà gestire l'attività di Continuous Penetration Test e il perimetro coprirà sia la Giunta Regionale sia il PSR. L'attività è basata sulla piattaforma Pentera (attualmente in possesso di Regione del Veneto), che permette di gestire in autonomia attività di Vulnerability Assessment e test automatizzati, con l'obiettivo di verificare e integrare la sicurezza dei propri sistemi. La soluzione Pentera, infatti, è in grado di analizzare in modo continuativo la superficie di attacco – interna o esterna – individuando e prioritizzando eventuali lacune di sicurezza, così da poter definire le misure più efficaci da intraprendere per rafforzare la propria infrastruttura e ridurre l'esposizione cyber. Relativamente alla prioritizzazione dei rischi, sarà a cura del fornitore definire un framework.

5.5.4.2 Servizio di Esercitazione Cybersecurity

Con l'obiettivo di potenziare la prontezza di Regione del Veneto contro le minacce informatiche, creando un ciclo virtuoso di valutazione e miglioramento continuo al fine di migliorare la sicurezza informatica dell'organizzazione, l'aggiudicatario dovrà pianificare, organizzare, realizzare ed eseguire almeno una esercitazione annuale, di tipo Blue Team e Red Team anche per testare le capacità di gestione delle minacce cyber.

Le esercitazioni dovranno essere condotte, per quanto riguarda il red team, da un soggetto e team di terza parte (ovvero non coinvolto nei servizi operativi erogati nella conduzione), con comprovata esperienza nel settore della cybersecurity, al fine di garantire una gestione trasparente e orientata ai risultati. Mentre per quanto riguarda il blue team l'aggiudicatario potrà avvalersi del team interno di conduzione eventualmente ed opportunamente integrato con figure professionali di supporto per la durata delle esercitazioni.

La scelta del soggetto e team proposto deve essere condivisa e concordata con RVE.

Le esercitazioni dovranno essere concepite come un'opportunità di apprendimento e adattamento. Sarà fondamentale avere un dialogo costante tra i team e Regione del Veneto, non solo prima e durante le esercitazioni, ma anche nella fase di follow-up, per implementare le raccomandazioni in modo efficace e tempestivo.

L'esercitazione dovrà prevedere almeno quanto segue:

Fasi Preparative

- Definizione degli Obiettivi: Stabilire insieme al committente gli obiettivi specifici e gli scenari di attacco.
- Pianificazione: Concordare le tempistiche e le modalità di esecuzione dell'esercitazione, inclusi dettagli operativi e aspetti logistici
- Selezione dei Partecipanti: Identificare i membri dei team Blue e Red, nonché eventuali enti esterni coinvolti, definendo ruoli e responsabilità per ciascun partecipante.

Esecuzione delle Esercitazioni

Durante le esercitazioni, il team Red simulerà le attività di attaccanti, mentre il team Blue testerà le sue capacità di

rilevazione e risposta agli attacchi. Dovrà essere garantito un ambiente controllato per evitare impatti dannosi sulle operazioni quotidiane di Regione del Veneto.

Reporting Post-Esercitazione

Al termine di ogni esercitazione, dovrà essere fornito un report dettagliato che includa:

- Sintesi delle Attività: Descrizione delle tecniche utilizzate e degli scenari affrontati.
- Esiti e Valutazione: Analisi delle performance dei team, con riferimento a metriche concordate precedentemente.
- Lezioni Apprese: Identificazione di punti di forza e aree di miglioramento al fine di integrare le conoscenze acquisite nel piano di sicurezza esistente.
- Piano di Remediation: Proposta di interventi correttivi, con tempistiche e attività specifiche.

Attuazione interventi correttivi

- Applicazione del piano di remediation nei tempi e nelle modalità presentate in fase di reporting post esercitazione
- Follow-up periodici per verificare l'applicazione delle contromisure previste nel piano di remediation

5.6 Servizi di gestione di licenze

Ambito del servizio è la presa in carico dei contratti (sia dal punto di vista gestionale sia dal punto di vista economico) relativi alle licenze Software, alle Subscription e agli eventuali contratti di manutenzione Hardware per l'intera durata della fornitura.

Il fornitore dovrà quindi organizzare e pianificare i rinnovi licenze nei tempi e modalità utili a consentire la continuità dell'erogazione dei servizi in sicurezza e nel rispetto degli adempimenti contrattuali e commerciali anche verso i provider delle licenze. Il mancato rispetto dei termini di attivazione o di rinnovo delle licenze comporterà l'applicazione, da parte dell'Amministrazione, di penali previste da capitolato tecnico. (vedasi Appendice 1 – Indicatori di qualità):

Dovrà quindi procedere a:

- Prendere in carico formalmente la titolarità delle licenze, qualora si richieda;
- Trasferire la titolarità delle licenze a RV al termine del contratto, qualora si richieda
- Monitorare le scadenze e fornitore report mensili (con il perimetro relativo alle licenze e manutenzioni e come profondità temporale di scadenza i 45 mesi di contratto) in coerenza col cruscotto di ITSM;
- Negoziare e rinnovare le licenze;
- Sostenere i costi di licenza (l'importo a disposizione per questo servizio consente all'aggiudicatario di gestire tali rinnovi e richiedere i servizi correlati).

Inoltre, il Fornitore avrà il compito di supportare la Regione del Veneto nella gestione di tali contratti, attraverso un'analisi approfondita del modello di licensing in uso, suggerendo eventuali modifiche qualora si verifichino variazioni nel modello di licensing dei prodotti coinvolti. Il dettaglio esaustivo delle licenze oggetto del servizio è descritto in Appendice 3 Contesto Tecnologico e Applicativo (par. 3.10).

Il fornitore dovrà inoltre garantire l'utilizzo delle licenze rinnovate per l'erogazione dei servizi in essere in RV anche al fornitore uscente (fino alla scadenza del contratto dell'uscente), qualora l'avvio del servizio da parte del fornitore entrante non fosse compatibile con la scadenza, ovvero il rinnovo delle licenze stesse.

6. Centro servizi e strumenti trasversali ai servizi e attività previste

Nel presente capitolo vengono indicati gli elementi che sono considerati trasversali e i costi relativi sono compresi nei servizi precedentemente descritti e alle attività ad essi sottesi.

6.1 Centro Servizi per l'operatività da remoto

Il Fornitore deve mettere a disposizione di RV e degli enti con convenzione PSR attiva, il centro servizi per l'erogazione dei servizi da remoto. Il Centro Servizi è attivo 24H, 7 giorni su 7, 365 giorni l'anno.

Le attività erogate da remoto dal centro servizi, e ricomprese comunque all'interno degli specifici servizi oggetto del contratto precedentemente illustrato, includono anche quanto segue:

- **Monitoraggio della gestione dei sistemi** con l'ausilio della "control room" del Centro e mediante l'impiego dello strumento indicato nella Tabella 2 - Elenco Strumenti;
- **Monitoraggio della sicurezza** con l'ausilio della struttura specializzata di Security Operation Center (SOC) del Centro e mediante l'impiego degli strumenti menzionati nell' Appendice 3 Contesto tecnologico e applicativo, e secondo le modalità del servizio descritte al § 5.1.7;
- **Monitoraggio End to End dei Servizi Applicativi** il tool nella configurazione finale dovrà essere reso disponibile entro 6 mesi dalla fine subentro/presa in carico;
- Analisi delle **performance dei Data Base dei servizi applicativi** mediante il tool che nella configurazione finale dovrà essere reso disponibile entro 3 mesi dalla fine subentro/presa in carico;
- Messa a disposizione della **piattaforma di reportistica e SLA management** mediante l'impiego di uno strumento che dovrà avere le caratteristiche riportate nel § 6.1.2.2;
- l'erogazione delle attività di **Log Collecting**, analisi e conservazione, mediante l'impiego di strumenti offerti da Fornitore; il tool nella configurazione finale dovrà essere reso disponibile entro 3 mesi dalla fine subentro/presa in carico;
- per l'erogazione delle attività da remoto al Fornitore è richiesto di attivare una VPN dal proprio Centro Servizi;
- l'erogazione delle attività di **gestione delle password** e dei certificati mediante l'impiego di strumenti offerti da Fornitore; il tool nella configurazione finale dovrà essere reso disponibile entro 3 mesi dalla fine subentro/presa in carico e dovrà rispettare specifiche caratteristiche come meglio dettagliate nel § 5.1.7.

Si specifica che quanto descritto non rappresenta uno o più servizi specifici aggiuntivi, ma sintetizza e dettaglia modalità e strumenti minimi che l'aggiudicatario dovrà mettere in campo nell'erogazione dei servizi stessi.

6.1.1 Caratteristiche ambientali e di sicurezza relative Centro Servizi

Si prevede che l'utilizzo del centro servizi non comporti alcun onere aggiuntivo per RV e che anche eventuali costi per il collegamento telematico tra il Centro Servizi del Fornitore e la rete dell'Amministrazione sono inclusi nel servizio.

Da tale centro, attraverso l'utilizzo degli opportuni strumenti e mediante l'impiego di personale specializzato, il Fornitore dovrà poter operare in collegamento con i sistemi di RV per effettuare tutte le attività di gestione sistemistica che non richiedono necessariamente la presenza di personale onsite, ovvero almeno le attività indicate al §5.6.

Il centro servizi deve quindi prevedere:

- una funzione di "service desk", attraverso la quale ricevere in modalità multicanale (telefono, mail, canale web) le segnalazioni e le richieste di RV;

- una “control room” per il monitoraggio e la gestione dei sistemi;
- strutture specializzate di Network Operation Center (NOC) e Security Operation Center (SOC);
- infrastrutture tecnologiche e strumenti operativi per il monitoraggio sistemi, la gestione dei processi di Service Management e la rendicontazione dei livelli di servizio, come dettagliato di seguito.

Si prevede che tale centro servizi venga messo a disposizione a RV anche nell’ambito dei servizi erogati con presidio onsite e deve essere utilizzato per quella parte di attività di gestione remotizzabili, il cui dettaglio sarà stabilito in sede di avvio del servizio; a titolo esemplificativo e non esaustivo, potrà essere utilizzato per quanto riguarda la funzione di service desk o la piattaforma di reportistica e SLA management.

Si richiede evidenza al Fornitore che il centro servizi sia obbligatoriamente ubicato nel territorio di uno degli Stati membri dell’Unione Europea, inoltre, la lingua di riferimento per l’erogazione dei servizi deve essere l’italiano.

Il Fornitore, compatibilmente con le politiche di sicurezza di RV, dovrà collegarsi alla sede (centrale) dell'Amministrazione ed utilizzare la rete dati (VPN) di RV stessa per l’erogazione in modalità remota.

Si prevede di instaurare comunicazioni sicure, basate su moderni standard di sicurezza delle reti e dei sistemi e protocolli di crittografia: il Fornitore deve fornire evidenza delle garanzie di sicurezza dei collegamenti e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l’applicazione di procedure e politiche di sicurezza da adottare al proprio interno (Sistema di Gestione delle Sicurezza delle Informazioni – SGSI), adeguate ai requisiti stabiliti da RV. Infatti, è responsabilità del Fornitore assicurare che il Centro Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni da e verso la rete dell’Amministrazione siano protette mediante l’adozione di adeguati sistemi e metodologie.

Il Fornitore deve garantire i seguenti servizi di sicurezza:

- mutua autenticazione: l'identità delle entità in comunicazione deve essere garantita attraverso meccanismi di crittografia asimmetrica, ovvero a chiave pubblica con lunghezza delle chiavi opportuna. È prevista a carico del Fornitore la certificazione digitale del canale di comunicazione con RV. É prevista a carico del Fornitore la gestione e la distribuzione delle chiavi e dei certificati;
- autorizzazione: individuare, sulla base delle credenziali fornite dall’utente, i diritti e le autorizzazioni che tale utente possiede e permetterne l’accesso alle risorse limitatamente a tali autorizzazioni;
- confidenzialità nella trasmissione dei dati: fornire gli strumenti per la cifratura della informazione, garantendo un adeguato livello di protezione della confidenzialità dei dati. Gli algoritmi crittografici utilizzati e la lunghezza delle chiavi devono essere opportunamente scelti in modo da garantire la confidenzialità dell'informazione;
- integrità dei dati: fornire meccanismi che permettano di garantire l'integrità del messaggio scambiato tra due entità; la possibilità di rilevare alterazione del messaggio deve essere basata su funzioni di hashing considerate “sicure” (MD5, SHA, RIPEMP- 160, ecc.) con opportuna lunghezza delle chiavi.

Nel seguito si riportano alcuni obiettivi di controllo, classificati sulla base di quanto previsto dallo standard 27001, che il Fornitore si impegna a mettere in pratica nel SGSI applicato nell’ambito del proprio Centro Servizi.

ID	ITEM	Obiettivi di controllo
A.6.2	Parti esterne	Mantenere la sicurezza delle informazioni dell'organizzazione e delle strutture di elaborazione delle informazioni oggetto di accessi, elaborate, comunicate o gestite da parti esterne

A.8	Sicurezza delle risorse umane	Assicurare la responsabilità di dipendenti, collaboratori e utenti di terze parti prima, durante e al termine dell'impiego
A.9.1	Aree Sicure	Prevenire l'accesso fisico non autorizzato, il danneggiamento e le interferenze verso i locali e le informazioni dell'organizzazione
A.10.4	Protezione contro software dannoso e codice autoeseguibile	Proteggere l'integrità del software e delle informazioni
A.10.5	Backup	Mantenere l'integrità e la disponibilità delle informazioni e delle strutture di elaborazione delle informazioni
A.10.6	Gestione della sicurezza della rete	Assicurare la salvaguardia delle informazioni nelle reti e la protezione delle infrastrutture di supporto
A.10.10	Monitoraggio	Individuare le attività di elaborazione delle informazioni non autorizzate
A.11.2	Gestione dell'accesso degli utenti	Assicurare l'accesso ai sistemi informativi agli utenti autorizzati e prevenire gli accessi non autorizzati
A.13.1	Segnalazione degli eventi e dei punti di debolezza relativi alla sicurezza delle informazioni	Assicurare che gli eventi relativi alla sicurezza delle informazioni e i punti di debolezza dei sistemi informativi siano segnalati in modo da permettere tempestive azioni correttive
A.14.1	Aspetti di sicurezza delle informazioni relativi alla gestione della continuità operativa	Contrastare le interruzioni delle attività relative al business, proteggerne i processi critici dagli effetti di malfunzionamenti significativi dei sistemi informativi o da disastri e assicurare il loro tempestivo ripristino

Tabella 4 - Obiettivi di controllo

6.1.2 Strumenti operativi del Centro Servizi

Come già indicato all'inizio del paragrafo, all'interno del proprio centro servizi il Fornitore deve disporre degli opportuni strumenti operativi da utilizzare nell'esecuzione delle attività di system management e in particolare:

- una piattaforma di monitoraggio sistemi;
- una piattaforma di Service Management;
- una piattaforma di reportistica e SLA management.

L'utilizzo degli strumenti suddetti è incluso nei costi dei servizi richiesti e pertanto non comporta alcun onere aggiuntivo per RV; in particolare, è incluso nei costi dei servizi l'eventuale installazione di componenti client (agent) per le attività di monitoraggio da remoto e qualsiasi altro costo collegato all'utilizzo degli strumenti. Nel seguito sono evidenziate le principali funzionalità che tali strumenti devono possedere.

6.1.2.1 Piattaforma di monitoraggio

Il monitoraggio dei sistemi richiede l'utilizzo di strumenti specifici per la rilevazione degli alert e dei parametri di funzionamento dei sistemi stessi; il Fornitore è tenuto a mettere a disposizione di RV una piattaforma di Monitoraggio dei sistemi e delle applicazioni. La piattaforma di monitoraggio dovrà consentire di tenere sotto controllo lo stato operativo dei sistemi e delle relative componenti e degli apparati di rete, rilevando automaticamente informazioni quali a titolo esemplificativo, ma non esaustivo:

- Stato dei diversi sistemi, sottosistemi, servizi ed apparati;
- Parametri critici per la funzionalità dei diversi sistemi, sottosistemi, servizi ed apparati, definendo dei valori di soglia che denuncino la prossimità di situazioni critiche. Ad esempio, per i server tali parametri potranno riguardare:

- Allocazioni di spazio disco;
- Utilizzo della memoria;
- Utilizzo della CPU;
- Utilizzo delle interfacce di rete.

- Stato dei processi applicativi che siano di particolare rilevanza per la funzionalità dei servizi erogati.

Nell'ambito della piattaforma di monitoraggio, il Fornitore deve prevedere una soluzione per il monitoraggio end-to-end dei servizi applicativi erogati agli utenti finali, in modo da poterne facilmente verificare lo stato operativo e prestazionale. Correlando tutte le informazioni provenienti dai vari sistemi che costituiscono l'ambiente di esercizio con quelle relative alle transazioni applicative, la soluzione dovrà dare evidenza dello stato operativo dei servizi applicativi erogati ed essere così di supporto alla rapida risoluzione dei problemi. In particolare, deve consentire di identificare automaticamente le componenti da controllare lungo la catena applicativa in caso di errore. Oltre a monitorare la disponibilità dei servizi applicativi e ad essere di supporto nella risoluzione dei problemi, la soluzione dovrà consentire di verificare e controllare sia le performance dei servizi erogati, in ottica di verifica dell'aderenza ai livelli di servizio attesi, sia la user experience, garantendo un'esperienza utente ottimale in termini di accessibilità, tempi di risposta e fruibilità complessiva.

6.1.2.2 Piattaforma di Service Management

Per l'erogazione dei servizi di gestione, il Fornitore è tenuto a mettere a disposizione di RV una piattaforma di Service Management, attraverso la quale operare applicando le best practices ITIL nei settori:

- Service operation (in particolare Event management, Incident management, Request fullfillment, Problem management, Access management);
- Service transition (in particolare Change management, Service Asset and Configuration management, Release and deployment management, Knowledge management).

In fase di avvio del servizio RV definirà in dettaglio gli elementi distintivi dei processi di System Management richiesti, come ad esempio:

- l'identificazione dei Configuration Items;
- la creazione e gestione della knowledge base;
- la definizione delle priorità degli incident (ad esempio attraverso una matrice urgenza/impatto: urgenza alta/media/bassa attribuita dal richiedente e impatto alto/medio/basso attribuito dall'Incident Manager);
- la definizione dei criteri di escalation e le correlazioni con eventuali strutture di supporto esterne;
- la classificazione delle operazioni di change in categorie standard/non standard e l'individuazione di ulteriori classi per la classificazione dei change standard, con le tempistiche di risposta;
- l'organizzazione della funzione di release management in relazione agli ambienti di sviluppo/test/preproduzione/produzione.

6.1.2.3 Piattaforma di reportistica e SLA management

Il Fornitore deve rendere disponibile a RV un sistema per l'analisi degli andamenti dei livelli di servizio, allo scopo di:

- verificare la conformità dei servizi rispetto a quanto richiesto;
- verificare l'effettivo andamento dei servizi e anticipare la gestione degli scostamenti;
- consuntivare i servizi e le attività;
- verificare l'andamento degli Indicatori di qualità;
- ottimizzare le attività di monitoraggio dei servizi.

Il sistema deve raccogliere i dati elementari, calcolare gli Indicatori di qualità della fornitura e, sulla base di essi, predisporre delle rappresentazioni dell'andamento della stessa. Nel caso in cui parte dei dati elementari siano gestiti

da sistemi di RV, il Fornitore deve predisporre ed assicurare tutto quanto necessario per il caricamento dei dati, nel formato e con la periodicità stabilita congiuntamente con RV e la successiva elaborazione e pubblicazione secondo le stesse modalità applicate ai dati elementari direttamente gestiti. Inoltre, il Fornitore si impegna a fornire la base dati di dettaglio contenente tutti i dati rilevati, utilizzata per la valorizzazione degli indicatori di qualità.

Il sistema deve prevedere la possibilità di esportare i report in formati dati e grafici di comune utilizzo e visualizzabili nelle comuni Suite applicative per l'ufficio, per un successivo ed eventuale trattamento (modifica, manipolazione, esportazione, ecc.). Inoltre, è richiesta la fornitura di strumenti idonei, cui verrà dato accesso a RV, per effettuare interrogazioni e query delle basi dati sopra definite.

Devono, inoltre, essere rese disponibili tutte le informazioni inerenti il personale impegnato in ciascun servizio onsite, in termini di figura professionale e grado di utilizzo.

6.1.3 Servizio di monitoraggio sicurezza

Al Fornitore è richiesta l'erogazione di un servizio di monitoraggio della sicurezza per l'individuazione e gestione delle minacce cyber che possono compromettere l'operatività dei servizi IT di RV e del PSR e la gestione dell'evento avverso e della definizione delle misure di contrasto e mitigazione.

Le attività comprese nel servizio riguardano l'acquisizione e la trattazione dei log degli asset IT, l'analisi degli eventi di sicurezza, l'individuazione degli incidenti e la loro mitigazione.

Sono inclusi nel perimetro di monitoraggio:

- le infrastrutture di rete;
- gli apparati di rete e sicurezza;
- i server su ambiente on premise e su ambienti cloud;
- le PDL.

Il servizio deve essere erogato in modalità as a service dal Centro Servizi del Fornitore. Esso dovrà rendere disponibile a RV l'accesso ad eventuali console di management al fine di poter visualizzare lo stato del servizio in tempo reale e di accedere alla reportistica concordata.

Ove necessario, è consentita l'installazione presso i DATA CENTER della Regione Veneto di eventuali componenti applicative da utilizzare per l'erogazione del servizio.

Nell'ambito del servizio per eventi di sicurezza si intendono tutti gli accadimenti che hanno impatto sia sulla sicurezza dei sistemi ICT, sia sulla protezione dei dati contenuti ed elaborati da tali sistemi ICT, sia sull'erogazione dei servizi e microservizi ICT di responsabilità e di competenza di RV.

Le attività previste riguardano:

- Raccolta, analisi e individuazione degli eventi e delle minacce di sicurezza; ivi incluse le segnalazioni di phishing da parte degli utenti e la verifica di eventuali allegati
- Classificazione degli incidenti di sicurezza;
- Gestione degli Incidenti di sicurezza
- Redazione di reportistica sulle attività eseguite.

Raccolta, analisi e individuazione degli eventi e delle minacce di sicurezza;

Il Fornitore deve essere in grado di collezionare i Log provenienti dagli asset definiti nel perimetro del servizio al fine di poter effettuare l'analisi e la correlazione degli eventi di sicurezza rilevati.

I Log possono provenire da apparati di rete, apparati di sicurezza e server posizionati sia presso i Data Center di Regione Veneto che su istanze Cloud. Il Fornitore dovrà rendere disponibili gli eventuali connettori necessari per interfacciare il proprio sistema di Log Collecting con i sistemi d'origine. È richiesto che il Fornitore conservi i Log acquisiti per un periodo di 24 mesi di cui almeno 6 online in formato RAW mantenendo la conservazione adeguata alle tempistiche richieste dalle normative di riferimento e che siano fruibili e accessibili a Regione del Veneto

Sulla base dei dati raccolti, il Fornitore deve aggregare le informazioni significative operando in tempo reale analisi e correlazioni finalizzate a individuare comportamenti anomali e segnali critici al fine di individuare possibili incidenti di sicurezza.

L'analisi delle minacce deve essere eseguita dal Fornitore utilizzando almeno le seguenti fonti:

- i bollettini di sicurezza emessi periodicamente da fornitori di hardware e software;
- gli enti di riferimento sia nazionali (es. CERT Italia, CERT-PA) che internazionali (es. SANS, US- CERT, CSIRT);
- feed specifici a pagamento;

Classificazione degli eventi di sicurezza:

Gli eventi di sicurezza dovranno essere classificati dal Fornitore al fine di procedere al corretto indirizzamento alle strutture preposte alla gestione ed a fornire le informazioni relative alla criticità di quanto rilevato.

Classificazione degli eventi di sicurezza e incidenti di sicurezza per criticità:

- Bassa criticità: eventi di sicurezza o offense che sono registrati e conservati per analisi successive;
- Media criticità: incidenti di sicurezza o offense che richiedono un intervento nel medio termine per prevenire situazione critiche;
- Alta criticità: incidenti di sicurezza o offense che richiedono un intervento immediato.

Classificazione degli incidenti per tipologia:

La classificazione degli incidenti di sicurezza per criticità deve essere eseguita da una classificazione in funzione della tipologia. A puro titolo di esempio:

- Contenuti illeciti;
- Codice Malevolo;
- Raccolta Informazioni;
- Tentativi di intrusione;
- Intrusioni;
- Availability;
- Sicurezza dei contenuti informativi;
- Frode.

Classificazione degli incidenti per severità:

Insieme alla classificazione per criticità preventivamente rilevata, dovrà essere operata una classificazione sul livello di severità dell'evento (es. offense), rilevando la potenziale o effettiva pericolosità dell'evento in funzione della pericolosità del tipo di minaccia rilevato in relazione al contesto di Regione Veneto e alla estensione dell'evento stesso.

Gestione degli incidenti

In caso di individuazione di un incidente, il Fornitore, una volta effettuata la classificazione, dovrà procedere a definire il piano di intervento suggerito e predisporre un report di incident da inviare alle strutture preposte alla conduzione operativa dell'Infrastruttura.

Il report di incident dovrà contenere almeno le seguenti informazioni:

- Data / ora rilevazione dell'incident;
- Asset / servizi coinvolti nell'incident;
- Classificazione per criticità e tipologia;
- Severità dell'incident;

- Remediation plan suggerito.

Il Fornitore dovrà inviare il report utilizzando il sistema di trouble ticketing reso disponibile dall'Amministrazione.

Reportistica

Il Fornitore deve produrre mensilmente un report di riepilogo relativo alle attività svolte nell'ambito del servizio.

Il report dovrà contenere almeno le seguenti informazioni:

- Il numero totale degli eventi di sicurezza rilevati nel periodo;
- La lista degli eventi che sono stati classificati come incidenti di criticità medio / alta;
- La lista degli asset / servizi coinvolti in un incidente di sicurezza;
- La lista delle tipologie di incidenti rilevati.

Il Fornitore dovrà produrre un report di sintesi statistica su base trimestrale, semestrale e annuale riepilogando i trend degli incidenti di sicurezza con indicazione delle classificazioni, dei sistemi impattati e delle criticità rilevate.

6.2 Strumenti a supporto della fornitura in uso presso RV

Nel presente paragrafo sono rappresentati i principali strumenti a supporto della fornitura in uso presso RV e che il Fornitore deve rendere disponibili per l'erogazione trasversale dei servizi ricompresi nell'appalto, come previsto nel "Servizio gestione licenze"

Pur lasciando al Fornitore la possibilità di proporre liberamente gli strumenti in fase di Offerta Tecnica, Regione Veneto privilegia la continuità con le scelte tecnologiche già adottate, valorizzando gli investimenti effettuati nel tempo e garantendo il mantenimento del livello di integrazione tra gli strumenti attualmente in uso, inclusi quelli menzionati nel presente paragrafo.

Strumenti principali	Piattaforma in uso
Monitoraggio infrastrutturale	Ivertix (Centreon)
Sistema di Trouble Ticket	Sysaid
Sistema IT Asset Management	
Sistema ITSM	
Piattaforma DevOps	Atlassian Open DevOps

Tabella 5 - Strumenti a supporto della fornitura in uso

Il dettaglio **completo** degli strumenti in uso è riportato in Appendice 3 Contesto Tecnologico e Applicativo.

7. METRICHE E DIMENSIONAMENTO DEI SERVIZI

In questo capitolo sono riportati i parametri di dimensionamento e le modalità di remunerazione e di eventuale variazione dei servizi, il relativo dimensionamento, riferito all'intera durata contrattuale, sulla base delle informazioni disponibili alla data di pubblicazione della presente procedura aperta. RV si riserva, comunque, in fase di presa in carico dei servizi, di effettuare una nuova valutazione degli asset affidati in gestione, ai fini dell'eventuale riconteggio dei canoni. Tale dimensionamento si intende, pertanto, non vincolante, riservandosi RV di attivare i servizi in misura maggiore o minore rispetto ai valori indicati.

7.1 Modalità di remunerazione e variazioni

I servizi saranno remunerati a Canone o a Consumo, ossia a Misura, come dettaglio nei paragrafi successivi e sintetizzato in tabella.

Nel seguito vengono illustrate anche le modalità di variazione previste

Macroservizio	ID Servizio	Sotto servizio	Rif.Par.	Metrica	Unità di misura	Modalità di remunerazione
Servizi conduzione operativa sistemi	COND-OP	Conduzione operativa sistemi e sicurezza	5.1	Canone mensile	€/mese	Canone posticipato
	MON24	Servizio di monitoraggio H24	5.2	Canone mensile	€/mese	Canone posticipato
Servizi di supporto	CAP-COO	Coordinatore - capo progetto	5.3	Numero di giorni	€/gg	A consumo
	SPEC-TEC	Specialista di tecnologia	5.3	Numero di giorni	€/gg	A consumo
	SIST-SEN	Sistemista senior	5.3	Numero di giorni	€/gg	A consumo
	SIST	Sistemista	5.3	Numero di giorni	€/gg	A consumo
	SIST-JN	Sistemista junior	5.3	Numero di giorni	€/gg	A consumo
Servizi di supporto – interventi fuori orario	SUP-CAP-COO	Coordinatore - capo progetto	5.3	Numero di ore	€/h	A consumo
	SUP-SPEC-TEC	Specialista di tecnologia	5.3	Numero di ore	€/h	A consumo
	SUP-SIST-SEN	Sistemista senior	5.3	Numero di ore	€/h	A consumo
Servizi di gestione operativa	SD-RIS	I° livello	5.4.1	Numero Ticket risolti I° livello	€/Tkt	A consumo
		II° livello	5.4.1	Numero Ticket inoltrati al II° livello	€/Tkt	A consumo
		Ore Extra-Orario SPOC	5.4.1	Numero Ore	€/h	A consumo
		Reperibilità SPOC	5.4.1	Numero Ore	€/h	A consumo
	PDL-PC	Gestione Postazioni di Lavoro	5.4.2	Numero di postazioni gestite	€/PDL mese	A canone per quantità gestita
	PDL-VDC	Gestione Videoconferenze	5.4.2.9	Canoni annuo	€/anno	A canone per quantità gestita
Servizi di Sicurezza	SIC-VAS	Vulnerability assessment dell'Infrastruttura	5.5.1	Numero Indirizzi IP	€/IP	A canone per quantità gestita
	SIC-VVA	Verifica della vulnerabilità Applicazioni WEB	5.5.2	Numero applicazioni gestite	€/app	A canone per quantità gestita
	SIC-THI	Threat intelligence	5.5.3	Canone mensile	€/mese	Canone posticipato
	SIC-SOC	SOC	5.5.4	Numero EPS	€/EPS/ mese	A canone per quantità gestita
Servizi gestione licenze	LIC	Servizi gestione licenze	5.6	Canone annuo	€/anno	Canone posticipato

Tabella 6 - Modalità remunerazione per Servizio

I supporti alla transizione (in avvio di servizio e al termine del contratto) sono inclusi nei costi dei servizi e la responsabilità della gestione contrattuale viene mantenuta dal Fornitore fino al termine delle attività di trasferimento dei servizi in conformità a quanto previsto nel contratto.

Tutte le eventuali variazioni verranno operate nel rispetto dell'art. 120 del D.Lgs. 36/2023, in conformità alla normativa vigente sugli appalti pubblici e comunque della normativa vigente.

7.1.1 Servizi a canone

I servizi remunerati a canone sono erogati in modalità continuativa per tutta la durata della fornitura, da svolgere negli orari previsti senza soluzione di continuità.

L'Amministrazione, inoltre, esegue un costante controllo sulle risorse professionali messe a disposizione dal Fornitore, mediante la rilevazione nominativa delle presenze controllando, inoltre, che i vincoli stabiliti per le sostituzioni del personale vengano rispettati, al fine di mantenere costante il grado di professionalità delle risorse che sono messe a disposizione.

7.1.1.1 Servizio conduzione operativa dei sistemi

Per il servizio di conduzione operativa dei sistemi (incluso il servizio di monitoraggio H24) e sicurezza in fase di esecuzione contrattuale, con cadenza annuale, il Fornitore effettuando una verifica degli asset oggetto del servizio (verifica che avviene con cadenza almeno annuale, salvo diversa richiesta da parte di RV), determina le quantità di server e database in conduzione operativa ("baseline anno n-esimo") e determina la differenza rispetto alla rilevazione ad inizio contratto ("baseline anno 1") e all'anno precedente ("baseline anno n-1") e presenta a RV un report di dettaglio.

Il contenuto di tale report verrà concordato in fase di avvio del servizio. Sulla base della differenza rilevata potranno essere adeguati gli importi da corrispondere al Fornitore aumentandoli o diminuendoli secondo la modalità di seguito descritte. Il modello descritto ha l'obiettivo di premiare un efficientamento del dimensionamento dell'infrastruttura.

Nel calcolo della **baseline** dell'infrastruttura in conduzione operativa e monitoraggio H24 l'Aggiudicatario dovrà tenere in considerazione quanto segue:

- Concorrono al calcolo delle quantità in baseline solo i server accesi alla data di rilevazione;
- Non concorrono al calcolo delle quantità in baseline i server fisici;
- Le VM dei servizi presso cloud provider concorrono al calcolo delle quantità in baseline;
- I server AIX concorrono al calcolo delle quantità in baseline come "VM Linux";
- Sono esclusi e non concorrono al calcolo delle quantità i servizi database PAAS dei cloud provider;
- Concorrono al calcolo delle quantità solo le istanze attive primarie, escludendo le repliche;
- Non concorre al calcolo delle quantità in baseline lo storage del backup;
- Non concorre al calcolo delle quantità in baseline lo storage degli ambienti iperconvergenti;
- Concorrono al calcolo delle quantità in baseline solo apparati attivi/accesi alla data di rilevazione.

Eventuali revisioni o integrazioni alle specifiche potranno essere concordate durante il corso del contratto in seguito a eventuali cambiamenti dell'ecosistema.

Di seguito le modalità di variazione, eventuale e annuale, del canone del servizio di conduzione operativa sistemi e sicurezza e monitoraggio H24.

Determinazione del parametro di sintesi del dimensionamento "Baseline" (Indice di Baseline)

L'indice di baseline dell'anno i-esimo ($IndB_i$) viene calcolato mediante la sommatoria dei prodotti tra le quantità rilevate per ogni singolo elemento e il coefficiente dell'elemento.

Indice di baseline $_{(anno\ i\text{-}esimo)} = IndB_i = \sum_{i=0}^{n} Ei \times Ci$

Elemento (E_i)	Parametro dimensionamento delle quantità	Coefficiente elemento (C_i)
Quantità server logici Unix/Linux	num. Server	50%
Quantità server logici Windows	num. Server	20%
Quantità apparati rete/sicurezza	num. Apparati	5%
Quantità DBMS presidio	num. Istanze	20%
Quantità Storage	q.tà TB	5%

Determinazione del parametro di sintesi della variazione della "Baseline" (Variazione di Baseline)

La variazione della baseline (Var_i) dei servizi di conduzione operativa è determinata dal rapporto tra l'indice di baseline dell'anno i-esimo rispetto all'indice di baseline dell'anno (i-1) con la seguente formula

Variazione delle baseline $_{(anno\ i\text{-}esimo)}$ **= Var$_i$ =** $\frac{IndB_i}{IndB_{i-1}}$ **- 1**

Determinazione della variazione dei canoni per i servizi di conduzione operativa dei sistemi

Sulla base delle variazioni della baseline viene determinata la variazione eventuale (in aumento o diminuzione) dei canoni per i servizi di conduzione operativa dei sistemi secondo le seguenti regole.

Variazione baseline in conduzione operativa (Var$_i$)	**Variazione canone**
Per Var$_i$ compreso tra 0 e 10% ($0 \leq Var_i \leq 10\%$)	Nessuna variazione rispetto al canone dell'anno precedente.
Per Var$_i$ superiore a 10% ($Var_i > 10\%$)	Aumento del canone per i servizi di conduzione operativa dei sistemi dell'anno successivo alla rilevazione per un valore pari al 20% del valore Var$_i$ eccedente il 10%. **Esempio** *Canone del servizio anno i-1 = 1.000.000 €* ***Variazione baseline, Var$_i$ = 15%*** *Variazione % canoni del servizio per l'anno i pari a (15%-10%)*20% = +1%* *Variazione del canone del servizio = 1.000.000 € + 1.000.000 € x 1%* **Variazione canone = +1%** A seguito dell'aumento della dimensione degli asset in conduzione operativa, il fornitore dovrà valutare l'eventuale necessità di aumentare anche le FTE dedicate al fine di garantire i livelli di servizio previste nel rispetto degli IQ.
Per Var$_i$ minore di 0% (ovvero negativo, $Var_i < 0$)	Riduzione del canone per i servizi di conduzione operativa dei sistemi dell'anno successivo alla rilevazione per un valore pari al 25% del valore Var$_i$. **Esempio** *Canone del servizio anno i-1 = 1.000.000 €* ***Variazione baseline, Var$_i$ = -10%*** *Variazione % canoni del servizio per l'anno i pari a (-10%)*25% = -2,5%* *Variazione del canone del servizio = 1.000.000 € - 1.000.000 x 2,5%* **Variazione canone = -2,5%**

Tabella 7 – Variazione canone baseline

7.1.1.2 Altri servizi

- Per il **servizio di Gestione Postazioni di Lavoro (par. 5.4.2)** il canone unitario contrattualizzato (a PDL) vale per tutta la durata del contratto e i corrispettivi vengono ogni mese determinati sulla base del numero di PC Desktop e Notebook rendicontati nei SAL mensili, presentati dal Fornitore ed approvati dall'Amministrazione. Il canone costituisce la modalità di remunerazione omnicomprensiva per tutte le attività rientranti nel servizio di postazioni di lavoro.
- Per il **servizio di gestione licenze (par 5.6),** il canone contrattualizzato vale di norma per tutta la durata contrattuale e può essere variato, di concerto fra Fornitore e RV, solo a seguito di consistenti variazioni (+ / - 10% del valore del servizio annuo definito a livello di offerta e dettagliato a livello di contratto) del parco licenze affidato in gestione, ovvero di complete dismissioni o sostituzioni delle licenze durante il periodo contrattuale.

  Si specifica che a livello di contratto sarà dettagliato l'importo del canone per singole licenze, al fine di determinare le eventuali variazioni.
- Per gli **altri Servizi a canone**, non precedentemente dettagliati, in fase di esecuzione contrattuale, con cadenza annuale, il Fornitore produce e presenta all'Amministrazione un report di dimensionamento e verifica delle quantità oggetto del servizio e variazione rispetto alle quantità determinate ad avvio contratto. A seguito di

approvazione del dimensionamento da parte dell'Amministrazione, gli importi di canoni da corrispondere al Fornitore sono quindi adeguati alla effettiva dimensione gestita, aumentandoli o diminuendoli proporzionalmente.

7.1.2 Servizi a consumo/misura

Per i servizi a consumo o a misura si prevedono le seguenti modalità:

Tempo/spesa in giorni per figura professionale

Per i servizi per i quali è prevista una remunerazione a consumo / misura con una valorizzazione a "Tempo/spesa in giorni per figura professionale (GG/PP)" saranno utilizzate le tariffe unitarie contrattualizzate per ciascuna figura professionale che varranno per tutta la durata del contratto.

I corrispettivi dovuti sono determinati sulla base della composizione dei gruppi di lavoro e delle attività stimate in fase di pianificazione ed effettivamente eseguite in ciascun mese di riferimento, indicati nei SAL mensili, presentati dal Fornitore ed approvati dall'Amministrazione.

Remunerazione a ore per figura professionale

Per gli "Interventi Fuori Orario" è prevista una remunerazione delle ore di lavoro erogate nell'ambito dei servizi, al di fuori dell'orario base anche in giornate festive e/o nel fine settimana, a seguito di attivazione da parte di RV in maniera formale e con almeno 4 giorni lavorativi di anticipo. Questa tipologia di intervento deve essere rendicontata in ore lavorate in extra orario, eseguite nel mese da ciascuna risorsa professionale e prevede una modalità di riconoscimento alla tariffa definita.

Remunerazione a Ticket (a consumo)

Per il servizio di SPOC, il controllo del servizio è sull'efficacia ed efficienza di risoluzione dei ticket e non sul numero di FTE.

La remunerazione del servizio sarà come segue, si considera:

- Numero di ticket chiusi e risolti al 1° livello per la relativa tariffa definita contrattualmente (comprende tutti i ticket che il 1° livello ha risolto in autonomia);
- Numero di ticket aperti al 1° livello ed inoltrati correttamente ad uno dei 2° livelli per la relativa tariffa (comprende anche i ticket di MAD, MAC, MEV, SVI, PP, GA di cui sia stata richiesta apertura da parte del personale RV). Sono esclusi dal computo: i ticket inoltrati erroneamente al 2° livello, e i ticket aperti direttamente al 2° livello dai soggetti deputati alle attività di conduzione operativa e monitoraggio.

Si specifica che i TKT chiusi e risolti (ovvero non riaperti o comunque non generanti altri ticket per una mancata risposta efficace e completa per la risoluzione) tramite soluzioni automatiche di chatbot verranno remunerati al 50% della tariffa.

L'Aggiudicatario produrrà un report periodico per la rendicontazione delle attività con le numeriche di chiusura e risoluzione e il dettaglio dei ticket ricadenti nei cluster (chiusi e risolti 1° livello vs aperti 1° livello e inoltrati 2° livello). RV si riserva di effettuare verifiche anche puntuali e verificare la qualità delle risoluzioni prodotte con soluzioni automatiche, ovvero l'effettiva risoluzione al 1° livello, ed eventualmente provvedere a richiedere storno delle quantità non correttamente classificate.

Reperibilità SPOC (a consumo)

Per il servizio di Reperibilità SPOC la metrica di riferimento sono le ore di lavoro erogate in sola reperibilità da una risorsa professionale nell'ambito dei servizi di Service Desk di 1° livello, a complemento dell'orario base esteso anche in giornate festive e/o nel fine settimana.

Questa tipologia di intervento deve essere rendicontata in numero di ore in reperibilità per la tariffa fissa. Il servizio di Reperibilità SPOC non deve essere attivato in caso di attivazione dell'extra orario SPOC.

Le eventuali interazioni del servizio SPOC erogate tramite chatbot o altra modalità automatica non sono conteggiate per la valorizzazione della Reperibilità SPOC.

Extra Orario SPOC (a consumo)

Per il servizio "Extra orario SPOC" la metrica di riferimento sono le ore di lavoro erogate nell'ambito dei servizi di Service Desk di 1° livello al di fuori dell'orario base esteso, anche in giornate festive e/o nel fine settimana, a seguito di attivazione da parte di RV in maniera formale e con almeno 4 giorni lavorativi di anticipo. Questa tipologia di intervento deve essere rendicontata in ore lavorate in extra orario e prevede una modalità di riconoscimento a tariffa fissa, che prescinde dal numero di operatori impiegati. Tale tariffa è aggiuntiva, rimanendo invariato il pagamento dei ticket che in extra orario vengono risolti correttamente al 1° livello oppure inoltrati correttamente ai 2° livelli.

Le eventuali interazioni del servizio SPOC erogate tramite chatbot o altra modalità automatica non sono conteggiate per la valorizzazione della Reperibilità SPOC.

7.2 Misurazione dei Servizi Conduzione Operativa dei sistemi e Sicurezza

Il servizio di conduzione dei sistemi è dimensionato sui seguenti parametri. Rimane inteso che il servizio viene remunerato a canone, con la richiesta di un dimensionamento minimo specifico del personale coinvolto (Par. 8.4.2), e eventualmente rivisto sulla base delle regole descritte nel presente capitolato.

Descrizione		Tipologia	N° elem. I Anno*	N° elem. II Anno	N° elem. III Anno	N° elem. IV Anno
Presidio onsite orario base server logici Unix/Linux	U1	Server logico Unix/Linux semplice	398	398	398	398
	U2	Server logico Unix/Linux complesso	930	930	930	930
Presidio onsite orario base server logici Windows	W1	Server logico Windows semplice	85	85	85	85
	W2	Server logico Windows complesso	198	198	198	198
Presidio onsite orario base apparati rete/sicurezza	R1	Apparato rete/sicurezza semplice				
	R2	Apparato rete/sicurezza complesso	70	70	70	70
Presidio onsite orario base sottosistemi DBMS	D1	Sottosistema DBMS semplice	52	52	52	52
	D2	Sottosistema DBMS complesso	120	120	120	120
Quantità complessiva di storage installato (TeraByte)			865	865	865	865
Livello di complessità infrastruttura storage (0, 1, 2, 3, 4) (**)			3	3	3	3

** con "I Anno" si intende il primo anno di contratto ovvero i mesi da 4° al 12° del primo anno.*

Quanto indicato rappresenta quanto in essere alla data di stesura del presente documento. Il contesto, ovvero le quantità potranno evolversi ulteriormente nel corso dei prossimi 12 mesi. L'aggiudicatario dovrà farsi carico dell'eventuale nuovo contesto e di eventuali variazioni che dovessero intercorrere nel corso del contratto.

(**) La classificazione della complessità dell'infrastruttura storage si basa su una scala da 0 a 4, determinata secondo la presenza o meno di specifici quattro parametri tecnici. Ogni parametro rilevato nell'ambiente di riferimento contribuisce all'incremento del livello di complessità, secondo una logica cumulativa. I parametri considerati sono i seguenti:

- Dimensione media dei sottosistemi (ovvero rapporto tra i TB complessivamente installati e il numero di sottosistemi di storage presenti) < 50 TB;
- Numero di tipologie di accesso alle unità disco (ad esempio FC/SAN, iSCSI, NAS, CAS) complessivamente presenti > 2;
- Numero di piattaforme tecnologiche (cioè appartenenti a vendor distinti) complessivamente utilizzate > 2;
- Numero di prodotti software di backup utilizzati > 1.

Laddove nessuno dei suddetti parametri sia applicabile, l'infrastruttura viene considerata semplice (livello = 0); laddove invece siano applicabili uno o più dei parametri suddetti, il livello di complessità aumenta progressivamente fino al livello massimo (livello = 4).

Il livello di complessità viene quindi determinato sulla base del numero di parametri riscontrati nell'infrastruttura:

- Livello 0: nessun parametro applicabile – infrastruttura semplice.

- Livello 1: un parametro applicabile – complessità bassa.
- Livello 2: due parametri applicabili – complessità medio-bassa.
- Livello 3: tre parametri applicabili – complessità medio-alta.
- Livello 4: tutti e quattro i parametri applicabili – complessità elevata.

Tale criterio è a titolo informativo che ne rappresenta lo stato dell'arte, non sono previste modifiche in caso di variazione della complessità e non influirà sui canoni base di remunerazione dei servizi.

Per il dettaglio sul dimensionamento del servizio di sicurezza logica e di conduzione e gestione della manutenzione hw si faccia riferimento a quanto descritto nell'Appendice 3 "Contesto Tecnologico e Applicativo", sottolineando che tale contenuto rappresenta quanto in essere alla data di stesura del presente documento e che potrà evolversi ulteriormente nel corso dei prossimi 12 mesi. L'aggiudicatario dovrà farsi carico dell'eventuale nuovo contesto e di eventuali variazioni che dovessero intercorrere nel corso del contratto

Per il dimensionamento del servizio di end point protection avanzato il fornitore dovrà considerare quanto segue:

End Point protection				
Descrizione	**Quantità I anno**	**Quantità II anno**	**Quantità III anno**	**Quantità IV anno**
End Point protection (Numero End Point)	**5.000**	**5.000**	**5.000**	**5.000**

** con "I Anno" si intende il primo anno di contratto ovvero i mesi da 4° al 12° del primo anno.*

7.3 Misurazione dei Servizi Supporto

SUPPORTO SPECIALISTCO				
Descrizione	**N° giorni I Anno**	**N° giorni II Anno**	**N° giorni III Anno**	**N° giorni IV Anno**
Supporto specialistico coordinatore - capo progetto	50	50	50	49
Supporto specialistico specialista di tecnologia	479	479	479	479
Supporto specialistico sistemista senior	1.025	1.025	1.025	1.024
Supporto specialistico sistemista	234	234	234	234
Supporto specialistico sistemista junior	62	62	62	63

INTERVENTO FUORI ORARIO				
Descrizione	**N° ore I Anno**	**N° ore II Anno**	**N° ore III Anno**	**N° ore IV Anno**
Interventi fuori orario coordinatore/capo progetto	20	20	20	20
Interventi fuori orario specialista di tecnologia	480	480	480	480
Interventi fuori orario sistemista senior	1.200	1.200	1.200	1.200

7.4 Misurazione dei Servizi di Gestione operativa

Service Desk (SPOC)				
Descrizione	**Quantità I anno**	**Quantità II anno**	**Quantità III anno**	**Quantità IV anno**
Ticket risolti al I° livello	**78.000**	**78.000**	**78.000**	**78.000**
Ticket inoltrati al II° livello	**72.000**	**72.000**	**72.000**	**72.000**
Reperibilità SPOC	**5.500**	**5.500**	**5.500**	**5.500**

Numero di ore annue Extra-Orario SPOC	50	50	50	50

** con "I Anno" si intende il primo anno di contratto ovvero i mesi da 4° al 12° del primo anno.*

Il servizio di Gestione Postazioni di Lavoro è dimensionato sui seguenti parametri. Rimane inteso che il servizio viene remunerato a canone sulla base dell'effettivo numero di PDL gestite, con la richiesta di un dimensionamento minimo del team di gestione coinvolto specificato al par. 8.4.2.

Gestione Postazioni di Lavoro				
Descrizione	**Quantità I anno**	**Quantità II anno**	**Quantità III anno**	**Quantità IV anno**
Numero di PC Desktop/Notebook gestiti	**3.590**	**3.590**	**3.590**	**3.590**

** con "I Anno" si intende il primo anno di contratto ovvero i mesi da 4° al 12° del primo anno.*

7.5 Misurazione di Servizi di sicurezza aggiuntivi rispetto alla conduzione

Vulnerability Assessment dell'Infrastruttura				
Descrizione	**Quantità I anno**	**Quantità II anno**	**Quantità III anno**	**Quantità IV anno**
Vulnerability Assessment dell'Infrastruttura (Indirizzi IP)	**450**	**450**	**450**	**450**

** con "I Anno" si intende il primo anno di contratto ovvero i mesi da 4° al 12° del primo anno.*

Verifica della Vulnerabilità delle Applicazioni Web				
Descrizione	**Quantità I anno**	**Quantità II anno**	**Quantità III anno**	**Quantità IV anno**
Verifica della Vulnerabilità delle Applicazioni Web (Applicazioni gestite)	**15**	**15**	**15**	**15**

** con "I Anno" si intende il primo anno di contratto ovvero i mesi da 4° al 12° del primo anno.*

SOC				
Descrizione	**Quantità I anno**	**Quantità II anno**	**Quantità III anno**	**Quantità IV anno**
EPS	**16.000**	**18.000**	**20.000**	**22.000**

** con "I Anno" si intende il primo anno di contratto ovvero i mesi da 4° al 12° del primo anno.*

Per il calcolo del corrispettivo saranno determinate gli EPS gestiti all'interno del mese.

Per il dimensionamento del CTI si faccia riferimento a quanto descritto nell'Appendice 3 "Contesto Tecnologico e Applicativo".

7.6 Misurazione del servizio di gestione licenze

Per il dettaglio si faccia riferimento a quanto descritto nell'Appendice 3 "Contesto Tecnologico e Applicativo".

Si ricorda che questo servizio ha una durata di 48 mesi.

8. MODALITA' DI ESECUZIONE DELLA FORNITURA

Di seguito vengono descritti:

- orario e modalità di erogazione dei servizi;
- sedi di lavoro;
- modalità di esecuzione dei servizi;
- organizzazione dei gruppi di lavoro;
- presentazione CV;

- affiancamento iniziale;
- trasferimento del know-how a fine fornitura;
- processi di Service Management;
- strumenti di RV a supporto della fornitura;
- centro Servizi per l'operatività da remoto.

8.1 Orario di erogazione dei servizi

La tabella seguente riporta in forma schematica gli orari di erogazione dei servizi, considerato che si intende per:

- **Orario base**: da lunedì a venerdì dalle 08:00 alle 18:00 esclusi i giorni festivi, erogato senza soluzione di continuità. Il Fornitore, pertanto deve garantire il servizio presidio minimo anche durante l'intervallo di pranzo.
- **Orario base esteso:** lunedì-venerdì dalle ore 8.00 alle ore 20.00 esclusi i giorni festivi; sabato dalle ore 8:00 alle ore 14:00.
- **Orario notturno e festivo:** 7 giorni su 7 incluso sabato, domenica e giorni festivi a complemento dell'orario base/orario base esteso.
- **H24:** 7 giorni su 7 incluso sabato, domenica e giorni festivi, 24h su 24h.

Servizio	Tipologia orario
Conduzione operativa sistemi e sicurezza	Orario base
	Reperibilità presidio del data center collocato all'housing: Orario notturno e festivo per le attività di Gestione Sistemi (par 5.1.2)
Servizio di monitoraggio H24	H24
Supporto specialistico a richiesta	Orario base
Interventi fuori orario	Orario notturno e festivo
Service Desk (SPOC)	Orario base esteso Extra-Orario: Orario notturno e festivo
	Reperibilità SPOC: Orario notturno e festivo
Gestione PdL	Orario base
Vulnerability assessment dell'infrastruttura	Orario base
Verifica della vulnerabilità delle Applicazioni Web	Orario base
Threat intelligence	H24
SOC	H24

Gestione licenze	Non applicabile *(i servizi professionali per l'esecuzione del servizio sono considerati erogabili in orario base, la disponibilità delle licenze è H24)*

Tabella 8 - Orario dei Servizi

8.2 Sedi di erogazione dei servizi

La sede principale di erogazione dei servizi è sita in Parco Scientifico Tecnologico VEGA - Edificio Lybra, Porto Marghera (Venezia), mentre il dettaglio delle sedi e del servizio da erogare sono indicate in Appendice 3 Contesto Tecnologico e Applicativo.

Per il servizio di Service Desk, il Fornitore deve operare presso sedi diverse da quelle di RV, purché nel territorio italiano, a condizione che venga garantita la presenza giornaliera presso la sede di Venezia Vega di almeno una risorsa del team allocato sul servizio, a garanzia del corretto interfacciamento con i Responsabili e Referenti dell'Amministrazione e di altri fornitori.

Si evidenzia che il numero degli utenti è pari a 3076 suddivisi come segue:

- VIP 276;
- STANDARD 2800 (utenti che possiedono un PC).

L'aggiornamento del numero degli utenti è oggetto di comunicazione formale da parte di RV al verificarsi di variazioni.

8.2.1 Utilizzo degli spazi di RV e postazioni di lavoro

Il fornitore è tenuto ad implementare una soluzione applicativa per la gestione delle postazioni di lavoro in uso presso RVE, ai fini di prenotazione e monitoraggio delle postazioni. Tale sistema sarà integralmente in carico al fornitore, comprese attività di gestione e mantenimento, includendo quindi aspetti economici e operativi.

La soluzione dovrà, quindi, garantire funzionalità di prenotazione, monitoraggio delle disponibilità e gestione dei flussi di lavoro.

Il sistema dovrà supportare sia la gestione delle postazioni fisse che di quelle temporanee , adattandosi alle necessità mostrate del fornitore stesso.

Dal punto di vista tecnico, il sistema dovrà integrare funzionalità di controllo della saturazione delle postazioni, compresi reminder per il rilascio delle postazioni, riducendo al minimo i tempi di inattività.

Inoltre, dovrà essere prevista la possibilità di generare report sull'utilizzo delle postazioni, permettendo l'ottimizzazione ulteriore della gestione delle risorse tramite l'analisi dei dati raccolti. La piattaforma dovrà essere accessibile tramite autenticazione sicura degli utenti; il fornitore dovrà garantire la continuità del servizio, provvedendo a eventuali aggiornamenti software in ottica di mantenere l'applicazione compliance agli standard di sicurezza, gestendo inoltre eventuali problematiche tecniche che potrebbero comportarne difficoltà nell'utilizzo.

Infine, in caso di necessità di integrazione con altri sistemi aziendali, il fornitore dovrà fornire le soluzioni necessarie per una piena interoperabilità.

Si specifica che la soluzione applicativa rientra nelle attività relative ai servizi di conduzione operativa dei sistemi e sicurezza.

8.3 Modalità di esecuzione dei servizi

Nella tabella seguente, per ciascun servizio, viene riportata la modalità di esecuzione prevista.

Servizio	Modalità di esecuzione
Conduzione operativa sistemi e sicurezza	Continuativa

Servizio di monitoraggio H24 da remoto	Continuativa
Supporto specialistico a richiesta	A richiesta
Interventi fuori orario	A richiesta
Service Desk (SPOC)	Continuativa Extra-Orario: A richiesta Reperibilità SPOC: Continuativa
Gestione PdL	Continuativa
Vulnerability Assessment dell'Infrastruttura	Continuativa
Verifica della Vulnerabilità Applicazioni Web	Continuativa
Threat intelligence	Continuativa
SOC	Continuativa
Gestione licenze	Continuativa

Tabella 9 -Modalità di esecuzione dei servizi

8.3.1 Modello operativo

Entro 1 mese dalla data di avvio del servizi successiva al periodo di subentro/presa in carico, il Fornitore dovrà indicare e presentare in modo dettagliato il modello operativo adottato, specificando in che modo lo stesso si allinea agli standard internazionali riconosciuti (a titolo esemplificativo e non esaustivo: ITIL, ISO 20000, COBIT, etc) e alle normative vigenti, oltre al contributo di tale modello al raggiungimento degli obiettivi strategici di RV e al miglioramento continuo dei servizi; pertanto, dovranno essere indicate almeno le seguenti informazioni:

1. **panoramica del modello operativo**: descrizione generale dell'approccio adottato per la gestione delle operazioni IT, evidenziando come il modello supporti gli obiettivi aziendali e garantisca l'efficienza operativa;
2. **processi implementati**: elenco dettagliato dei processi in uso, delle interrelazioni tra gli stessi indicando ed il contributo offerto;
3. **strumenti e tecnologie impiegati**: indicazione delle piattaforme e degli strumenti impiegati;
4. **ruoli e responsabilità**: descrizione chiara dei ruoli all'interno del team, delineando le responsabilità specifiche per ciascun processo operativo;
5. **metriche e KPI**: descrizione delle metriche chiave e degli indicatori di performance utilizzati per valutare l'efficacia delle operazioni IT.

In ottica di garantire una presentazione chiara e condivisa del modello, la presentazione dello stesso dovrà essere supportata dall'evidenza dell'architettura operativa, ovvero presentando un diagramma o una descrizione dell'architettura operativa, evidenziando le interazioni tra i vari processi e sistemi, includendo esempi di casi pratici o risultati raggiunti in contesti analoghi. Infine, tale modello dovrà essere mantenuto aggiornato.

8.4 Organizzazione dei gruppi di lavoro

Di seguito sono riportate le caratteristiche minime che il Fornitore deve garantire ai fini dell'organizzazione della fornitura.

Si sottolinea che a garanzia dei servizi oggetto del presente documento, il Fornitore, nel rispetto delle pianificazioni, degli SLA e delle caratteristiche di ciascun servizio, deve organizzare i propri gruppi di lavoro al fine di assicurare lo svolgimento delle attività, progetti e/o servizi in parallelo, senza che eventuali spostamenti delle risorse professionali tra servizi penalizzi il risultato da erogare.

Il Fornitore deve, inoltre, garantire un'organizzazione flessibile delle risorse professionali, al fine di far fronte agli eventuali picchi di attività, oltre a compiere gli sforzi necessari al fine di garantire la corretta comunicazione tra i vari team di lavoro, con l'obiettivo di assicurare una gestione più efficace delle criticità e implementazione delle remediation. A tale fine dovrà essere previsto, tra gli altri, il Piano di Comunicazione, assicurando che tutte le parti coinvolte nel progetto (fornitore, cliente, e altre figure interessate) siano adeguatamente informate sugli sviluppi, le decisioni e le problematiche, in modo che possano prendere azioni tempestive ed efficaci; per il dettaglio si rimanda al § 9.2.3 Piano di comunicazione.

Infine, si prevede la possibilità, da parte di RV, di richiedere la rimodulazione dei gruppi di lavoro in base a specifiche esigenze operative e/o organizzative emerse durante il periodo di erogazione del servizio, e che tale attività venga effettuata entro un tempo massimo di 6 mesi dalla richiesta formale di modifica, garantendo la tracciabilità del processo, quindi delle figure precedentemente impiegate, le figure attualmente in sostituzione e le relative motivazioni.

8.4.1 RUAC e Responsabile dei Servizi

Il Fornitore deve indicare, entro 5 giorni dalla data di decorrenza del Contratto:

- Il Responsabile unico delle attività contrattuali (Responsabile del Contratto-RUAC);
- Il Responsabile dei Servizi quale interfaccia unica nei confronti di RV coordinando tutte le attività previste nel presente documento, indipendentemente dall'organizzazione interna del Fornitore, anche in presenza di RTI. Questo ruolo deve essere assegnato dal RUAC del Fornitore alla risorsa di maggiore esperienza che può comunque essere contemporaneamente parte dei team operativi.

Si sottolinea che per entrambi i ruoli, di seguito dettagliati, si richiedono le certificazioni PMI e ITIL 4 practitioner; inoltre, la messa a disposizione del Responsabile dei Servizi e del RUAC non comporta alcun onere aggiuntivo per RV.

Il **RUAC** deve:

- farsi carico della gestione del personale componente i vari gruppi di lavoro (ad esempio ferie, malattie, indisponibilità in genere) al fine di garantire la regolare disponibilità delle risorse nell'orario di servizio. L'organizzazione del Fornitore deve essere tale da garantire l'autonomia delle proprie risorse dall'Amministrazione e pertanto è responsabilità del Fornitore proporre ed aggiornare i piani di presenza e di eventuale turnazione in funzione dello specifico piano di lavoro (copertura in caso di picchi di lavoro, ferie, reperibilità, extraorario, ecc.);
- riferire all'Amministrazione (in funzione delle specifiche competenze) su tutte le attività legate alla corretta esecuzione dei servizi quali, ad esempio, gli adempimenti legati alla qualità, il controllo dell'avanzamento lavori, la verbalizzazione degli incontri con l'utenza, ecc.;
- garantire un costante e adeguato grado di conoscenza e di attenzione delle risorse del Fornitore evitando discontinuità;

Il **Responsabile dei Servizi** (service manager) del Fornitore ha il compito di coordinare e garantire la corretta esecuzione di tutte le attività di propria competenza. In particolare, deve, a titolo esemplificativo ma non esaustivo:

- è responsabile della gestione e risoluzione delle problematiche relative al funzionamento dei servizi digitali su tutto il perimetro di competenza. Hanno il compito di prendere in carico i problemi segnalati, coordinarsi con i fornitori applicativi e di rete, e facilitare le attività necessarie per ripristinare la piena operatività dei servizi.
- garantire la costante e tempestiva comunicazione verso il RUAC;
- garantire le attività di competenza del RUAC nei periodi di assenza temporanea di quest'ultimo (ferie, malattia, ecc.);
- predisporre tempestivamente piani di lavoro e consuntivi attività relativi a ciascun servizio;
- garantire la corretta esecuzione delle attività, nel rispetto di tempi e costi stimati;

- presidiare il corretto funzionamento dei Servizi rispetto alle indicazioni presenti nella documentazione di gara e nell'offerta tecnica;
- interfacciarsi costantemente con RV, al fine di garantire interventi tempestivi di aggiornamento e risoluzione delle problematiche relative alla corretta esecuzione dei servizi.

8.4.2 Composizione minima del presidio

Per garantire un'efficace e tempestiva esecuzione delle attività, la Regione del Veneto richiede che il Fornitore assicuri un numero minimo di risorse dedicate ai servizi di Conduzione Operativa e Gestione delle Postazioni di Lavoro (PDL). (Tabella 10 e Tabella 11)

8.4.2.1 Team di presidio servizi di Conduzione Operativi Sistemi e Sicurezza

In particolare, per quanto riguarda l'organizzazione dei servizi di conduzione operativa sistemi e sicurezza (par 5.1), è richiesta una soluzione organizzativa composta da 42 FTE (come indicato nella Tabella 10), di cui almeno 25 FTE con presidio on-site presso la Regione del Veneto. Sarà a discrezione del Fornitore organizzare eventuali turnazioni interne tra le proprie risorse, al fine di garantire la costante copertura di tutte le attività e servizi durante l'orario di erogazione e prevenire eventuali situazioni di assenza non presidiata, assicurando quindi in ogni momento la piena operatività dei servizi.

Il Fornitore dovrà inoltre garantire la presenza continuativa sia del *Service Manager sia dei Coordinatori-Capo Progetti* presso la sede di servizio, dal lunedì al venerdì, durante l'intero orario di attività (presenza di 8 ore lavorative). La figura sia del Service Manager sia dei Team Leader sono da considerarsi all'interno delle 25 FTE richieste in presidio on site.

Inoltre, le figure professionali di Change Management dovranno garantire la propria presenza in sede presso la Regione del Veneto per almeno il 80% delle giornate lavorative settimanali, dal lunedì al venerdì. Tale percentuale di presenza si intende su base settimanale.

Inoltre, le figure di *Coordinatori-Capo Progetti* di ciascun gruppo dovranno designare preventivamente una risorsa sostitutiva appartenente al medesimo gruppo, con un livello di seniority adeguato, da attivare in caso di assenza del *Coordinatori-Capo Progetti* (es. per malattia, ferie o altri impedimenti), al fine di garantire la continuità operativa del servizio e comunicata all'Amministrazione.

Si specifica che laddove l'andamento degli IQ, ovvero i livelli di servizio non fossero rispettati, RV si riserva di chiedere il rientro nei valori soglia anche mediante una richiesta di variazione di FTE nel team di presidio on site, senza alcun onere aggiuntivo per l'Amministrazione, fatto salvo le variazioni previste al cap 7.

È altresì richiesto che il Fornitore predisponga un *rapportino attività giornaliero,* nel quale siano puntualmente riportate almeno le seguenti informazioni per ogni singola risorsa delle 42 risorse (Tabella 10):

- le riunioni effettuate;
- i ticket lavorati;
- le Change gestite.

La condivisione del rapportino attività giornaliero con RVE deve avvenire una volta a settimana. Eventuali ritardi/ mancanza della consegna dei rapportini, devono essere adeguatamente giustificati all'Amministrazione. Si richiede che il Fornitore proponga un template del rapportino attività giornalieri con successiva approvazione da parte dell'Amministrazione.

La Regione del Veneto, in collaborazione con il monitoraggio contratti, provvederà ad effettuare audit periodici su quanto prodotto e sugli adempimenti contrattuali, al fine di verificarne la coerenza, la qualità e la continuità rispetto ai livelli di servizio attesi.

Per quanto riguarda le competenze e le certificazioni richieste per entrambi i gruppi di lavoro sono riportate nell'**Appendice 2 – Profili Professionali**.
A prescindere dalla struttura organizzativa interna adottata dal Fornitore per l'erogazione dei servizi, è richiesto un elevato livello di sinergia tra le diverse figure professionali coinvolte, al fine di garantire un costante ed adeguato livello di conoscenza, cooperazione e attenzione operativa. È responsabilità del RUAC assicurare tale sinergia.
Inoltre, dovrà essere promossa una forte collaborazione tra le figure appartenenti ai gruppi di lavoro elencati nella tabella seguente.

Nella tabella sottostante è indicata l'organizzazione del gruppo di lavoro per la **conduzione operativa (par 5.1)**:

Figure Professionali							
Gruppo	**Coordinatore-Capo progetto**	**Specialista di tecnologia**	**Sistemista Senior**	**Sistemista**	**Sistemista junior**	**Specialista Cloud**	**Totale risorse**
Service Manager	1						**1**
Architecture design		1					**1**
Project/ Change Management	1		3	3		1	**8**
Security	1	2	2	1	1		**7**
Infrastructure			2	3	1		**6**
Middlleware	1	1	5	2	2		**11**
DBA	2	1	2	1	1		**7**
Quality			1				**1**
Totale conduzione	**6**	**5**	**15**	**10**	**5**	**1**	**42**

Tabella 10 - Composizione team di Conduzione

È richiesto, comunque, di garantire una flessibilità nell'organizzazione per la gestione picchi di attività.

8.4.2.2 Team di presidio servizi di Gestione delle PdL

In merito alla Gestione delle PdL on site (par 5.4.2), l'attività di presidio è richiesta per la sede di Venezia Vega e presso la sede della giunta Regionale (Balbi), dove deve essere previsto un presidio fisso di 2 persone che si alternano a coprire l'intero servizio, inoltre per la sede Grandi Stazioni di Venezia dovrà essere garantito un presidio fisso di 1 persona. Il servizio di postazioni di lavoro deve essere erogato da un team di risorse che abbia in maggioranza figure professionali con esperienza medio-alta, come indicato nella tabella sottostante:

Gestione PdL	**Figura Professionale**			
	Sistemista senior	Sistemista	Sistemista junior	**Totale Risorse**
Numero risorse	3	4	4	11

Tabella 11 - Composizione presidio on site Gestione PDL

Per il Servizio di assistenza di 1° livello, al Fornitore è richiesta la presenza presso RV di una figura di riferimento che

svolga attività di collegamento tra il gruppo di primo livello e gli altri livelli di supporto, oltre che interfacciarsi con i referenti di RV del servizio, per agevolare la soluzione di problematiche urgenti o gestire proposte di miglioramento del servizio.

La stima delle FTE è fatta sulla base del modello di gestione definito nel capitolato, sulla base dell'effort storico per l'erogazione di un servizio di qualità e sulla base del dimensionamento attuale delle PDL di RVE in gestione.

Le risorse sopra menzionate sono intese come FTE. Per il loro calcolo, si considerano 210 giorni lavorativi annui per ciascun FTE.

Il Fornitore dovrà incaricare due referenti dedicati come presidio onsite del servizio SPOC, i quali avranno il compito di gestire operativamente le attività e fungere da punto di riferimento per Regione del Veneto, garantendo il coordinamento e la continuità del servizio.

8.5 Presentazione CV

I curricula professionali nominativi riferiti al Responsabile unico delle attività contrattuali, al Responsabile dei Servizi e alle risorse professionali impiegate nell'esecuzione dei servizi in modalità di esecuzione continuativa, devono essere consegnati entro i primi 10 giorni lavorativi dalla data di sottoscrizione del Contratto.

I CV sono sottoposti a valutazione relativamente alle competenze e certificazioni richieste come requisiti minimi nell'Appendice 2 Profili professionali e alle competenze e certificazioni aggiuntive. Si precisa che i CV nominativi presentati devono essere firmati dall'intestatario del CV.

8.5.1 Certificazioni

A ogni curriculum devono essere allegate le seguenti informazioni:

- descrizione sintetica autocertificata delle attività professionali svolte negli ultimi 24 mesi, contenente l'indicazione del datore di lavoro, l'azienda presso cui si è svolto il servizio, la durata della prestazione e la qualifica professionale ricoperta;
- certificazioni personali (laddove presenti). Per il dettaglio delle certificazioni professionali minime richieste, si rimanda all'Appendice 2 Profili professionali.

Con particolare riferimento alla certificazione delle risorse, dovranno essere necessariamente indicate:

- la data di conseguimento
- data di scadenza delle stesse;

Inoltre, ogni 6 mesi RVE si riserva di effettuare delle verifiche sulle certificazioni delle risorse, tramite la richiesta dei profili con le certificazioni. Possibilità da parte di RVE di effettuare dei colloqui delle risorse dell'organizzazione del fornitore.

8.5.2 Censimento delle risorse

Il Fornitore dovrà curare la predisposizione e l'aggiornamento di un Registro del Personale Esterno riportante (almeno) le seguenti informazioni:

- area di impiego;
- ruolo;
- principali responsabilità;
- data inizio;
- data fine (eventuale);
- motivo sostituzione (eventuale);
- risorsa sostituente (eventuale).

Tale elenco dovrà essere messo a disposizione di RVE, aggiornato alla data della richiesta, tramite un ambiente condiviso.

8.5.3 Sostituzione delle risorse

Nel caso di sostituzione di Risorse in corso di esecuzione del contratto devono essere presentati, per accettazione da parte di RV, i CV delle Risorse inserite, in possesso degli stessi o superiori requisiti delle Risorse da sostituire. RV ha facoltà di rifiutare un CV, secondo quanto specificato in Appendice 1 - Indicatori di qualità e nel Contratto. In caso di sostituzione della risorsa, la fase di training on the job e affiancamento alla risorsa uscente per il passaggio di conoscenze è a carico del Fornitore stesso e a titolo gratuito per RV (i costi, pertanto, relativi alla risorsa entrante non possono essere addebitati a RV).

Parimenti, si dovrà provvedere all'aggiornamento del Registro del Personale Esterno.

Per quanto riguarda la comunicazione della disattivazione dell'account di Regione del Veneto, nel momento in cui, il fornitore comunica le dimissioni della risorsa uscente, è tenuto ad inoltrare, tramite comunicazione formale, la disattivazione dell'account entro l'ultimo giorno lavorativo della risorsa uscente. Qualora il fornitore non lo comunicasse, Regione del Veneto si riserverà di applicare le dovute penali secondo Appendice 1- Indicatori di Qualità.

8.6 Affiancamento iniziale

A partire dalla data di stipula del Contratto di fornitura, il Fornitore deve procedere alla presa in carico dei servizi.

Si specifica che i canoni non si avviano all'avvio del contratto, ovvero nell'affiancamento iniziale ma si avviano al termine della presa in carico.

L'affiancamento iniziale si pone l'obiettivo di permettere il passaggio di consegne tra il Fornitore di servizio uscente e quello entrante e deve avvenire secondo quanto disposto dal presente Capitolato, nonché come eventualmente migliorato nell'offerta tecnica, in termini di logistica, organizzazione, sicurezza, documentazione e quanto altro necessario.

Il personale del Fornitore entrante deve affiancare il personale dell'Amministrazione e/o da terzi indicati dalla stessa, al fine di acquisire le competenze necessarie all'erogazione dei servizi contrattualmente previsti e raggiungere il necessario livello di autonomia operativa.

A tal fine il Fornitore entrante deve organizzare, pianificare e partecipare attivamente alle attività di affiancamento iniziale e acquisizione del know-how, secondo i tempi contrattualmente previsti, nonché predisporre quanto necessario e/o dichiarato in sede di Offerta tecnica per garantire l'efficace presa in carico dei servizi e l'avvio delle attività contrattuali. In questa fase deve provvedere, inoltre, all'installazione e all'avvio operativo degli eventuali strumenti a supporto della fornitura richiesti dall'Amministrazione al § 6.2.

La fase di affiancamento della **durata di 3 mesi** consiste in: riunioni di lavoro, sessioni formative, esame della documentazione esistente con assistenza di personale esperto, affiancamento al personale che eroga i servizi nell'operatività quotidiana, specie sui servizi continuativi.

Le risorse del Fornitore che partecipano all'affiancamento devono essere le stesse che prenderanno in carico i servizi. Il Fornitore deve garantire la presenza di almeno una figura professionale, con adeguati skill per ciascun ambito (es. futuro responsabile del servizio), al fine di garantire la completa presa in carico del servizio.

Gli ambiti sono:

- Infrastruttura;
- Middleware;
- DataBase;
- SPOC;
- PDL;
- Sicurezza.

Modalità e tempi effettivi devono essere concordati e pianificati con l'Amministrazione.

Durante le attività di affiancamento la responsabilità delle operazioni continua ad essere in capo al Fornitore uscente e/o all'Amministrazione. Le attività devono essere svolte in modo da non incidere negativamente sulla conduzione e gestione dei servizi erogati e di limitarne l'impatto sull'operatività dell'Amministrazione stessa.

Nel periodo di allestimento del servizio, che va dalla data di decorrenza contrattuale fino alla data di inizio attività, il Fornitore deve:

- Consegnare il Piano di Subentro comprensivo della pianificazione dettagliata delle richieste attività di affiancamento, esplicitando le risorse professionali ed il loro successivo impiego nei servizi della fornitura, le attività, i tempi e gli strumenti offerti, entro i primi 15 giorni lavorativi dalla data di sottoscrizione del contratto. Per il dettaglio del piano si rimanda al § 9.2.5 Piano di Subentro;
- Consegnare il Piano della Qualità, entro 60 giorni solari dalla data di sottoscrizione del Contratto, con la descrizione dei processi operativi e degli output documentali relativi a ciascuno dei servizi oggetto dell'appalto, con particolare riferimento alle procedure di interazione tra l'Amministrazione (o terzi designati) e Fornitore;
- Predisporre per la consegna, entro il termine fissato dall'Amministrazione, del Piano dei Servizi con tutti i servizi previsti, come indicato al § 9.2.

Durante la fase di presa in carico il Fornitore entrante deve attivare il collegamento in VPN fra la sede di RV e la propria sede operativa, da cui effettuare gli eventuali interventi da remoto.

Nel corso delle attività di presa in carico, le eventuali incompletezze della documentazione ricevuta devono essere segnalate dal Fornitore all'Amministrazione.

La fine delle attività di presa in carico dei servizi viene verbalizzata dai Responsabili del Fornitore e dell'Amministrazione, con evidenza di eventuali segnalazioni da parte del Fornitore entrante e della documentazione riscontrata carente/mancante.

Per tutto il periodo di affiancamento di inizio fornitura, il Fornitore non percepisce alcun corrispettivo per le attività e i servizi oggetto della presa in carico. A partire dalla data di inizio attività cominciano a maturare i corrispettivi previsti per l'erogazione dei servizi.

Nella fase di affiancamento di inizio fornitura, il Fornitore deve effettuare un assessment relativo alla consistenza e coerenza dei dati di asset e delle licenze (non solo relative agli asset) delle relazioni tra gli stessi, sulla base di quanto già in possesso presso RV. L'assessment del Fornitore è sottoposto alla verifica dell'Amministrazione, per verificare eventuali difformità tra il contenuto delle basi dati e l'effettiva configurazione dei sistemi affidati in gestione e provvedere all'eliminazione di tali difformità.

Il Fornitore, entro 2 mesi dalla data di avvio dei servizi successiva al periodo di subentro/presa in carico, deve fornire un rapporto dettagliato sullo 'stato di salute' dei sistemi di RV presi in carico, evidenziando eventuali criticità e/o debolezze riscontrate sulla base di Penetration Test, Vulnerability Assessment e ulteriori test che ritiene opportuno. A seguito di tale attività, deve essere condiviso con RV un remediation plan con l'indicazione di tutte le contromisure necessarie da porre in essere, al fine di eliminare le vulnerabilità eventualmente rilevate (tale attività è remunerata nel canone dei servizi base).

8.7 Trasferimento del know-how a fine fornitura

In prossimità della conclusione del contratto, il Fornitore deve garantire un periodo di almeno 3 mesi di supporto alla transizione verso un nuovo eventuale Fornitore, o alla presa in carico dei servizi da parte dell'Amministrazione. In tale periodo, il Fornitore si impegna a collaborare all'ordinata migrazione di infrastrutture tecnologiche, comprensive dei DBMS utilizzati per il governo della fornitura e l'erogazione dei servizi e al trasferimento delle competenze verso l'Amministrazione o ad un terzo designato dall'Amministrazione, secondo il Piano di Trasferimento.

Il piano di trasferimento deve essere formalizzato almeno 6 mesi prima della data di scadenza del contratto, oppure entro 30 giorni solari successivi alla data di comunicazione dell'evento di cessazione delle attività, oppure entro 15

giorni solari dalla data di richiesta dell'Amministrazione se il trasferimento è richiesto durante il periodo di durata contrattuale; il Piano va sottoposto all'approvazione dell'Amministrazione e deve essere mantenuto aggiornato per tutto il periodo di vigenza contrattuale.

Il Piano di Trasferimento consiste nella redazione di un piano di massima di tipo esecutivo, articolato in attività con l'indicazione di scadenze di inizio e fine, di responsabilità, di contenuti e risultati tali da attivare il "Trasferimento" e da renderne controllabile la sua effettiva attuazione. Deve almeno descrivere:

- I servizi oggetto del trasferimento;
- Le attività previste e le relative modalità di esecuzione;
- I compiti e le responsabilità di ciascuna delle Parti;
- Il programma temporale in base al quale le attività devono essere eseguite;
- I piani di collaudo dei servizi oggetto di trasferimento.

I documenti prodotti dal Fornitore, quali processi e procedure operative, manuali operativi, specifiche di prodotti realizzati nel corso della fornitura, aggiornati alla data di inizio della fase di trasferimento di know how, devono essere consegnati prima dell'avvio di tale fase. Il Fornitore uscente deve rendere disponibile e fruibile tutta la documentazione prevista dalla propria fornitura, prima dell'inizio delle attività di trasferimento di know-how.

Per lo svolgimento del passaggio di consegne suindicato, il Fornitore deve mettere a disposizione un apposito gruppo di lavoro dedicato e opportunamente dimensionato, nonché strumenti organizzativi e tecnologici.

8.8 Processi di Service Management

Al Fornitore è richiesto di assicurare l'erogazione dei servizi secondo un approccio process-driven, in cui la complessa struttura organizzativa/operativa dei servizi sia scomposta in una serie di processi integrati e correlati tra loro in accordo con le best practice ITIL, con l'obiettivo di:

- Migliorare la qualità dei servizi IT;
- Ridurre i costi di erogazione dei servizi;
- Allineare i servizi IT con i bisogni correnti e futuri del business e dei clienti.

Al Fornitore in fase di offerta è richiesto di presentare una propria proposta di descrizione dei processi che su decisione di RV possono essere recepiti e/o modificati ed adottati nel corso della fornitura.

La descrizione dei processi deve indicare il modello di funzionamento, gli attori coinvolti, la documentazione che si prevede di rilasciare e le modalità di interazione-comunicazione-escalation.

I processi da descrivere riguardano i seguenti aspetti:

Service Operation

- **Event Management:** è il processo responsabile della gestione degli eventi, ovvero fornire una base solida per il monitoraggio ed il controllo operativo oltre ad individuare gli eventi, identificarli, comprenderne cause e conseguenze ed intraprenderle opportune azioni di controllo.
  L'evento è definito come un cambio di stato che ha rilevanza ai fini della gestione di un Configuration Item o di un servizio IT. Un evento potrebbe indicare un malfunzionamento di una parte dell'infrastruttura e, quindi, essere un trigger per la generazione di un incidente. Gli eventi, comunque, possono anche indicare un andamento normale delle attività oppure la finalizzazione di un intervento di routine.
- **Incident Management:** l'obiettivo del processo di incident management è la gestione del ciclo di vita delle attività necessarie per ripristinare le operazioni normali di servizio il più velocemente possibile con la minima

interruzione di servizio al business, assicurando che i migliori livelli di servizio e disponibilità siano mantenuti.

- **Request Fullfillment:** gli obiettivi di questo processo sono di fornire agli utenti un canale per richiedere (e ricevere) servizi standard per i quali esiste uno schema predefinito di approvazione.
- **Problem Management:** l'obiettivo del Problem Management è di minimizzare l'impatto sul business degli incidenti e dei problemi causati da errori nell'infrastruttura IT, e di prevenire la ricorrenza di tali incidenti. Per poter raggiungere questo obiettivo, il Problem Management cerca di determinare la "root cause" (causa ultima) degli incidenti, e focalizza la propria attenzione a migliorare o correggere queste situazioni.
- **Access Management:** gli obiettivi di questo processo sono di fornire agli utenti i diritti per usare uno o più servizi ed eseguire le politiche definite nei processi di Availability e Security Management.

Service Transition

- **Change Management:** l'obiettivo del processo di Change Management è l'utilizzo di metodi e procedure standardizzate per una efficiente e rapida gestione di tutti i cambiamenti all'infrastruttura, con lo scopo di minimizzare l'impatto di possibili incidenti correlati sui servizi IT.
- **Service Asset and Configuration Management:** l'obiettivo del Configuration Management è di fornire un modello logico dell'infrastruttura attraverso l'identificazione, il controllo, la gestione e la verifica di tutte le versioni di "Configuration Items" esistenti.
- **Release and Deployment Management:** l'obiettivo del processo di Release Management è la pianificazione e il coordinamento delle implementazioni di software nuovi (o di upgrade) con hardware e documentazione associati, attraverso il coordinamento con il Change Management per validare l'esatto contenuto della release e assicurando che tutti gli item oggetto (o target) di implementazione siano tracciabili via CMDB.
- **Knowledge Management:** lo scopo principale di questo processo è di assicurare che le giuste informazioni siano disponibili a chi deve prendere delle decisioni, migliorando l'efficienza e la qualità nella fornitura dei servizi mediante un prodotto/strumento a sé stante, o come add-on del prodotto già in essere, offerto dal Fornitore.

Service Design

- **Service Level Management:** l'obiettivo del processo di Service Level Management è mantenere e gradualmente migliorare la qualità dei servizi IT, attraverso un ciclo costante di accordi, monitoraggio, reporting, e revisione degli "achievement" dei servizi IT e attraverso l'implementazione di azioni per eliminare livelli di servizio inaccettabili. In particolare, il Service Level Management assicura che i target di qualità del servizio siano documentati in Service Level Agreements (SLA) e si occupa di monitorare il raggiungimento di tali target e di migliorare i servizi (ove possibile), nel rispetto dei limiti di costo esistenti.
- **Capacity Management:** l'obiettivo del processo di Capacity Management è di comprendere i futuri requisiti aziendali, le operazioni dell'organizzazione, l'infrastruttura informatica e garantire che tutti gli aspetti relativi alle prestazioni e alle capacità attuali e future siano forniti in maniera "cost effective". Le principali attività del Capacity Management sono l'analisi, il disegno, la realizzazione ed il monitoraggio, attraverso un processo iterativo. Le aree su cui principalmente si focalizza sono il Service Capacity Management, ovvero la gestione delle prestazioni dei servizi IT erogati e il Resource Capacity Management, ovvero la gestione delle risorse dell'infrastruttura IT.
- **Availability Management:** l'obiettivo del processo di Availability Management è garantire un livello di disponibilità dell'infrastruttura IT adeguato affinché l'organizzazione possa raggiungere i propri obiettivi di servizio. Il processo di Availability management deve considerare il problema della disponibilità sia dal punto di vista del componente dell'infrastruttura che dal punto di vista del servizio e quindi dell'utente finale.

Fondamentale per l'implementazione di un sistema di Availability Management è la creazione di un piano di Availability, focalizzato sia sui processi che sui metodi che sulla tecnologia.

- **IT Service Continuity Management:** l'obiettivo del processo di IT Service Continuity Management è di supportare il processo di Business Continuity Management assicurando che i servizi IT possano essere ripristinati in tempi e modi predeterminati, attraverso la valutazione delle differenti opzioni di IT Service Continuity e la selezione di quelle più opportune in base alle necessità del business (e quindi del Business Continuity Plan), la creazione del piano di IT recovery e l'identificazione di ruoli e responsabilità nell'ambito del piano di IT recovery in particolare e di ITSCM in generale.
- **Information Security Management:** l'obiettivo del processo di Gestione della sicurezza delle informazioni (Information Security Management o ISM) è di allineare la sicurezza delle informazioni alla sicurezza attesa dal business ed assicurarsi che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi.

9. GOVERNO DELLA FORNITURA

Di seguito vengono descritti gli elementi principali che caratterizzano il governo della fornitura richiesta.

9.1 Prodotti della fornitura

La fornitura oggetto del presente contratto riguarda l'erogazione di servizi di system management necessari per garantire la gestione, il mantenimento e l'ottimizzazione dell'infrastruttura tecnologica di RV.

Nel corso della vigenza contrattuale il Fornitore deve produrre e consegnare deliverable relativi ai diversi servizi/attività gestite, siano essi di pianificazione, di consuntivazione delle attività o risultato di specifiche attività/processi di lavorazione in conformità agli standard di qualità definiti nel presente capitolato e in linea con le migliori pratiche di settore.

Nella tabella sottostante sono elencati i documenti contrattuali che il Fornitore deve realizzare con le rispettive date di scadenza, dei quali, in fase di avvio delle attività, RV si riserva di meglio dettagliare i contenuti.

Prodotto	Termine	Mezzo di invio a RV
Curriculum vitae risorse/certificazioni risorse	Entro i primi 10 giorni lavorativi dalla data di sottoscrizione del Contratto. Una volta all'anno aggiornamento e condivisione tra Fornitore e Amministrazione. In caso di sostituzione o integrazione di risorse, almeno 10 giorni prima della presa di servizio della nuova risorsa sulle attività del contratto.	Email o Email PEC
Piano dei Servizi (Piano di Lavoro)	Entro i primi 15 giorni lavorativi dalla data di sottoscrizione del Contratto	PEC
Piano di Subentro	Entro i primi 15 giorni lavorativi dalla data di sottoscrizione del Contratto	PEC
Report baseline fornitura	Entro i primi 20 giorni lavorativi dalla data di avvio del servizio (ovvero dalla data di termine del subentro). Aggiornato due volte all'anno	Email o Email PEC
Portale della fornitura	Entro i primi 35 giorni lavorativi dalla data di sottoscrizione del contratto.	PEC

Prodotto	Termine	Mezzo di invio a RV
Piano di comunicazione	Entro i primi 40 giorni lavorativi dalla data di sottoscrizione del contratto.	Email o Email PEC
Piano della Qualità	Entro 60 giorni solari dalla data di sottoscrizione del Contratto	PEC
Stato Avanzamento lavori	Entro il quinto giorno lavorativo del mese successivo a quello di riferimento	Email o Email PEC
Specifiche preliminari	Entro il primo mese dell'anno devono essere condivise tra fornitore e amministrazione le SP valide per l'anno in corso. L'esigenza di nuove SP nate nel corso dell'anno devono essere condivise tra fornitore e Amministrazione almeno 1 mese prima dell'inizio dell'erogazione dell'attività.	Email o Email PEC
Piano di Trasferimento	120 giorni solari prima della data di scadenza del Contratto, e comunque entro la data di avvio del subentro nuovo fornitore.	PEC

Tabella 12 - Prodotti della fornitura

Per quanto attiene la documentazione il fornitore deve garantire la qualità in termini di:

- Accuratezza
- Attualità
- Coerenza
- Completezza
- Consistenza

Per maggiori dettagli su queste caratteristiche si rinvia alla ISO 25024.

9.2 Pianificazione

9.2.1 Piano dei Servizi

Le attività richieste devono essere svolte in affiancamento e a supporto dell'Amministrazione collaborando con i Referenti di RV dei vari servizi, secondo le modalità opportunamente concordate ad avvio fornitura. Entro 15 giorni lavorativi dalla data di inizio attività, il Fornitore deve consegnare, il Piano dei Servizi (Piano di Lavoro) contenente la descrizione di tutte le componenti della fornitura, in modo tale da consentire il controllo in ogni momento dello stato reale di esecuzione. In particolare, il Piano dei Servizi deve contenere i piani operativi inerenti all'attività previste suddivise per tipo di servizio, una volta concordate con RV, i tempi necessari al completamento delle singole attività, le responsabilità e le risorse associate alle attività, le milestone, gli eventuali deliverable, stima dell'intervento, ove applicabile. Successivamente il Piano dei Servizi viene verificato da Amministrazione e dal Team di monitoraggio ed aggiornato con frequenza almeno trimestre. Gli eventuali aggiornamenti devono essere resi noti a RV e al team di monitoraggio entro 5 lavorativi dall'ultimo giorno lavorativo del trimestre di riferimento. In ogni caso è cura del Fornitore consegnare un aggiornamento del Piano dei Servizi al verificarsi di una variazione significativa nei contenuti.

Qualora non venisse comunicato dal Fornitore a RV un aggiornamento del Piano dei Servizi durante il corso dei trimestri, verranno adottate le azioni contrattuali di cui al par 9.4.1 Rilievi.

Qualsiasi modifica al piano, deve essere approvata formalmente dall'Amministrazione tramite PEC.

In nessun caso l'approvazione potrà avvenire per tacito assenso a meno di specifiche indicazioni sulle tempistiche indicate dall'Amministrazione.

9.2.2 Piano della Qualità

La struttura ed i requisiti minimi del Piano della Qualità vengono descritti di seguito:

Nella redazione del piano il Fornitore terrà come guida lo schema di riferimento di seguito descritto.

1. Scopo del piano della qualità (elenca le motivazioni e le peculiarità dell'obiettivo per le quali è richiesto il documento)
2. Documenti applicabili e di riferimento
3. Ruoli e Responsabilità di riferimento
4. Cicli di vita (descrive i cicli di vita, l'eventuale deroga a quello previsto dal piano di qualità generale, le fasi/sprint in cui sono suddivisi, i criteri di uscita, l'insieme della documentazione da produrre ed eventualmente le attività richieste al Fornitore per il collaudo/accettazione).
5. Metodi, tecniche e strumenti specifici dell'obiettivo (Contiene l'indicazione dei metodi, delle tecniche, degli strumenti, degli standard di prodotto specifici dell'obiettivo solo se diversi da quelli descritti nel Piano della Qualità generale).
6. Indicatori di qualità specifici dell'obiettivo (Contiene gli attributi di qualità con riferimento alle metriche, ai valori limite -Valore di soglia- definiti negli indicatori di qualità e gli eventuali ulteriori indicatori specifici per il Contratto Esecutivo, se diversi da quelli descritti nel Piano della Qualità generale).
7. Riesami, verifiche e validazioni (Contiene l'elenco dei controlli da effettuare (riesami, test, verifiche e validazioni, valutazioni, ecc.) per l'obiettivo e le modalità di esecuzione dei controlli comprensive sia degli strumenti da utilizzare e sia della modulistica di rendicontazione dei risultati, se diversi da quelli descritti nel Piano della Qualità generale).

Il fornitore dovrà mantenere i propri Piani di qualità aggiornati allo stato della tecnologia, di automazione, misurazione e controllo. Il RUAC è responsabile della piena applicazione ed aggiornamento del Piano di Qualità.

9.2.3 Piano di comunicazione

Il Piano di comunicazione è un documento che definisce le modalità e le tempistiche con cui le informazioni vengono gestite, condivise e diffuse durante la durata di un contratto. Questo piano assicura che tutte le parti coinvolte nel progetto (fornitore, cliente, e altre figure interessate) siano adeguatamente informate sugli sviluppi, le decisioni e le problematiche, in modo che possano prendere azioni tempestive ed efficaci.

Questo piano diventa cruciale per garantire che le operazioni, le modifiche e i problemi tecnici vengano comunicati tempestivamente e in modo chiaro, riducendo al minimo i rischi di incomprensioni o malintesi.

La struttura del Piano di comunicazione dovrà contenere i seguenti elementi:

1. Introduzione
    - Scopo: Una descrizione del motivo per cui è stato creato il piano e degli obiettivi che si intendono raggiungere tramite le comunicazioni.
    - Definizione delle parti coinvolte: Elenco delle persone, gruppi e organizzazioni che parteciperanno alla comunicazione.
2. Obiettivi della comunicazione
    - Definizione degli obiettivi specifici delle comunicazioni, ad esempio garantire la chiarezza nelle informazioni, mantenere la trasparenza, e assicurare che le comunicazioni siano tempestive e adeguate.
3. Stakeholder (Partecipanti)
    - Elenco delle figure coinvolte nella comunicazione con indicazione dei loro ruoli e delle informazioni di contatto.

- Identificazione dei livelli di responsabilità per ciascun stakeholder.

4. Tipologie di comunicazioni
   - Descrizione dei vari tipi di comunicazioni che saranno utilizzate, ad esempio:
     - Comunicazioni periodiche,
     - Comunicazioni urgenti (gestione di emergenze o problemi critici),
     - Comunicazioni informali (riunioni ad hoc, aggiornamenti via email),
     - Comunicazioni ufficiali (documenti formali, contratti, modifiche contrattuali).
5. Canali di comunicazione
   - Dettaglio dei canali attraverso i quali avverranno le comunicazioni, come email, riunioni virtuali, videoconferenze.
6. Ruoli e responsabilità
   - Descrizione di chi è responsabile per la creazione, approvazione e distribuzione di ciascun tipo di comunicazione e chi ha il compito di ricevere determinate informazioni.
7. Gestione delle modifiche
   - Un piano che descrive come verranno gestite le modifiche alle comunicazioni durante il corso del progetto, con indicazioni su come informare i vari stakeholder di eventuali cambiamenti nei piani o nelle tempistiche.

Il fornitore è obbligato a fornire il Piano di comunicazione come parte della documentazione prevista. Questo implica che il fornitore dovrà:

- Preparare e condividere un piano di comunicazione entro 40 giorni lavorativi dalla data di sottoscrizione del contratto
- Assicurarsi che tutte le parti coinvolte nel progetto siano informate sulle modalità e tempistiche delle comunicazioni
- Garantire che i canali di comunicazione siano adeguati e che le informazioni vengano diffuse correttamente.

9.2.4 Stato Avanzamento Lavori (SAL)

Il fornitore dovrà condividere con l'Amministrazione la sezione relativa allo stato di avanzamento dei lavori, fornendo indicazioni, attraverso un format approvato da RVE, sulle attività concluse ed in corso, esplicitando la percentuale di avanzamento, su eventuali rischi/criticità/ritardi, su eventuali impatti dei rischi/criticità, su azioni di recupero e razionali dello scostamento, sulle attività in servizio esteso ed in reperibilità. A titolo esemplificativo, di seguito alcuni punti che devono emergere dal documento:

- Attività concluse, in progress, non ancora iniziate ma in perimetro nel mese corrente
- Milestone relative alle attività concluse, in progress, non ancora iniziate ma in perimetro nel mese corrente (Gantt di progetto)
- Evidenza delle attività critiche, identificando le cause delle criticità
- Risorse impegnate per ogni singola attività (nome, cognome, azienda di appartenenza, ruolo, cluster)
- Ore/GG delle risorse impegnate per ogni singola attività
- Livelli di servizio del mese corrente (dare evidenza dei dati di sintesi ma anche di dettaglio)
- Rendicontazione/fatturazione

Il documento deve essere inviato via PEC all'Amministrazione entro 5 giorni lavorativi del mese successivo a quello di riferimento.

Qualora non venisse condiviso all'Amministrazione entro tale data, verranno adottate le azioni contrattuali di cui al par 9.4.1 Rilievi.

Lo stato avanzamento lavori dovrà essere verificato dall'Amministrazione e dal team di monitoraggio e successivamente dovrà essere approvato tramite firma digitale dal DEC e dagli assistenti al DEC.

In nessun caso l'approvazione potrà avvenire per tacito assenso a meno di specifiche indicazioni da parte dell'Amministrazione.

L'approvazione del SAL mensile da parte del DEC di RV costituisce il riconoscimento delle attività svolte da parte del Fornitore e, ove presenti, della verifica del rispetto dei livelli di servizio. Il DEC, al fine dell'approvazione, può avvalersi del supporto dei diversi Assistenti DEC direttamente impegnati nel coordinamento di specifici servizi. Con cadenza trimestrale i SAL approvati dal DEC vengono formalmente approvati dal RUP ai fini dell'autorizzazione alla fatturazione.

E' diritto dell'Amministrazione programmare incontri periodici di SAL sull'avanzamento complessivo del contratto, sull'avanzamento di specifici servizi. E' fatto obbligo al fornitore la partecipazione agli incontri con la presenza del personale necessario per lo specifico argomento e scopo del SAL (es. RUAC e Responsabile del Servizio durante i SAL di contratto, eventuali altri referenti in caso di focus su specifici sottoservizi o argomenti). Il fornitore dovrà predisporre i contenuti di discussione e procedere alla verbalizzazione.

Fatte salve eventuali esigenze di urgenza, escalation, criticità o accordi tra le parti, i SAL saranno programmabili con almeno 2 settimane di anticipo rispetto alla data di incontro e avranno una frequenza almeno trimestrale (ovvero RV si riserva di chiedere una maggiore frequenza).

Il fornitore è comunque obbligato a partecipare con il personale designato anche agli incontri periodici di programmazione e gestione attività ordinarie (es. CAB) o eventuali altri incontri di coordinamento e indirizzo attività programmati dai referenti del servizio di RV.

9.2.5 Piano di Subentro

La fase di subentro si sviluppa dalla data di efficacia del contratto fino alla data di effettiva presa in carico della gestione dei sistemi da parte del Fornitore e si pone l'obiettivo di permettere il passaggio di consegne tra la struttura di servizio precedente all'efficacia del contratto e la nuova. La durata di tale fase è fissata entro i primi 15 giorni lavorativi dalla data di sottoscrizione del contratto, salvo diversa indicazione dell'Amministrazione. La fase di subentro prevede in generale le seguenti attività principali:

- Affiancamento e gestione transitoria iniziale: affiancamento al/ai gestori dei servizi oggetto del contratto (Strutture organizzative dell'Amministrazione e/o ai fornitori in scadenza di contratto).
- Predisposizione del piano generale della fornitura e del piano di subentro e startup, in linea con le linee guida definite dall'Amministrazione nel Piano dei fabbisogni o nella Richiesta di Offerta.
- Acquisizione della documentazione, degli standard, linee guida e metodologie in uso presso l'Amministrazione. - Eventuale predisposizione dei collegamenti telematici e di rete con l'Amministrazione, propedeutici all'attivazione del servizio di Monitoraggio H24 remoto;
- Eventuale avvio della predisposizione e configurazione degli strumenti operativi a supporto della fornitura previsti dal contratto.

Le attività di subentro, effettuate prima della presa in carico dei servizi (quando la responsabilità di gestione sono ancora in capo al fornitore uscente e/o all'Amministrazione) sono a carico del Fornitore, senza alcun onere aggiuntivo per l'Amministrazione. Tutte le attività di subentro dovranno essere avviate entro 5 giorni dalla data di efficacia del contratto ed eseguite secondo le tempistiche concordate con l'Amministrazione nel Piano di Subentro.

Gli obiettivi principali del piano di subentro sono:

- **Garantire la continuità operativa**: Assicurarsi che i servizi continuino a essere forniti all'amministrazione senza interruzioni o disservizi.

- **Assicurare il passaggio delle risorse**: Trasferire correttamente risorse umane, documentazione, tecnologie e conoscenze dal fornitore uscente al subentrante.
- **Proteggere gli interessi dell'Amministrazione**: Tutelare gli interessi dell'amministrazione attraverso un processo chiaro, trasparente e ben documentato.
- **Minimizzare i rischi di operazioni incomplete o errate**: Gestire i rischi legati al passaggio di funzioni critiche e risorse, evitando disguidi operativi e legali.

Il Piano di Subentro, distinto per servizio e deve contenere il dettaglio delle attività che devono essere espletate ad inizio contratto, la relativa tempificazione e le stime di impegno.

In particolare, dovranno essere esplicitate le risorse professionali ed il loro successivo impiego nei servizi, le attività, i tempi, gli strumenti offerti e quanto necessario al:

- subentro: ossia alla completa presa in carico di tutti i servizi;
- set-up: predisposizione degli ambienti, degli strumenti, delle soluzioni, dei sistemi e delle migliorie offerte (obbligatorio).

Per le risorse impiegate nei servizi a carattere continuativo e per tutti i referenti dovranno essere forniti i relativi Curricula Vitae.

Coerentemente con le caratteristiche offerte dal Fornitore e concordate con l'Amministrazione, il Piano riporterà:

- Codice, nome, descrizione delle attività di set-up e di subentro;
- Prodotti delle singole attività;
- Nominativo dei referenti delle attività;
- Puntamento ai paragrafi dell'offerta tecnica in cui l'attività è richiesta;
- Impegno in GGP, stimato ed effettivo, suddiviso per mese e figura professionale, ove applicabile;
- Gantt delle attività, contenente:
  - date di inizio e fine, previste ed effettive, delle singole attività;
  - date di consegna, previste ed effettive, dei singoli prodotti;
  - date di consegna, previste ed effettive;

Per la parte di stato di avanzamento le informazioni da riportare riguardano:

- Data a cui si riferisce lo stato di avanzamento;
- Percentuale di avanzamento delle singole attività;
- Razionali di ripianificazione, preventivamente concordate con la Amministrazione, scostamento
- eventuale delle date, dell'impegno e del volume;
- Vincoli/criticità e relative azioni da intraprendere e/o intraprese.

Allegato al piano dovrà essere sempre presente il Rendiconto Risorse.

9.2.6 Piano di Trasferimento

Entro 120 giorni solari dal termine di validità del contratto, o nel caso di cessazione anticipata del rapporto contrattuale, il Fornitore è tenuto, su richiesta dell'Amministrazione, a consegnare il piano di trasferimento e pianificare le attività da svolgersi negli ultimi 3 mesi di validità contrattuale. In questi mesi, il Fornitore dovrà quindi, in parallelo con i servizi richiesti dal capitolato, effettuare il passaggio di tutte le conoscenze relative alla presente fornitura all'Amministrazione o a terzi da questa indicati. Il Fornitore è pertanto obbligato a redigere e rispettare il Piano di trasferimento di know-how approvato dall'Amministrazione.

Inoltre il fornitore subentrante, su richiesta della Amministrazione, dovrà poter affiancare il personale del Fornitore

uscente nell'operatività quotidiana. La responsabilità dell'esecuzione dei servizi e del raggiungimento dei livelli di servizio contrattuali continuerà ad essere in capo al Fornitore uscente. Si precisa che, qualora alcuni servizi siano espletati presso le proprie sedi, il Fornitore è tenuto ad ospitare, senza nessun onere aggiuntivo, il personale designato dall'Amministrazione. L'aggiornamento della documentazione prevista dal piano di qualità generale e specifico, essendo prodotti obbligatori dei servizi oggetto della presente fornitura, dovrà essere effettuato dal fornitore uscente senza alcun onere aggiuntivo per l'Amministrazione. I documenti aggiornati dovranno essere consegnati sei mesi prima del periodo di fine erogazione servizi e, per le ultime attività, prima dell'inizio della fase di erogazione del trasferimento di know-how. Le attività di trasferimento del know-how si intendono comprese nel corrispettivo dei servizi, fatta salva la facoltà, ove l'Amministrazione lo reputi necessario, di richiedere al Fornitore di integrare i team impegnati nell'erogazione del servizio di Presidio operativo con ulteriori risorse da individuare nell'ambito del servizio di Supporto Specialistico, riconoscendo al Fornitore stesso un effort aggiuntivo per il trasferimento di know-how, fermo restando il corrispettivo massimo complessivo del contratto.

Il Piano dovrà contenere una presentazione esaustiva degli aspetti organizzativi, amministrativi e tecnici della fornitura, dei processi di riferimento, dell'architettura generale del sistema.

Si dovrà prevedere:

- Consegna della documentazione della fornitura prevista dal contratto:
  - dettaglio dei processi organizzativi, tecnici e amministrativi adottati,
  - descrizione dei ruoli chiave e delle responsabilità operative durante il contratto, architettura generale del sistema, inclusi schemi logici e fisici.
  - Manuali operativi e procedure.
  - Documentazione tecnica (progetti, architetture, configurazioni).
  - SLA e reportistica storica.
- Consegna di una base di conoscenza aggiornata, comprensiva di FAQ, casi risolti e best practice.
- Verifica congiunta della completezza e accuratezza dei documenti consegnati.
- Elenco e configurazione degli strumenti software/hardware impiegati, inclusi licenze e accessi.
- Predisposizione di quadri di sintesi architetturali a livello generale: predisposizione di mappe architetturali generali e specifiche per ogni componente, schema dei flussi di integrazione tra i sistemi (API, database, processi).
- Predisposizione di questionari e sessioni di domande/risposte per verificare il grado di apprendimento sugli ambienti tecnologici;
- Presentazione degli aspetti di criticità di ogni servizio/applicazione con l'esposizione chiara delle soluzioni proposte ed attuate durante la fornitura;
- Creazione di un rapporto finale che certifichi il completamento delle attività di trasferimento del know-how e che venga approvato dall'ente e dal fornitore subentrante.

Inoltre, coerentemente con le caratteristiche del know how da trasferire, il Piano riporta:

- Codice, nome, delle attività di trasferimento di know how;
- Prodotti delle singole attività;
- Impegno in GGP, stimato ed effettivo, ove applicabile, suddiviso per mese e figura professionale;
- Gantt delle attività, contenente:
  - date di inizio e fine, previste ed effettive, di ogni attività;
  - date di consegna, previste ed effettive, di ogni prodotto.

Per la parte di stato di avanzamento le informazioni da riportare riguardano:

- Data a cui si riferisce lo stato di avanzamento;
- Percentuale di avanzamento delle singole attività;
- Razionali di ripianificazione, scostamento eventuale delle date, dell'impegno e del volume;
- Vincoli/criticità e relative azioni da intraprendere e/o intraprese.

Allegato al piano dovrà essere sempre presente il Rendiconto Risorse.

9.2.7 Report baseline fornitura ed attività di inventariato

L'attività di gestione dell'inventario degli asset ha l'obiettivo di rendere disponibile e mantenere aggiornata, durante tutta la durata della fornitura, una base informativa completa e dettagliata del parco macchine in servizio presso l'Amministrazione e gestite dal Fornitore. Tali informazioni devono evidenziare sia gli aspetti logistici e amministrativi, che quelli di configurazione hardware e software. Il Fornitore deve effettuare un censimento iniziale di tutte le risorse da gestire nell'ambito del servizio, presenti nelle sedi dell'Amministrazione indicate in Appendice 3 Contesto Tecnologico e Applicativo, oltre che il censimento delle giacenze delle apparecchiature e degli altri beni materiali eventualmente presenti nel magazzino. Il censimento deve essere completato al massimo entro i primi 20 giorni lavorativi dalla data di avvio del servizio (ovvero dalla data di termine del subentro dalla data di avvio del servizio (ovvero dalla data di termine del subentro e l'esito deve essere consegnato tramite email o email PEC all'Amministrazione.

Il report deve descrivere lo stato attuale delle baseline e deve riportare almeno le seguenti informazioni:

- baseline di partenza;
- baseline aggiornata.
- Data;
- eventi che hanno determinato l'aggiornamento

Oltre alle informazioni sopracitate, il report degli asset condiviso con l'Amministratore deve avere le seguenti informazioni minime:

Server/Database

- Nome Virtual Machine
- Descrizione
- Ambiente (staging, collaudo, produzione)
- Data Creazione della Virtual Machine

Storage

- Tipologia storage
- SITO/Marca/Modello
- Data installazione
- Quantità

Apparati sicurezza

- Nome apparato sicurezza
- Fisico
- Virtuale

Si richiede che il fornitore condivida con l'Amministratore il report della baseline 2 volte all'anno. Qualora non venisse consegnato, verranno adottate le azioni contrattuali di cui al par 9.4.2 Penali.

Qualsiasi aggiornamento al report, deve essere comunicata ed approvata formalmente dall'Amministrazione tramite

email e/o eventualmente in riunione

In nessun caso l'approvazione potrà avvenire per tacito assenso a meno di specifiche indicazioni sulle tempistiche indicate dall'Amministrazione.

9.2.8 Curriculum vitae risorse/certificazioni risorse

Il presente capitolo stabilisce i requisiti per la presentazione del curriculum vitae (CV) delle risorse umane che il Fornitore si impegna a mettere a disposizione per l'esecuzione del servizio oggetto della gara. La qualità, l'esperienza e le competenze delle risorse assegnate rappresentano un elemento fondamentale per il successo del progetto e per il rispetto dei tempi e degli standard di qualità richiesti dall'Amministrazione.

Il Fornitore dovrà presentare un elenco dettagliato delle risorse che saranno impegnate nel progetto, specificando per ciascuna:

- Nome e cognome.
- Ruolo specifico e responsabilità all'interno del progetto.
- Qualifiche professionali (titoli di studio).
- Esperienza professionale rilevante per il progetto (inclusi progetti simili).
- Eventuali competenze aggiuntive (lingue parlate, software utilizzati, ecc.).
- Certificazioni delle risorse (È preferibile che le risorse siano in possesso di certificazioni professionali specifiche per il settore, come ad esempio ITIL, PMP, ISO 9001, o altre pertinenti, si veda Appendice 2 Profili Professionali

Il fornitore dovrà indicare il numero complessivo di risorse che saranno coinvolte nei vari servizi, suddivise per competenze specifiche, e descrivere brevemente il ruolo e le responsabilità di ciascuna risorsa.

Il fornitore dovrà caricare nel portale della fornitura i CV delle risorse coinvolte nelle attività progettuali e dovrà aggiornarli una volta all'anno, in caso di modifiche significative nelle competenze o nell'esperienza lavorativa, e fornire tali aggiornamenti all'amministrazione tramite email o email PEC.

L'amministrazione, a cadenza semestrale, si riserva la facoltà di richiedere sia i CV sia le certificazioni delle risorse al fornitore per verificare la correttezza delle informazioni.

Tutte le certificazioni delle risorse devono essere valide secondo la validità di ogni certificazione.

Durante la verifica da parte dell'Amministrazione, qualora le certificazioni fossero scadute e non rinnovate, l'amministrazione si riserverà la facoltà di applicare eventuali penali.

Modalità di presentazione

I CV delle risorse devono essere inviati in formato elettronico (PDF) Europeo e dovranno rispettare i seguenti requisiti:

- Ogni CV dovrà essere redatto in lingua italiana o, qualora specificato, in lingua inglese.
- I CV dovranno essere strutturati in modo chiaro, con evidenza dei punti di forza e delle esperienze più rilevanti.
- Il Fornitore dovrà attestare che tutte le informazioni contenute nei CV sono veritiere e che le risorse dichiarate sono effettivamente disponibili per il progetto.

Nel caso di sostituzione di Risorse, si veda par. 8.5.3 Sostituzione delle risorse

9.2.9 Specifiche preliminari

Le specifiche preliminari si riferiscono a un documento o a una fase in cui vengono definite le linee guida e le caratteristiche di un progetto, prima che inizi la progettazione dettagliata o l'esecuzione. All'inizio dell'anno, con cadenza annuale, il Fornitore e l'Amministrazione devono concordare le attività progettuali per l'intero anno solare.

Il documento deve essere redatto secondo standard regionali e deve seguire le seguenti linee guida:

- **Overview generale**
  - Titolo del progetto o servizio: Il nome del progetto
  - Riferimenti normativi: Eventuali normative e leggi che disciplinano l'appalto o il progetto (ad esempio, il Codice degli Appalti).
  - Descrizione del contesto e degli obiettivi: Una panoramica che descrive il progetto, inclusi gli scopi generali e gli obiettivi da raggiungere.
  - Obiettivi
  - Contesto generale
- **Requisiti (funzionali, tecnologici, prestazionali e di sicurezza)**
- **Soluzione**
- **Risorse coinvolte**
- **Tempistiche e scadenze**: La durata prevista per la realizzazione o la fornitura. Questo potrebbe includere una cronologia con le principali fasi del progetto. (es. Gaant di progetto)
- **Stima e valutazione economica:** importo economico gg/u per le attività sopra descritte

Inoltre all'interno dello Stato avanzamento lavori (SAL), dovrà esserci un capitolo destinato alle SP.

Approvazione delle specifiche preliminari

Una volta che il Fornitore condivide con l'Amministrazione il documento relativo alla specifica preliminare di un progetto, l'Amministrazione procede con le verifiche interne. Successivamente il DEC e gli assistenti al DEC procederanno con l'approvazione tramite firma digitale. Qualora mancasse anche solo la firma tra il DEC e gli assistenti al DEC coinvolti nell'SP, le attività progettuali non avanzeranno. In nessun caso l'approvazione potrà avvenire per tacito assenso a meno di specifiche indicazioni sulle tempistiche indicate dall'Amministrazione. Una volta firmato il documento, l'Amministrazione reinvierà, via PEC, al fornitore il documento approvato.

Per tutte le sezioni sopra citate, il fornitore deve obbligatoriamente fornire all'Amministrazione e a chi deve effettuare le opportune verifiche, ai fini di confermare la veridicità di quanto comunicato, la documentazione inerente alle attività svolte durante il mese. Queste devono essere cariche nel portale della fornitura. A titolo di esempio si citano alcuni documenti che devono essere resi visibili:

1. CV delle risorse
2. Certificazioni delle risorse
3. Documentazione di sintesi e di dettaglio degli indicatori di qualità
4. Minute, Verbali in cui si evidenziano eventuali variazioni/modifiche contrattuali
5. File di allocazione risorse per ciascun servizio

9.2.10 Portale della fornitura

A supporto delle attività di governo, gestione e monitoraggio della fornitura, il fornitore dovrà realizzare il Portale della Fornitura e mantenerlo aggiornato durante tutto il periodo di contratto. Questa piattaforma, accessibile dal personale della Regione e condivisa tra le aziende del RTI, offrirà funzionalità personalizzate in base ai ruoli e ai profili degli utenti, consentendo di:

- Pianificare e monitorare le attività contrattuali e le risorse coinvolte
- Tracciare eventi e dati per la creazione di indicatori di qualità e performance, nonché per la condivisione di informazioni utili alla governance
- Abilitare la comunicazione e la collaborazione attraverso diversi canali

Il Portale, insieme ai cruscotti e agli strumenti associati, permetterà al Fornitore e ai Referenti di RV di seguire in tempo reale l'avanzamento delle attività, verificando il rispetto delle previsioni relative a tempi, costi e qualità.

Si specifica che il portale della fornitura (disegno ed implementazione) è incluso negli adempimenti del contratto e le attività di realizzazione, gestione e manutenzione dello stesso non dovranno avere alcun onere aggiuntivo per RVE e non dovranno essere svolte dai Team di presidio (Team servizio di conduzione operativa dei sistemi e sicurezza, Team servizio PdL)

9.3 Modalità di consegna

Il piano di Qualità, il piano di servizio e i documenti richiesti contrattualmente secondo capitolo 9.1Prodotti della fornitura devono essere consegnati formalmente via PEC. Il ciclo di vita dei documenti ufficiali dovrà essere definito nel Piano della Qualità e tracciato già a partire dalla prima nello strumento di gestione documentale dell'Amministrazione. Si precisa che la mancata approvazione di documenti contrattuali (e/o artefatti di servizi) da parte dell'Amministrazione a seguito di motivati rilievi costituisce inadempimento contrattuale cui può conseguire l'adozione delle azioni contrattuali indicate nell'Appendice 1 -Indicatori di Qualità.

Il Fornitore deve consegnare tutta la documentazione sul portale della gestione documentale a disposizione di RV.

Ogni comunicazione formale relativa alla gestione e all'esecuzione del contratto può essere inviata per posta certificata o formalizzata in una comunicazione sottoscritta dal soggetto contrattualmente responsabile indirizzata all'attenzione del RUP del contratto.

L'Amministrazione si riserva di aggiornare in corso d'opera il formalismo corrente della documentazione o di variare i contenuti della documentazione concordati, nonché di emettere nuovi standard, sia come contenuti che come modalità di produzione, anche durante il corso della fornitura. Tali nuove indicazioni devono essere adottate per tutti i nuovi interventi, mentre saranno concordate le eventuali modalità di transizione per gli interventi in corso al momento. Tutta la documentazione della fornitura deve essere sempre tenuta aggiornata, sia essa basata su documentazione preesistente, per gli interventi progettuali, sia essa prodotta ex novo. L'aggiornamento della documentazione può avvenire per intero documento o per addendum, secondo quanto di volta in volta concordato con RV.

9.4 Azioni contrattuali

Ogni inadempimento contrattuale darà origine ad un'azione commisurata alla criticità dell'inadempimento stesso. I principali aspetti delle prestazioni contrattuali vengono presidiati da appositi indicatori di qualità. Pertanto, il mancato rispetto dei requisiti minimi richiesti e/o migliorati dal fornitore in Offerta Tecnica determina azioni contrattuali conseguenti che possono consistere in una o più delle seguenti azioni:

- Coinvolgimento di un livello più elevato di interlocutori sino ad eventuali organismi di governo dei contratti strategici, allo scopo di prendere le decisioni necessarie al ripristino delle situazioni fuori soglia o fuori controllo (attivazione di una procedura di escalation);
- Ripetizione da parte del fornitore dell'erogazione di una prestazione, rifacimento di una attività, riconsegna di un prodotto (chiusura di una non conformità);
- Azione di intervento sui processi produttivi del fornitore per evitare il ripetersi di sistematiche non conformità (esecuzione di una azione correttiva);
- Applicazione di rilievi;
- Perdita della quota variabile del corrispettivo legato al raggiungimento di un livello di qualità minimo;
- Applicazione di penali;

- Azioni aggiuntive (richiesta danni, risoluzione anticipata del contratto, ecc.) laddove previsto contrattualmente.

9.4.1 Rilievi

I rilievi sono le azioni di avvertimento da parte dell'Amministrazione conseguenti il non rispetto delle indicazioni contenute nella documentazione contrattuale. Pertanto, oltre a quanto esplicitamente previsto, potrà essere emesso un rilievo su qualunque inadempimento. I rilievi non prevedono di per sé l'applicazione di penali, ma costituiscono avvertimento sugli aspetti critici della fornitura e, se reiterati e accumulati, danno luogo a penali, secondo quanto previsto nell'Appendice 1 Indicatori di qualità. I rilievi possono essere emessi dal Direttore dell'esecuzione dell'Amministrazione (DEC), RUP, dal team di monitoraggio che è a supporto del DEC e dagli assistenti al DEC e sono formalizzati attraverso una nota di rilievo inviata via PEC, ognuna delle quali potrà contenere uno o più rilievi. Qualora il fornitore ritenga di procedere alla richiesta di annullamento del rilievo, dovrà sottoporre all'Amministrazione un documento con elementi oggettivi ed opportune argomentazioni entro 3 giorni lavorativi dall'emissione del rilievo.

Qualora il fornitore non fornisca alcun documento a supporto, il rilievo è da considerarsi formalizzato e confermato.

A fronte di 3 rilievi sulla stessa tematica, sarà a carico dell'Amministrazione valutare o meno se procedere con la comunicazione di una penale.

9.4.2 Penali

Lo scopo delle penali è quello di riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) da RV al corrispettivo da erogarsi che è stabilito per prestazioni effettuate a regola d'arte. Le penali da adottare sono individuate contrattualmente secondo quanto previsto nell'Appendice 1 Indicatori di qualità e normalmente sono organizzate in modo progressivo in relazione alla gravità o al ripetersi della mancata soddisfazione degli adempimenti richiesti.

Le penali vengono di solito applicate quando viene accertato l'inadempimento da parte dell'Amministrazione verso il fornitore, ma il contratto deve specificare le modalità di applicazione:

- **Accertamento dell'inadempimento**: RV deve valutare se si è verificato un inadempimento e determinarne l'entità.
- **Comunicazione al fornitore**: L'applicazione delle penali deve essere formalmente notificata al Fornitore, con la specifica dell'importo e della motivazione tramite PEC
- **Pagamento delle penali**: Il Fornitore deve effettuare il pagamento della penale entro un termine concordato.

Nel caso in cui il fornitore contesti l'applicazione delle penali, è possibile inviare all'amministrazione entro i 5 giorni dal ricevimento della penale, ogni eventuale controdeduzione in ordine alle contestazioni supportate da chiara ed esauriente documentazione.

Qualora il Fornitore non inviasse entro i 5 giorni alcuna contestazione, decade ogni controdeduzione che il Fornitore vuole rilevare.

9.5 Monitoraggio

Le attività di monitoraggio sull'esecuzione del contratto saranno conformi a quanto previsto dalla circolare n. 1 del 20-01-2021 emessa dall'AgID, ai sensi dell'art. 14-bis, comma 2, lett. h.) del CAD, come modificato dal decreto legislativo 16 luglio 2020 n.76. Il fornitore si impegna a fornire all'Amministrazione tutti i documenti necessari all'attività di monitoraggio, nei formati richiesti e necessari per il controllo e la verifica della fornitura, salvo evoluzioni derivanti dall'introduzione, da parte della Amministrazione, di strumenti automatici a ciò deputati. Il fornitore si impegna ad inviare all'Amministrazione la documentazione comprovante l'eventuale esito delle visite di sorveglianza della società di certificazione della qualità e/o il rinnovo della certificazione entro 1 mese dalla data della verifica.

Inoltre il fornitore e/o i subfornitori devono rendersi disponibili alle verifiche anche ispettive effettuate dall'Amministrazione tramite personale proprio o da terzi da essa incaricati, svolte nel rispetto di quanto prescritto dalla serie di norme EN ISO 19011:2003.

Le tempistiche con cui le lavorazioni o elaborazioni richieste dovranno essere portate a termine e la consegna dei contenuti richiesti dovranno essere compatibili con le azioni di monitoraggio stesse e non dovranno, in alcun modo, generare o contribuire ad aumentare eventuali ritardi.

9.6 Requisiti di Qualità e Sicurezza della Fornitura

Nell'esecuzione delle attività previste dalla presente procedura aperta, il Fornitore deve:

- Rispettare i principi di assicurazione e di gestione della qualità della norma EN ISO 9001 rispetto alla quale gli è stata richiesta la certificazione;
- Attenersi ed essere conforme a quanto previsto dal proprio Sistema di Gestione della Qualità e dal Piano della Qualità;
- Implementare e perseguire le soluzioni migliorative proposte dal Fornitore in sede di offerta;
- Essere compliant al regolamento europeo GDPR per quanto attiene la protezione dei dati e la gestione degli incidenti;
- Rispettare la normativa ISO 25010 e successive sulla qualità del software e dei dati;
- Rispettare la normativa ISO 27001 Sistemi di gestione della sicurezza delle informazioni - Requisiti;
- Rispettare la normativa ISO 20000 e successive sulla Gestione dei Servizi di Information Technology;
- Rispettare la normativa ISO 22301 e successive sulla Sicurezza della società - Sistemi di gestione della continuità operativa
- Rispettare i livelli di servizio e gli indicatori di qualità.
- Rispettare comunque le certificazioni esistenti o future e le specifiche procedure / manuali operativi in essere in Regione del Veneto.

Inoltre, il Fornitore deve garantire il rispetto degli adempimenti di sicurezza, per quanto attiene al Centro Servizi che il Fornitore deve mettere a disposizione per l'erogazione dei servizi da remoto.

9.6.1 Indicatori di Qualità

Gli indicatori di qualità sono strumenti utilizzati per valutare l'efficacia, l'efficienza e l'affidabilità dei servizi forniti dal fornitore. Questi indicatori permettono di misurare la performance e di garantire che il fornitore stia rispettando gli impegni contrattuali, gli standard di servizio e le normative applicabili. La misurazione della qualità dei servizi è essenziale per monitorare i risultati, migliorare le prestazioni e ottimizzare la gestione del contratto.

In un contesto come quello di RV, gli indicatori di qualità devono essere definiti con attenzione, per essere oggettivi, misurabili e rilevanti rispetto agli obiettivi del contratto o del servizio. Tutti gli Indicatori di qualità devono essere riportati nel Piano della Qualità da sottoporre all'approvazione dell'Amministrazione, con indicazione delle fonti dati utilizzate per la raccolta delle misure elementari, nonché gli strumenti per l'elaborazione delle informazioni di dettaglio.

La rendicontazione dei livelli di servizio ha lo scopo di:

- Verificare la conformità dei servizi rispetto a quanto richiesto;
- Verificare l'effettivo andamento dei servizi e anticipare la gestione degli scostamenti;
- Consuntivare i servizi e le attività;

- Verificare l'andamento degli indicatori di qualità;
- Ottimizzare le attività di monitoraggio dei servizi.

Il Fornitore deve raccogliere i dati elementari e calcolare gli Indicatori di qualità della fornitura e, sulla base di essi, predisporre delle rappresentazioni dell'andamento della stessa. Il Fornitore si impegna a mettere a disposizione nel portale della fornitura a RV, la base dati di dettaglio contenente tutti i dati rilevati, utilizzata per la valorizzazione degli indicatori di qualità.

Il Fornitore deve presentare i report in formato dati e grafici di comune utilizzo e visualizzabili nelle comuni Suite applicative per l'ufficio, per un successivo ed eventuale trattamento (modifica, manipolazione, esportazione, ecc.).

Durante l'intero periodo contrattuale ciascun indicatore di qualità può essere riesaminato su richiesta dell'Amministrazione; il riesame può derivare da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o dall'adeguamento delle metodiche atte alla rilevazione dei singoli indicatori di qualità che sono risultate non efficaci. L'Amministrazione ed il Fornitore, in caso di necessità, concordano eventuali modifiche ai metodi di calcolo successivamente riportati e tracciati nel Piano della Qualità, che il Fornitore si impegna a rispettare nel rispetto delle modifiche intercorse.

In presenza di estensioni di contratto rispetto al contratto originario, gli indicatori di qualità saranno i medesimi e devono necessariamente essere calcolati dal primo mese di attività.

9.6.2 Normative di riferimento

Di seguito si evidenziano alcune normative di riferimento per l'esecuzione delle attività:

- Cancellazione sicura dei dati quale obbligo di Legge secondo quanto contenuto nel Decreto Legislativo 196 del 2003 – Codice in materia di protezione dei dati personali – e nel GDPR (General Data Protection Regulation) del 2016/679;
- Direttiva Europea 2012/19/UE sui RAEE, entrata in vigore il 13 agosto 2012, recepita con il D.Lgs. del 14 marzo 2014 n. 49 e s.m.i.;
- ISO 27001:2022 Sistemi di gestione della sicurezza delle informazioni;
- Legge 241/1990 (Norme sul procedimento amministrativo);
- Sicurezza informatica (Direttiva NIS 2 e Legge 105/2019 e Articolo 44 del codice degli appalti;
- ISO 20000 e successive sulla Gestione dei Servizi di Information Technology.

9.6.3 Documentazione

Nel contesto della Regione del Veneto, ogni fornitore è tenuto a rispettare gli standard regionali previsti, allineandosi ai requisiti della ISO 9001 per la gestione della qualità. La documentazione fornita deve essere completa, aggiornata e garantire la tracciabilità, la qualità e la conformità dei processi erogati.

In linea con la ISO 9001, è essenziale che il fornitore adotti un sistema di gestione che consenta di registrare, archiviare e rendere accessibili tutte le informazioni relative alla progettazione, implementazione e verifica dei servizi offerti. La documentazione deve essere consultabile in modo semplice, gestita con sicurezza e sottoposta a revisioni periodiche, per garantire il rispetto degli standard regionali e delle normative vigenti.

Inoltre, il fornitore è obbligato a garantire la tracciabilità delle modifiche documentali, le quali devono essere approvate da figure competenti. Tutti gli aggiornamenti documentali relativi a interventi tecnici o progettuali, che sono

parte integrante della fornitura, devono essere consegnati in formato digitale e caricati sul sistema di gestione documentale della Regione, Alfresco. (https://documentazioneict.regione.veneto.it/share/page).

Inoltre il fornitore è tenuto ad inserire in Bitbucket, piattaforma già utilizzata da Regione del Veneto, i codici sorgenti dei software.