Istituto Zooprofilattico
Sperimentale delle Venezie

Capitolato Tecnico

Procedura aperta, di importo superiore alle soglie comunitarie, per l'aggiudicazione dei servizi di assistenza sistemistica per l'IZSVe

Gara n. 8257206 – CIG: 887346789C

SOMMARIO

CAPITOLATO TECNICO

Il presente capitolato tecnico disciplina le prestazioni, le modalità di svolgimento delle stesse, i termini e le specifiche tecniche minime dei servizi inclusi nell'appalto indicato in oggetto per l'Istituto Zooprofilattico Sperimentale delle Venezie (di seguito "*IZSVe*", "*Istituto*" o "*Stazione Appaltante*").

Il medesimo capitolato costituisce parte integrante e sostanziale della *lex specialis* di gara e costituirà parte integrante e sostanziale del contratto di appalto che l'Istituto stipulerà, all'esito della procedura di gara, con l'operatore economico aggiudicatario.

1. PREMESSA

L'Istituto Zooprofilattico Sperimentale delle Venezie opera nell'ambito del SSN come strumento tecnico-scientifico dello Stato e delle Regioni Veneto, Friuli Venezia Giulia e Trentino Alto Adige e persegue obiettivi di salute pubblica svolgendo attività di controllo, sorveglianza e ricerca scientifica nell'ambito dei rischi alimentari, del benessere animale e delle malattie trasmissibili dagli animali (zoonosi).

Per garantire tale operatività l'IZSVe è strutturato su una rete informatica che comprende la sede centrale di Legnaro (PD) e n. 10 sedi diagnostiche territoriali distribuite nel proprio territorio di competenza (6 in Veneto, 2 in Friuli Venezia Giulia e 2 in Trentino Alto Adige), di seguito elencate:

Sede	Riferimenti
Sede centrale di Legnaro (PD)	Viale dell'Università, 10 - 35020 - Legnaro (PD)
Sede territoriale di Adria (RO)	Via L. Da Vinci, 39 - 45011 - Adria (RO)
Sede territoriale di Belluno	Via Cappellari, 44/A - 32100 - Belluno
Sede territoriale di Bolzano	Via Laura Conti, 4 - 39100 - Bolzano
Sede territoriale di Pordenone	Via Bassa del Cuc, 4 - 33084 - Cordenons (PN)
Sede territoriale di San Donà (VE)	Via Calvecchia, 10 - 30027 - San Donà di Piave (VE)
Sede territoriale di Trento	Via Lavisotto, 129 - 38100 - Trento
Sede territoriale di Treviso	Vicolo Mazzini 4 int 5/6 - 31020 - Fontane di Villorba (TV)
Sede territoriale di Udine	Via della Roggia, 100 - 33030 - Basaldella di C. (UD)
Sede territoriale di Verona	Via Bovolino, 1/C – 37060 Buttapietra (VR)
Sede territoriale di Vicenza	Viale Fiume, 78 - 36100 - Vicenza

Le sedi territoriali sono collegate alla sede centrale tramite una rete MPLS con topologia a stella; tutti i principali servizi del Sistema IT IZSVe, il Data Center aziendale e gli accessi a Internet sono collocati nella sede centrale di Legnaro che rappresenta il centro stella, e sono gestiti dal Servizio Informatica - Direzione Generale dell'IZSVe.

I servizi sanitari forniti dall'IZSVe che si appoggiano all'infrastruttura IT devono essere erogati con costante **garanzia di sicurezza e affidabilità, senza interruzione di continuità e con prestazioni adeguate**, imponendo di perseguire standard informatici sempre più elevati.

Tali richieste, oltre che rispondere alle necessità di supporto allo svolgimento delle attività istituzionali dell'IZSVe, devono soddisfare le nuove esigenze di miglioramento basate su fonti normative che richiedono al Servizio Informatica di adeguare i propri sistemi e policy IT per essere conformi alle disposizioni in materia; per citare solo le più importanti:

- Sicurezza ICT (direttiva del PCM/AgID sulle Misure minime di sicurezza ICT per le PA – aprile 2016)
- Protezione dei dati (Direttive UE contenute nel General Data Protection Regulation - maggio 2016)
- Infrastrutture IT, connettività, sicurezza informatica, ecc. (direttive AgID contenute nel Piano triennale per l'informatica nella PA 2020-2022)

Una gestione del Sistema IT dell'IZSVe non conforme agli standard richiesti può causare delle **interruzioni di servizio** (in termini di ore/giorni di fermo parziale o totale delle attività) o comunque può determinare dei **danni diretti/indiretti** all'Istituto che possono essere di entità anche molto rilevante in termini economici, di ore di lavoro perse e/o da impiegare per rettificare le anomalie/danni, di disservizio verso gli utenti finali, fino alla configurazione di gravi danni di immagine.

Un altro fattore di contesto è riconducibile all'evoluzione costante delle tecnologie che determina la necessità di un continuo aggiornamento, la messa a punto delle stesse, la loro diffusione e gestione, la quale richiede una disponibilità sempre crescente in termini di numero e di qualità di risorse umane.

Considerata la grande complessità del Sistema IT IZSVe, la costante evoluzione tecnologica in ambito informatico e la criticità dei servizi erogati, è necessario ed estremamente importante che il personale del Servizio Informatica sia supportato con **Servizi di Assistenza Informatica Specialistica**, oggetto principale della presente gara, che permettano di garantire il rispetto degli standard richiesti, di assicurare la funzionalità del sistema stesso e di garantirne un alto grado di efficienza e di sicurezza.

E' necessario quindi far ricorso ad organizzazioni esterne (*System Integrator*) in grado di mettere a disposizione *know how* specialistico e risorse altamente qualificate che opereranno sulla base di indicazioni specifiche definite dal Dirigente Responsabile del Sistema IT IZSVe o da un suo delegato all'interno degli ambiti, delle attività e delle responsabilità definiti dal presente capitolato.

2. DEFINIZIONI

Servizio Informatica	Servizio interno all'IZSVe che gestisce il Sistema IT IZSVe
NOC	Network Operation Center
Incidente	Qualsiasi evento che non fa parte dell'operatività ordinaria / standard di un servizio e che causa, o può causare, un'interruzione e una riduzione della qualità di tale servizio
Workaround	Correzione temporanea ad un incidente o una sequenza di azioni alternativa a quella che produce l'incidente, utilizzabile dall'utente
Service Request	Richiesta da un utente per un'informazione, un consiglio, un cambiamento standard (standard change) o per un accesso ad un servizio IT
Incidente di sicurezza	Qualsiasi evento che non fa parte dell'operatività ordinaria / standard di un servizio che può costituire una minaccia alla sicurezza informatica con un impatto sui sistemi / servizi IT
MDRS	Managed Detection & Response System
CSIRT	Computer Security Incident Response Team
Data Center	L'insieme di tutti i dispositivi tecnologici informatici (server fisici/virtuali, apparati di storage e di networking, cablaggi e rack, ecc.) che costituiscono l'asset IT centralizzato dell'Istituto
Rete dati	L'insieme degli apparati di networking che interconnettono l'assett IT periferico dell'Istituto collegando tra loro gli edifici del campus della sede centrale, la sede centrale con le sedi periferiche e la rete privata dell'Istituto con la rete Internet

3. OGGETTO DELL'APPALTO

L'appalto si compone dei seguenti servizi:

1) Servizi e sistemi di monitoraggio dell'infrastruttura del Sistema IT IZSVe
2) Servizi e sistemi di gestione delle configurazioni
3) Servizio di raccolta e conservazione a norma dei log degli amministratori
4) Servizio di Asset Management e scadenziario
5) Servizi di supporto e assistenza sistemistica tramite NOC (Network Operation Center)
6) Servizio di supporto per la sicurezza IT tramite MDRS (Managed Detection & Response System) e CSIRT (Computer Security Incident Response Team)

7) Servizio di supporto specialistico (a giornata).

I Servizi vengono suddivisi in:

- **Servizi base,** remunerati tramite canone mensile; sono da ricomprendersi nelle attività cd. "*a canone*" tutte le prestazioni continuative previste dai servizi oggetto di affidamento come specificato nel prosieguo; in linea generale, si tratta di attività che non necessitano di preventiva autorizzazione da parte dall'Istituto, ma devono essere eseguite dall'appaltatore con le periodicità previste nel contratto e nella documentazione di gara ovvero ogniqualvolta siano richieste dalla stazione appaltante, fermi gli eventuali previ accordi di dettaglio da concordarsi con il Direttore dell'Esecuzione del Contratto (DEC).

Tali attività sono prestate a fronte del pagamento in favore dell'appaltatore di un canone mensile calcolato mediante applicazione dei prezzi offerti dall'aggiudicataria in sede di partecipazione alla procedura, aggiunti i costi per l'eliminazione dei rischi interferenziali.

- **Servizi a richiesta,** non compresi nel canone ed espletati a seguito di specifica richiesta dell'Istituto; i servizi a richiesta saranno remunerati applicando i prezzi offerti dall'appaltatore in sede di gara, aggiunti gli eventuali costi per l'eliminazione dei rischi interferenziali.

Tutte le attività extra-canone saranno gestite per il tramite della preventiva emissione di buoni d'ordine trasmessi al Direttore Tecnico dell'appaltatore unitamente alle eventuali ulteriori informazioni di dettaglio; tali buoni valgono quali richieste di intervento da prestarsi nel rispetto dei termini massimi eventualmente previsti dalla documentazione di gara come integrata dall'offerta dell'aggiudicataria del servizio.

Sono compresi nei servizi di base e remunerate tramite canone mensile:

- Servizi e sistemi di monitoraggio dell'infrastruttura del Sistema IT IZSVe
- Servizi e sistemi di gestione delle configurazioni
- Servizio di raccolta e conservazione a norma dei log degli amministratori
- Servizio di Asset Management e scadenziario
- Servizi di supporto e assistenza sistemistica tramite NOC (Network Operation Center)
- Servizio di supporto per la sicurezza IT tramite MDRS (Managed Detection & Response System) e CSIRT (Computer Security Incident Response Team)
- n. 10 giornate di supporto specialistico (giornate a consumo), per ogni anno di contratto.

Sono comprese nei servizi a richiesta remunerati applicando i prezzi offerti dall'appaltatore:

- Servizio di supporto specialistico - giornate a consumo supplementari rispetto alle n. 10 giornate/anno comprese nel canone.

Per i servizi a richiesta si riporta di seguito la stima annuale dei fabbisogni per gli stessi stimati dalla stazione appaltante:

Tipo di servizio	Fabbisogno annuo presunto
Giornate di supporto specialistico (ulteriori rispetto alle giornate comprese nel canone)	10

Si precisa che tale fabbisogno - stimato sulla base dello storico della stazione appaltante committente – è da intendersi come meramente presuntivo e non vincolante per la stazione appaltante, la quale sarà tenuta a corrispondere all'appaltatore esclusivamente i servizi supplementari effettivamente ed espressamente richiesti nel corso dell'esecuzione contrattuale.

Le modalità di erogazione dei servizi e i loro specifici contenuti sono descritti nel prosieguo del presente capitolato.

Requisiti minimi di esecuzione:

1) **Personale dedicato all'esecuzione del servizio:**
   In ragione della complessità del servizio appaltando e degli SLA fissati nel presente Capitolato vengono individuati i seguenti requisiti MINIMI mediante i quali il servizio dovrà essere espletato:
   a) il servizio di NOC dovrà essere eseguito con un organico minimo pari a n. 30 operatori di cui:
      - almeno n. 5 operatori con il profilo di capo progetto (esperienza accertata in ambito informatico specialistico di oltre 10 anni);
      - almeno n. 5 operatori con il profilo di sistemista senior (esperienza accertata in ambito informatico specialistico da 6 a 10 anni);
      - almeno n. 20 operatori con il profilo di sistemista junior (esperienza accertata in ambito informatico specialistico fino a 5 anni);

   b) il servizio di sicurezza CSIRT dovrà essere eseguito con un organico minimo pari a n. 15 operatori.

2) **Certificazioni attive:**
   a) almeno uno degli operatori del servizio NOC dovrà possedere le seguenti certificazioni attive:
      - Cisco: CCIE routing e switching
      - NetApp: NCIE – NetApp Certified Implementation Engineer
      - VMware: VCP – VMware Certified Professional
      - Check Point: CCSE – Check Point Certified Security Expert
      - ITIL: ITIL Foundation

   b) almeno uno degli operatori del servizio CSIRT dovrà possedere le seguenti certificazioni attive:
      - ISC2 Certified Information Systems Security Professional (CISSP)
      - GIAC Certified Incident Handler (GCIH)
      - GIAC Certified Perimeter Protection Analyst (GPPA)
      - GIAC Web Application Penetration Tester (GWAPT)
      - ISECOM OSSTMM Professional Security Tester (OPST)
      - GIAC Reverse Engineering Malware (GREM)

4. DESCRIZIONE DEI SERVIZI

I servizi sistemistici richiesti dovranno agire direttamente oppure indirettamente, supportando gli addetti del Servizio Informatica, operando per la messa a punto e la gestione dei sistemi dettagliati nel relativo paragrafo del presente Capitolato, garantendone il corretto funzionamento, agendo sulle installazioni e sulle configurazioni e risolvendo i malfunzionamenti.

In considerazione dell'evoluzione tecnologica e dei relativi adeguamenti dell'infrastruttura che possono impattare sui sistemi oggetto del servizio, si specifica che i servizi richiesti si intendono applicati anche ai sistemi oggetto di *upgrade* e/o rinnovo tecnologico.

Si precisa che il dominio di intervento dei servizi richiesti è riconducibile all'infrastruttura del Sistema IT dell'IZSVe, gestito direttamente dal Servizio Informatica insieme ai vari partner tecnologici. Esso è costituito da elementi fisici e logici presenti principalmente nel Data Center (dove sono ospitati tutti i server e i dispositivi tecnologici che costituiscono l'asset IT centralizzato dell'Istituto) e dall'infrastruttura della rete dati aziendale (insieme degli apparati che interconnettono l'assett IT periferico dell'Istituto collegando tra loro gli edifici del campus della sede centrale, la sede con i laboratori periferici e l'Istituto con la rete Internet).

Si rinvia al successivo paragrafo dedicato per l'analitica descrizione del dominio di intervento.

Viene di seguito descritto il contenuto tecnico – prestazionale di ciascun servizio oggetto del presente appalto.

a) Servizi e sistemi di monitoraggio dell'infrastruttura del Sistema IT IZSVe

Il **servizio di monitoraggio** deve permettere un controllo continuo e in tempo reale dello stato di funzionamento dell'infrastruttura del Sistema IT al fine di garantire la massima disponibilità dei sistemi e la contemporanea massima riduzione del tempo di *downtime*.

Il servizio di monitoraggio deve essere disponibile con un ***uptime*** **di almeno 99,9%**.

Il servizio dovrà essere espletato nel rispetto delle seguenti modalità, da intendersi quali caratteristiche tecniche minime richieste a pena di inammissibilità dell'offerta alla procedura:

- erogazione in modalità *as a service*: tutte le componenti del sistema devono risiedere presso il fornitore con esclusione del sistema VPN di collegamento all'infrastruttura che sarà fornito dall'IZSVe secondo lo standard IPSec con crittografia almeno DES; la disponibilità di un sistema VPN rappresenta l'unico requisito richiesto all'IZSVe;
- utilizzo di protocolli standard (es. SNMP) al fine di garantire la massima compatibilità;
- garanzia di massima riservatezza dei dati raccolti e memorizzati;
- memorizzazione dei dati raccolti in un database centralizzato e conservazione per almeno 12 mesi;
- erogazione con una unica piattaforma integrata accessibile mediante una unica console di gestione;
- soluzione interamente web based accessibile mediante i più comuni browser con protocollo HTTPS;
- visualizzazione grafica dei sistemi e di tutti gli oggetti monitorati che devono essere "navigabili" e "cliccabili" per la visualizzazione dei dettagli con approccio intuitivo;
- visualizzazione delle informazioni di stato e di performance degli oggetti monitorati;
- sistema di rendicontazione dei dati raccolti con report grafici basati su intervallo temporale;
- sistema di esportazione dei dati raccolti dal monitoraggio in formato standard (es. XLS, PDF);
- sistema gerarchico di notifica e alerting via email e sms in tempo reale sulla base di soglie di errore e allarme personalizzabili;
- monitoraggio dello stato generale degli oggetti (online / offline);
- monitoraggio dei parametri primari dei server fisici e virtuali (CPU, memoria, occupazione dischi logici, sessioni attive);
- monitoraggio di infrastrutture VMWare;
- monitoraggio di sistemi storage SAN / NAS;
- monitoraggio dei parametri primari degli apparati di rete (CPU, memoria, parametri di environment);
- monitoraggio di traffico ed errori su singole interfacce di apparati di rete Ethernet;
- documentazione sull'utilizzo delle porte degli apparati di rete Ethernet;
- documentazione sulle VLAN attive sulle reti Ethernet / Wireless;
- analisi qualitativa del traffico sui link tra apparati di rete Ethernet;
- controllo del traffico anomalo sui link tra apparati di rete Ethernet;
- monitoraggio dei client attivi e del livello di segnale su reti Wireless;
- monitoraggio delle VPN statiche (lan-to-lan) e dinamiche (client-to-lan);
- monitoraggio delle connettività MPLS tra sedi IZSVe;
- monitoraggio dei parametri primari di UPS di Data Center (assorbimento e potenza);
- monitoraggio ambientale del Data Center (temperatura, umidità, dew point).

b) Servizio e sistemi di gestione delle configurazioni

Il servizio di **gestione delle configurazioni** deve garantire la documentazione, il salvataggio e la disponibilità delle configurazioni degli apparati di rete monitorati al fine di un loro rapido ripristino in caso di danno rilevante.

Il servizio dovrà essere espletato nel rispetto delle seguenti modalità, da intendersi quali caratteristiche tecniche minime richieste a pena di inammissibilità dell'offerta alla procedura:

- raccolta dati sicura attraverso una connessione VPN IPSec con crittografia almeno DES;
- integrazione completa con il servizio di monitoraggio dell'infrastruttura IT IZSVe e fuibilità mediante lo stesso portale web based di accesso e gestione;
- supporto degli apparati di rete di Cisco e HP;
- rilevamento, salvataggio, storicizzazione e visualizzazione delle configurazioni rilevabili;
- possibilità di associare una descrizione mnemonica alle configurazioni;
- download diretto da portale web delle configurazioni degli apparati.

c) Servizio di raccolta e conservazione a norma dei log degli amministratori

Il servizio di **Log Management** ha come oggetto il trattamento degli accessi ai sistemi IT IZSVe da parte degli amministratori erogato in maniera conforme alle disposizioni della normativa italiana ed europea in materia. Si fa particolare riferimento alla normativa in materia di Privacy che è regolata dal Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" , al quale si aggiungono alcuni provvedimenti generali emessi dal Garante della Privacy e tra questi in particolare il Provvedimento Generale in materia di amministratori di sistema (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 e s.m.i.).

La conformità deve essere garantita anche relativamente alle disposizioni contenute nel regolamento UE 2016/679 (GDPR – General Data Protection Regulation) e relative eventuali indicazioni del Garante della Privacy sul tema indicato.

Il sistema dovrà disporre delle seguenti caratteristiche, da intendersi quali caratteristiche tecniche minime richieste a pena di inammissibilità dell'offerta alla procedura:

- funzionamento del sistema in modalità *as a service*: le componenti principali del sistema devono risiedere presso il fornitore; l'accesso ai sistemi IZSVe da gestire viene garantita mediante collegamento VPN IPSec;
- garanzia della massima riservatezza dei dati raccolti e memorizzati;
- conservazione per almeno 6 mesi dei log raccolti in un database centralizzato presso il fornitore;
- configurazione personalizzabile di tutti i sistemi da cui raccogliere i log di accesso;
- integrazione con il servizio di monitoraggio dell'infrastruttura IT IZSVe, gestione e accesso al sistema mediante lo stesso portale web based per analisi e consultazione dei log raccolti e della relativa reportistica.

d) Servizio di Asset Management e scadenziario

Il servizio di **Asset Management** deve permettere l'archiviazione degli oggetti che fanno parte del dominio di applicazione del contratto e sottoposti al monitoraggio. Deve essere possibile gestire uno scadenziario dei contratti di manutenzioni / supporto attivi sui sistemi monitorati al fine poterne gestire i rinnovi.

Il servizio dovrà disporre delle seguenti caratteristiche, da intendersi quali caratteristiche tecniche minime richieste a pena di inammissibilità dell'offerta alla procedura:

- integrazione completa con il servizio di monitoraggio dell'infrastruttura IT IZSVe e fuibilità mediante lo stesso portale web based di accesso e gestione;
- indicazione e descrizione dell'oggetto monitorato (funzionalità di asset inventory);
- indicazione dei riferimenti ai contratti di manutenzione / supporto attivi sull'oggetto;
- indicazione della data di fine manutenzione / supporto attivi sull'oggetto (scadenziario rinnovi).

e) <u>Servizio di supporto e assistenza sistemistica tramite NOC (Network Operation Center)</u>

Il **servizio di assistenza sistemistica** - **NOC (Network Operation Center)** - è finalizzato sia a supportare il personale dei Servizio Informatica con compiti di amministrazione dell'infrastruttura del Sistema IT IZSVe sia ad intervenire direttamente nella gestione dell'infrastruttura stessa su richiesta del Responsabile del Servizio Informatica o suoi delegati.

I servizi erogati dal NOC devono prevedere l'utilizzo delle tecnologie abilitanti il monitoraggio remoto e la completa gestione dei sistemi da remoto.

Le **attività di supporto del NOC** devono essere di tipo proattivo e direttamente erogabili a fronte di allarme proveniente dal sistema di monitoraggio. Il personale IT dell'IZSVe deve comunque essere informato – nei casi necessari anche preventivamente - di ogni operazione effettuata.

Le attività richieste al NOC, senza alcun limite nel numero complessivo, sono quelle necessarie a:

- configurare, personalizzare, mantenere in efficienza e concorrere alla corretta gestione del Sistema IT nelle sue componenti hardware e software collaborando, quando necessario, anche con personale tecnico dei fornitori / partner / collaboratori dell'IZSVe;
- contribuire a mantenere i sistemi elaborativi, di rete e gli storage ad un livello di piena disponibilità, efficienza, affidabilità e sicurezza;
- rilevare e rimuovere tutti i problemi che dovessero manifestarsi nell'infrastruttura informatica;
- collaborare alla realizzazione degli interventi che saranno ritenuti necessari per garantire la continuità operativa dell'infrastruttura informatica;
- fornire informazioni tecniche di supporto al personale del Servizio Informatica per lo svolgimento delle attività ordinarie e straordinarie di gestione e evoluzione dell'infrastruttura informatica.

Il NOC dovrà operare in maniera conforme alle linee guida ITIL v2 e v3 di seguito richiamate in maniera sintetica. Per ogni altro approfondimento si può fare riferimento alle librerie ufficiali.

Il NOC viene attivato su **esplicita richiesta (ticket)** degli operatori del Servizio Informatica, e inoltre deve operare anche in **modalità proattiva** su tutto il dominio di intervento dei servizi richiesti, gestendo e recependo direttamente le problematiche segnalate dal sistema di monitoraggio e agendo per la loro soluzione in maniera autonoma dando evidenza agli operatori del Servizio Informatica sia della problematica affrontata che della risoluzione adottata.

Il servizio dovrà essere espletato nel rispetto delle seguenti modalità, da intendersi quali caratteristiche tecniche minime richieste <u>a pena di inammissibilità dell'offerta alla procedura</u>:

- modalità di accesso / intervento da remoto sui sistemi del dominio di intervento (mediante VPN);
- espletamento del servizio di NOC mediante i seguenti processi principali, erogati secondo le specifiche tecniche e organizzative descritte in dettaglio successivamente:
    - **Gestione degli incidenti (Incident Management);**
    - **Gestione delle richieste e configurazioni standard (Request Fulfilment).**

➢ **Gestione degli incidenti (Incident Management)**

Il processo di Incident Management comprende la gestione degli incidenti che possono presentarsi nei sistemi o apparati inclusi nel dominio di intervento dei servizi richiesti.

L'obiettivo del processo di Incident Management è di ripristinare le normali funzionalità di servizio il più velocemente possibile, garantendo la **minima interruzione di servizio possibile**, e assicurando che i livelli di servizio e disponibilità siano mantenuti.

Nel processo di Incident Management si intende per:

- **Incident**: un qualsiasi evento che non fa parte dell'operatività standard di un servizio e che causa, o può causare, un'interruzione e una riduzione della qualità di tale servizio.
- **Workaround**: una correzione temporanea ad un incidente o una sequenza di azioni alternativa a quella che produce l'incidente, utilizzabile dall'utente.

Un incident deve essere classificato secondo **4 livelli di criticità e urgenza** (critica, alta, media e bassa) in base all'impatto che hanno sull'infrastruttura.

A titolo esemplificativo si riporta una classificazione di massima:

Tipologia	Descrizione
1 (Critica)	Perdita di servizio immediata, senza un workaround disponibile
2 (Alta)	Perdita di servizio imminente, oppure immediata, ma riducibile tramite workaround
3 (Media)	Nessuna perdita di servizio di business, da uno a più utenti impattati
4 (Bassa)	Nessuna perdita di servizio, gli utenti continuano a lavorare seppure con qualche disagio

Le fasi e le responsabilità nel processo di Incident Management sono le seguenti:

1. La registrazione dell'incidente
2. La classificazione dell'incidente ed il supporto iniziale
3. L'analisi e la diagnosi dell'incidente
4. La soluzione ed il ripristino dell'operatività
5. La chiusura dell'incidente
6. La *ownership* dell'incidente, il monitoraggio e le relative comunicazioni

A tal fine il fornitore dovrà:

- disporre nella propria organizzazione di un Help Desk strutturato su più livelli con progressione crescente di competenze;
- assicurarsi che ci siano risorse umane dedicate all'incident management con specifiche competenze certificate negli ambiti specifici del dominio di intervento;
- formare le risorse umane a comprendere il processo di incident management e le relazioni con altri processi (*process awareness*);
- mettere l'utente al centro del servizio;
- creare una *knowledge base* (storico incident) condivisa con i referenti informatici dell'IZSVe per la risoluzione degli incidenti:
  - la consultazione della *knowledge base* deve far parte del processo,
  - la *knowledge base* deve essere aggiornata come risultato del processo;
- avere un tool software di assegnamento/tracciamento degli incidenti che implementi il processo; il tool deve essere parte della *knowledge base* (i tecnici del NOC devono avere accesso a tutti gli incidenti per poter vedere le soluzioni già implementate);
- formalizzare le procedure di incident management e formare il personale su quelle procedure nel rispetto dei livelli di servizio richiesti;
- definire le priorità degli incidenti in base a criteri obiettivi (matrice urgenza/impatto);
- monitorare i livelli di servizio in maniera periodica fornendo i report con le metriche di misurazione richieste;
- formalizzare accordi con gruppi di supporto esterni qualora gli incidenti vadano scalati;
- definire il ciclo di vita degli incidenti per evitare che vi siano "zone morte" in cui non si sa chi è il responsabile.

Il servizio di Help Desk del NOC dovrà gestire i processi nelle seguenti fasi:

1. Registrazione della richiesta (apertura ticket)
2. Classificazione richiesta

3. Assegnazione priorità
4. Escalation delle richieste
5. Risoluzione degli incidenti segnalati
6. Chiusura richiesta (chiusura ticket)
7. Analisi dei trend e delle cause.

Di seguito si descrivono in dettaglio le attività richieste al servizio di Help Desk del NOC che deve essere strutturato su tre livelli con progressione crescente di competenze.

Il **primo livello di Help Desk** è costituito da un unico punto di accesso al servizio e la sua attivazione può avvenire mediante le seguenti modalità:

- **Su richiesta** degli operatori del Servizio Informatica dell'IZSVe oppure dai tecnici esterni del Servizio CSIRT (per gli incidenti di sicurezza) mediante apertura di un ticket (identificato da un codice numerico univoco: numero di ticket) via telefono, email o portale web (integrato con il portale del servizio di monitoraggio dell'infrastruttura IT IZSVe).
- **Proattivamente** su allarme innescato dal servizio di monitoraggio del sistema.

I compiti dell'Help Desk di primo livello sono:

1. Comprendere la richiesta e confermare l'esistenza di un problema / incidente
2. Registrare la richiesta e la relativa data/ora sul sistema di ticketing e assegnare il numero di ticket (apertura ticket), se non già presente
3. Classificare la richiesta assegnando una tipologia / sottotipologia e un ambito di competenza (sistemi, networking, sicurezza, ecc.)
4. Assegnare una priorità (1. Critica, 2. Alta, 3. Media, 4. Bassa)
5. Segnalare al Servizio Informatica la presa in carico della richiesta tramite email
6. Valutare la possibilità di una immediata soluzione in base alle procedure fornite e in presenza di richiesta già nota, e in tal caso procedere alla risoluzione e alla chiusura del ticket dando riscontro al richiedente
7. Nel caso di impossibilità a procedere direttamente, assegnare la richiesta ad un operatore tecnico specialista interno (1^ escalation) attraverso il sistema di ticketing interno. Nel caso di problemi bloccanti di particolare urgenza verrà attivato direttamente il personale tecnico interno di specifica competenza per una sua pronta attivazione sul problema.

Il **secondo livello di Help Desk** è costituito dal personale tecnico specialistico del NOC che si attiverà sulla richiesta nel sistema di ticketing in base alle specifiche competenze e in base alle assegnazioni del primo livello di Help Desk.

I compiti dell'Help Desk di secondo livello sono:

1. Valutare la possibilità di una immediata soluzione in base alle specifiche competenze e in presenza di richiesta già nota, e in tal caso procedere alla risoluzione e alla chiusura del ticket dando riscontro al richiedente.
2. Nel caso di impossibilità a procedere direttamente, assegnare la richiesta ad un operatore tecnico specialista esterno (2^ escalation).

La gestione del **terzo livello di Help Desk** è sempre in carico all'operatore interno del NOC che dovrà gestire la chiamata con il supporto esterno, solitamente identificato con il vendor del prodotto / servizio e le relative figure specializzate nella soluzione oggetto della richiesta.

I compiti dell'Help Desk di terzo livello sono:

1. Aprire una chiamata di intervento presso il supporto esterno / vendor
2. Gestire tutti i rapporti con il supporto esterno e il relativo intervento
3. Controllare l'esito dell'intervento del supporto esterno
4. Chiudere il ticket dando riscontro al richiedente

- **Gestione delle richieste e configurazioni standard (Request Fulfilment)**

Per Request Fulfillment si intende l'esecuzione di operazioni di riconfigurazione dei sistemi oggetto del servizio, dovute ad esigenze legate alla normale operatività, che implica un'attività di modifica che produce un cambiamento che può comportare un rischio di impatto gestibile.

Le attività di Request Fulfillment possono essere richieste solo su sistemi e tecnologie inclusi nel dominio di intervento dei servizi richiesti.

Le richieste sono classificate in due livelli:

Tipologia	Descrizione
Standard Change	Attività ricorrenti ben definite, la cui procedura di esecuzione è documentata, caratterizzate da basso rischio e basso impatto e con impegno non superiore alle 2 ore di attività da remoto. Queste attività si intendono preapprovate (in quanto richieste dagli operatori abilitati ad accedere al servizio), non richiedono cioè ulteriori autorizzazioni, possono essere svolte durante il normale orario lavorativo e non causano disservizi.
Minor Change	Attività di ordinaria amministrazione dei sistemi ICT con impegno complessivamente inferiore o uguale a 2 ore di attività da remoto, per le quali non esiste una procedura preapprovata. Sono attività a basso rischio e basso impatto. Sono soggette alla necessità di approvazione esplicita del Servizio Informatica qualora: • Riguardano sistemi business critical • Modificano politiche di sicurezza • Possono causare disservizi

Gli obiettivi di questo processo sono i seguenti:

- richiedere servizi standard per i quali esiste uno schema predefinito di approvazione;
- richiedere informazioni sui servizi disponibili e sulle procedure per ottenerli;
- ricevere l'erogazione dei servizi standard di cui sopra;
- ricevere assistenza su richieste generiche, consigli e lamentele.

Nell'ambito del processo di Request Fulfilment si definisce la **Service Request** come una richiesta rivolta al NOC per un'informazione, un consiglio, un cambiamento standard (standard change) o per un accesso ad un servizio IT. Per ogni tipologia di Service Request dovrà esserci un chiaro flusso di attività che determini la fornitura, o non approvazione, del particolare servizio all'utente.

Il processo in generale include le seguenti fasi:

- inoltro della Service Request al NOC, mediante il servizio di Help Desk o altre modalità;
- eventuale approvazione della richiesta;
- compimento della richiesta, anche da parte dello stesso Help Desk;
- chiusura della richiesta con verifica della soddisfazione.

Un ambito specifico di Request Fulfillment per il quale viene richiesto il supporto del NOC è la **gestione del sistema di backup**, che viene descritto in dettaglio nel relativo paragrafo dedicato.

Si richiede al NOC di supportare gli addetti del Servizio Informatica, e di operare in autonomia quando richiesto, per la messa a punto e la gestione del sistema di backup nell'ambito delle seguenti attività:

- definire ed implementare nel sistema di backup in uso le politiche di backup più adeguate alle esigenze che emergono di volta in volta da una analisi congiunta tra operatori del NOC e operatori del Servizio Informatica;
- schedulare i relativi job di backup sulla base delle politiche di backup definite;

- verificare la corretta esecuzione dei job di backup e implementare un sistema di notifica dell'esito dei job via email;
- intervenire proattivamente nel caso di job di backup falliti o non terminati correttamente per ripristinarne la corretta funzionalità;
- verificare la consistenza dei dati / sistemi sottoposti a backup mediante l'esecuzione di prove di ripristino pianificate con cadenza almeno mensile;
- eseguire il ripristino dei dati / sistemi sottoposti a backup nel caso di necessità su richiesta e indicazioni specifiche del Servizio Informatica.

f) <u>Servizio di supporto per la sicurezza IT tramite MDRS (Managed Detection & Response System) e CSIRT (Computer Security Incident Response Team)</u>

Il servizio di supporto per la sicurezza IT richiesto è finalizzato a far fronte alle minacce alla sicurezza informatica che richiedono un approccio di difesa innovativo e strategico che comprenda sia gli aspetti di prevenzione del rischio (ossia sistemi e processi finalizzati alla riduzione della probabilità che un determinato evento avverso possa verificarsi), sia la capacità di identificare la presenza di attacchi e minacce non ancora noti, e di gestirne gli effetti riducendone gli impatti sull'operatività del Sistema IT o di sue specifiche parti.

In quest'ottica viene richiesta l'erogazione di un servizio di **Cyber Security** in grado di soddisfare le seguenti esigenze:

- migliorare l'efficacia complessiva della protezione del Sistema IT IZSVe ottimizzando la capacità di identificare minacce alla sicurezza informatica;
- riconoscere rapidamente i segnali di intrusioni in corso all'interno del perimetro monitorato;
- determinare la natura e le caratteristiche dell'attacco mediante specifiche attività di investigazione;
- elaborare in modo rapido ed efficace le azioni di contenimento e rimozione dell'intrusione;
- coordinare efficacemente le azioni di mitigazione e la capacità di ridurre gli impatti degli attacchi;
- comprendere come perfezionare i controlli di sicurezza per riuscire a bloccare futuri tentativi di attacco.

Il servizio di supporto per la sicurezza IT dovrà essere espletato nel rispetto delle seguenti modalità, da intendersi quali caratteristiche tecniche minime richieste <u>a pena di inammissibilità dell'offerta alla procedura</u>:

- erogazione in modalità *as a service*: le componenti principali del sistema devono risiedere presso il fornitore con esclusione del sistema VPN per il collegamento all'infrastruttura IT IZSVe;
- espletamento del servizio mediante i seguenti processi e secondo le specifiche esplicitate successivamente:
    - **Sistema MDRS (Managed Detection & Response System)**
    - **Servizio CSIRT (Computer Security Incident Response Team)**

➢ **Sistema MDRS (Managed Detection & Response System)**

Il **Sistema MDRS** deve essere composto da un insieme di servizi e soluzioni in grado di monitorare e intervenire in tutti gli scenari di rischio associati ad attacchi di *cybercrime*, tra i quali i più importanti sono:

- presenza di malware, talvolta basati su attacchi a vulnerabilità di tipo Zero-Day;
- malware Targeted ed Advanced Persistent Threat (APT);
- attacchi diretti verso applicazioni (es. attacchi di tipo Server-side);
- frodi informatiche (es. Phishing, CEO Fraud, ecc.);
- distributed Denial of Service;
- sfruttamento di vulnerabilità note.

La suite di servizi **MDRS (Managed Detection & Response System)** dovrà fornire una infrastruttura tecnologica *as a service* - residente presso il fornitore - in grado di rilevare gli attacchi verso il Sistema IT IZSVe e di

offrire tutti gli elementi necessari per individuare e rispondere efficacemente alle intrusioni informatiche attraverso il supporto del **CSIRT (Computer Security Incident Response Team).**

L'erogazione del servizio di Managed Detection & Response dovrà avvenire attraverso una soluzione trasversale rappresentata da una **Piattaforma SOAR (Security Orchestration, Automation and Response)** e da una serie di **moduli di detection (Endpoint Detection Module)** che sono deputati alla raccolta di tutte le informazioni necessarie a delineare gli scenari di rischio ed attacco informatico elencati in precedenza.

Piattaforma SOAR - Security Orchestration, Automation and Response

La **Piattaforma SOAR** memorizza e organizza tutte le informazioni raccolte dai moduli di detection ed abilita l'erogazione del servizio MDRS mediante l'interazione diretta tra il Servizio Informatica IZSVe e il team di specialisti CSIRT per favorire l'orchestrazione dei processi e la gestione completa di un incidente di sicurezza durante tutte le fasi previste.

La Piattaforma SOAR deve essere accessibile e gestibile tramite un portale web, utilizzato per il tracciamento di tutti i processi relativi al servizio erogato e la gestione degli incidenti di sicurezza.

I processi di identificazione, analisi e gestione degli incidenti di sicurezza oggetto del servizio prevedono tipicamente la seguemnte serie di fasi:

1. I **moduli di detection** attivati nella porzione di infrastruttura dell'IZSVe che si intende analizzare raccolgono informazioni ed eventi di diverse tipologie, come ad esempio: il traffico di rete, il comportamento di un processo in esecuzione su un sistema, il rilevamento di una vulnerabilità, ecc.
2. Tramite l'applicazione di **logiche di correlazione** proprietarie e non i moduli di detection evidenziano la presenza di possibili condizioni anomale e le inviano, unitamente ai dati di contesto che hanno causato la specifica condizione, alla piattaforma centralizzata del fornitore, tramite l'utilizzo di canali di comunicazione cifrati e sicuri.
3. Gli eventi identificati come potenzialmente anomali vengono arricchiti con informazioni tattiche di *Threat Intelligence*, e resi disponibili al Team di Incident Response (CSIRT) che, tramite una console dedicata ed integrata nel portale web della Piattaforma SOAR, procede con la **fase di investigazione**.
4. Gli analisti di primo livello verificano gli allarmi attivati con opportune procedure di investigazione e definiscono con precisione la natura dell'anomalia e determinano l'eventuale attribuzione ad un problema di sicurezza:
    4.1. Se le analisi confermano la presenza di una minaccia, di un tentativo concreto di intrusione o di un Data Breach, il Team di Incident Response (CSIRT) procede all'**apertura di un incidente di sicurezza** utilizzando l'apposita sezione dedicata nel portale web della Piattaforma SOAR (specifico **sistema di ticketing**): il servizio CSIRT prende in carico e gestisce gli incidenti di sicurezza rilevati e mette in atto la **fase di incident response**.
    4.2. Se gli eventi analizzati non rappresentano una reale minaccia di sicurezza da gestire (es. falsi positivi o attacchi non andati a buon fine), i relativi allarmi vengono chiusi ed archiviati, rimanendo consultabili a posteriori sul portale web.

Piattaforma SOAR – Portale web

Il portale web della Piattaforma SOAR rappresenta l'interfaccia tra il team di sicurezza del fornitore e il Servizio Informatica dell'IZSVe. Il portale web permette al cliente di accedere alle proprie dashboard, agli alert, agli incident di sicurezza generati ed a tutte le informazioni relative alle varie fasi della gestione dell'incidente.

La home page del portale web deve indicare graficamente la situazione generale sullo stato degli incidenti e degli allarmi rilevati ed analizzati dal Team di Incident Response.

Nel dettaglio il portale web deve fornire le seguenti statistiche:

- Numero di incidenti di sicurezza negli ultimi 30 giorni e/o altri periodi di tempo selezionabili
- Numero di attacchi di sicurezza negli ultimi 30 giorni e/o altri periodi di tempo selezionabili
- Evidenza e dettaglio dei ticket aperti sulla piattaforma

- Elenco dei task di containment, eradication e post-incident, da portare a termine all'interno del processo di gestione dei ticket aperti
- Stato degli incidenti aperti sulla piattaforma e numero di task ancora aperti, in sospeso e chiusi
- Informazioni di dettaglio sul traffico analizzato dai moduli di detection.

Da specifiche sezioni del portale deve essere possibile accedere alle informazioni relative agli allarmi / ticket scattati, analizzati e gestiti dal servizio CSIRT:

- **Allarmi**: analisi sommaria / dettagliata dell'evento, cause che hanno scatenato l'allarme, rispettivi task di remediation e motivo per cui è stato gestito e chiuso dal Team di Incident Reponse.
- **Tickets**: elenco dei ticket aperti e dettagli completi degli incidenti di sicurezza presi in carico e gestiti dal Team di Incident Reponse:
    - La descrizione generale dell'evento / allarme
    - Livello di 'global severity' dell'incidente / allarme (calcolata su parametri di Confidenzialità, Integrità, Disponibilità)
    - Analisi tecnica dell'evento / allarme
    - Dati di base degli eventi che hanno generato l'evento / allarme
    - Ulteriori informazioni utili per l'analisi raccolte durante il processo di investigazione
    - Descrizione dettagliata delle fasi di incident response (containment ed eradication)
    - Descrizione di eventuali attività di post incident

Piattaforma SOAR – Mobile App

Oltre all'accesso al portale web è richiesta la possibilità di accedere alla Piattaforma SOAR e alle informazioni sugli allarmi / incidenti attraverso una **applicazione Mobile**, disponibile sugli store di Apple IOS e Android.

Attraverso l'utilizzo di notifiche push direttamente sull'applicazione, il Servizio Informatica dell'IZSVe viene informato della presenza di attacchi o compromissioni relative alla propria infrastruttura e può seguire lo svolgimento delle azioni di Remediation Proposal e Incident Response.

Moduli di detection - Endpoint Detection Module

I moduli di detection (**Endpoint Detection Module**) sono l'unica componente del sistema MDRS installata presso l'infrastruttura dell'IZSVe, nei dispositivi endpoint che costituiranno il perimetro di gestione del servizio di supporto per la sicurezza IT: gli endpoint oggetto di questo specifico servizio rientrano nel complessivo dominio di intervento dell'infrastruttura IT oggetto di gara, ma verranno definini e individuati dal Servizio Informatica dell'IZSVe in **numero massimo di 100**, tra i dispositivi con sistema operativo Microsoft Windows, Linux (Red Hat, CentOS) e Mac OSX.

Il modulo di detection del servizio è basato sull'utilizzo di un agente di analisi forense attivato sui sistemi client e server maggiormente critici che verranno identificati dal Servizio Informatica, che attiverà i moduli tramite l'installazione di un agent software di telemetria che permette di ottenere un livello di visibilità massima sugli endpoint.

Gli agent devono avere un basso impatto in termini di utilizzo delle risorse e sulle prestazioni dei sistemi, e consentire di monitorare costantemente le attività dei processi e dei servizi in esecuzione sui sistemi, relativamente alle operazioni sul file system, alle connessioni di rete utilizzate, alle operazioni di scrittura sul registry di Windows, ecc. al fine di identificare particolari condizioni di anomalia.

Ogni anomalia / minaccia rilevata dai sensori viene trasmessa direttamente e tracciata nel sistema centralizzato della Piattaforma SOAR residente presso il fornitore / in cloud, senza passare per l'infrastruttura dell'IZSVe, per poi essere presa in carico e analizzata dai tecnici specialisti del servizio CSIRT.

- **Servizio CSIRT (Computer Security Incident Response Team)**

Il servizio di sicurezza IT richiesto si basa sulle competenze e funzioni del **CSIRT (Computer Security Incident Response Team)** erogate in modalità *as a service* con **copertura 24/7/365** (copertura continua e ininterrotta: 24

h / giorno; 7 giorni / settimana; 365 giorni / anno). Il Servizio Informatica dell'IZSVe avrà a disposizione un team di tecnici specializzati dedicati al rilevamento, all'analisi e alla gestione degli incidenti di sicurezza informatica, il cui obiettivo principale è quello attuare la fase di **Incident Response**: tradurre la complessità di un problema di sicurezza informatica in un flusso di attività sistemistiche (**Remediation Proposal**) da comunicare direttamente al Servizio Informatica e/o al servizio esterno di NOC (Network Operation Center) per l'adozione operativa delle misure di contenimento e gestione necessarie per la risoluzione dell'incidente di sicurezza rilevato.

La suite di servizi MDRS fornisce all'IZSVe una infrastruttura tecnologica *as a service* in grado di rilevare automaticamente gli attacchi verso i propri sistemi IT, mentre il servizio del CSIRT offre le competenze necessarie per rispondere efficacemente alle intrusioni informatiche rilevate, mediante un supporto qualificato e competente per contenere la propagazione dell'attacco, ripristinare i sistemi coinvolti ed elaborare metriche di intervento che consentano di valutare e migliorare l'efficacia dei propri sistemi di sicurezza preventiva (es. Firewall, Antivirus, Secure Web Gateway, Intrusion Prevention System, Antispam, ecc.) nonché il reale livello di rischio.

Nello svolgimento delle attività di gestione degli incidenti di sicurezza il servizio CSIRT deve fare riferimento ai principali **framework di Cyber Security** ed adottare le seguenti raccomandazioni / standard:

- Computer Security Incident Handling Guide
- NIST© Special Publication 800-61 Rev. 2
- ISO/IEC 27035 Information technology — Security techniques — Information security incident management
- CMU Handbook for Computer Security Incident
- Response Teams (CSIRTs)

Gestione degli incidenti di sicurezza – fasi di incident Response

Ogni **incidente di sicurezza** viene gestito dal Team di Incident Response - CSIRT seguendo le linee guida del *framework del NIST (800-61 Rev. 2)* ed è suddiviso logicamente per eseguire le seguenti diverse **fasi di Incident Response**:

1) Ogni incidente viene classificato sulla base di una **analisi della minaccia** rilevata (sommaria e di dettaglio) in un **severity level**: **1** (**Informational**); **2** (**Low impact**); **3** (**Moderate impact**); **4** (**High impact**); **5** (**Critical impact**).
2) Unitamente all'analisi viene proposta una **Remediation Proposal** suddivisa per fasi / task, che viene condivisa con il Servizio Informatica ed eventualmente con il servizio NOC e che contiene un elenco di attività puntuali che il Team di Incident Response consiglia di applicare - nel più breve tempo possibile – per gestire adeguatamente la procedura di risposta, garantendo il contenimento della minaccia e la rimozione della stessa dai sistemi impattati.
3) Ad ogni incidente che richiede un intervento del NOC esterno, il Team di Incident Response effettuerà l'**apertura di un ticket di sicurezza** direttamente al servizio NOC (mediante le rispettive modalità descritte nel relativo paragrafo di Incident Management / primo livello di Help Desk) che dovrà applicare i task previsti dalla Remediation Proposal.
4) Sulle tipologie di incidenti informatici che richiedono la massima rapidità di risposta ai fini del contenimento degli impatti e delle conseguenze dell'attacco, in modo concordato tra Servizio Informatica, servizio CSIRT e NOC esterno, verranno preventivamente determinate la casistiche per le quali **automatizzare le specifiche azioni di contenimento** (es. blocco di un indirizzo IP sul firewall, ban di un processo in esecuzione su un sistema, isolamento di un host infetto dalla rete, ecc.).
5) Una volta applicate le azioni di contrasto e di rimozione della minaccia, l'incidente può considerarsi concluso e il Team di Incident Response, valutata la situazione, può far seguire un'analisi post-mortem con l'obiettivo di identificare le *root cause* dell'evento, fornendo indicazioni di carattere tecnologico e/o di processo, con l'obiettivo di **incrementare la resilienza dell'infrastruttura** ad attacchi informatici della stessa tipologia.
6) Infine il servizio CSIRT deve provvedere a formulare e fornire al Servizio Informatica dell'IZSVe un **bollettino di sicurezza**, da inviare via email almeno ogni mese, che contiene l'analisi e le eventuali indicazioni di prevention / containment che possono essere intraprese per ridurre i rischi di impatto di

minacce informatiche in caso di presenza di vulnerabilità note particolarmente critiche o di campagne di spam / malware attive e particolarmente aggressive e diffuse a livello nazionale ed internazionale.

g) Giornate di supporto specialistico

Viene inclusa nell'erogazione del servizio generale richiesto la fornitura al personale del Servizio Informatica di **giornate di supporto specialistico** necessario e utile all'analisi e alla progettazione di sviluppi evolutivi dell'infrastruttura del Sistema IT dell'IZSVe, nel suo complesso o in sue parti specifiche.

Sono comprese anche eventuali attività di *hands-on training* e proposte di adozione di soluzioni innovative o migliorative rispetto a quelle attualmente utilizzate.

Sono comprese in generale tutte le attività di intervento per installazione e avviamento di nuovi sistemi informatici sia hardware che software oltre che il supporto per implementare aggiornamenti rilevanti (update/upgrade di sistema e di sicurezza, passaggio a nuove release dei prodotti e servizi, ecc.) a tutti i sistemi inclusi nel dominio di intervento del servizio. Tali attività specifiche verranno concordate con il Servizio Informatica e svolte da tecnici specialisti fuori dall'ambito ordinario del NOC (Incident Management / Request Fulfilment) e del SOC.

Le attività erogate nell'ambito delle giornate di supporto specialistico dovranno essere svolte da tecnici informatici adeguatamente formati ed in possesso delle competenze tecniche richieste dalle specifica attività di volta in volta analizzate e definite in collaborazione con gli operatori del Servizio Informatica. Tali attività dovranno essere erogate da remoto o in presenza onsite (presso la sede centrale dell'IZSVe) secondo le esigenze contestuali, anche in giornate non lavorative o fuori orario di lavoro; l'analisi dell'attività richiesta e la pianificazione dell'erogazione degli interventi deve avvenire entro 10 giorni lavorativi dalla data della richiesta inoltrata al fornitore dal Servizio Informatica.

Si precisa che saranno comprese nel canone n. 10 giornate, per ogni anno di contratto, di supporto specialistico; ulteriori giornate supplementari saranno specificatamente richieste dall'Istituto e remunerate applicando i prezzi offerti dall'appaltatore in sede di gara, aggiunti gli eventuali costi per l'eliminazione dei rischi interferenziali.

5. DESCRIZIONE DEL DOMINIO DI INTERVENTO DEI SERVIZI RICHIESTI

Il dominio di intervento dei servizi richiesti è riconducibile all'infrastruttura del Sistema IT dell'IZSVe, gestito direttamente dal Servizio Informatica insieme ai vari partner tecnologici. Esso è costituito da elementi fisici e logici presenti principalmente nel Data Center (dove sono ospitati tutti i server e i dispositivi tecnologici che costituiscono l'asset IT centralizzato dell'Istituto) e dall'infrastruttura della rete dati aziendale (insieme degli apparati che interconnettono l'asset IT periferico dell'Istituto collegando tra loro gli edifici del campus della sede centrale, la sede con i laboratori periferici e l'Istituto con la rete Internet).

A livello macro, il **dominio di intervento dei servizi richiesti** è composto dalle seguenti categorie di oggetti:

- Sistemi di rete LAN / WAN
- Sistema di rete WiFi
- Infrastruttura del Data Center
- Sistemi server / storage
- Hypervisor / sistemi operativi
- Sistema di sicurezza perimetrale
- Sistema di sicurezza server
- Sistema di sicurezza client
- Sistema di backup
- Sistema di posta elettronica / antispam

Vengono di seguito descritti gli oggetti attivi all'interno del Sistema IT e dell'infrastruttura tecnologica che caratterizza l'IZSVe sui quali devono agire i servizi richiesti all'interno della presente gara; tali oggetti potranno subire un incremento fino al 20% senza che questo comporti alcuna variazione degli oneri contrattuali.

a) Schema generale

Il Sistema IT IZSVe è basato su un'**infrastruttura di rete geografica** che interconnette i vari edifici del campus della sede centrale con il Data Center aziendale, e collega la sede centrale con le 10 sedi periferiche territoriali tramite una rete MPLS Fastweb con topologia a stella.

Il centro stella della rete geografica è la sede centrale di Legnaro (PD), dove risiede il Data Center che ospita tutti i principali servizi del sistema informatico, gli accessi a Internet e il sistema di difesa perimetrale.

b) Sistemi di rete LAN / WAN

Il sistema della rete dati aziendale è composto da apparati di rete ethernet classificabili principalmente nelle seguenti categorie:

- **Switch di core** (collocati nella sala server del Data Center in sede centrale):
  - N. 2 Switch Cisco Catalyst 3850 48 Port 10G Fiber
  - N. 4 Switch Cisco Catalyst 2960-X 48 GigE, 2 x 10G SFP
- **Switch di backup** (collocati nella sala di backup in sede centrale):
  - N. 1 Switch Cisco Catalyst 2960-X 48 GigE, 2 x 10G SFP
- **Switch periferici** (distribuiti tra sede centrale e sedi periferiche come punti di accesso delle postazioni di lavoro e dei dispositivi ethernet):
  - N. 65 circa Switch HP ProCurve 2910-24G/48G e HP Aruba 2920-24G/48G

La connettività della rete MPLS che collega la sede centrale e le sedi periferiche è garantita dal provider Fastweb che ha in gestione e manutenzione tutti i router e gli apparati di backup. Su questa connettività è richiesto che vengano monitorati i link di collegamento tra le sedi, che devono essere compresi nel sistema di notifica e allarme nel caso di interruzione del collegamento.

Negli switch della LAN del campus della sede centrale sono configurate e distribuite le seguenti VLAN:

NOME	DESCRIZIONE
DATI	Subnet di produzione primaria
LAB	Subnet dei laboratori e strumenti NGS (Bioinformatica)
NGS	Subnet dell'infrastruttura NGS (Bioinformatica)
DMZ	Subnet DMZ con servizi esposti
GUEST	Subnet IZSVE-GUEST per dispositivi WiFi
PUB	Subnet per apparati link Internet GARR (IP pubblici)
VOIP	Subnet per centrali telefoniche VoIP
PUB2	Subnet per apparati link Internet Fastweb (IP pubblici)
vMotion	Subnet per vMotion VMware
NFS	Subnet per NFS (UCS/NetApp - Core)
MGMT	Subnet di management

c) Sistema di rete WiFi

La rete dati aziendale è integrata da un **sistema di rete WiFi** basato su tecnologia Cisco (Cisco 5508 Wireless Controller e Cisco Aironet Access Point).

Sono attivi n. 35 punti di accesso alla rete wireless, distribuiti nei vari uffici e laboratori della sede centrale e delle sedi periferiche, da cui è possibile collegarsi a 2 reti WiFi:

- **IZSVE-GUEST**: rete dedicata agli utenti ospiti esterni, mediante la quale possono avere l'accesso a Internet con qualsiasi dispositivo wireless. L'utilizzo della rete è protetto da credenziali di accesso fornite preventivamente dal Servizio Informatica.
- **IZSVE-NETWORK**: rete dedicata al personale interno, mediante la quale gli utenti possono avere accesso a tutti i servizi IT IZSVe soltanto con dispositivi wireless aziendali. L'utilizzo della rete è protetto da chiave di accesso e filtro mac-address preventivamente configurati dal Servizio Informatica. I dispositivi che si collegano alla rete aziendale mediante questo accesso sono sottoposti a tutte le policy di sicurezza standard per le postazioni di lavoro aziendali.

d) Infrastruttura del Data Center

Il Data Center aziendale è costituito da una sala server collocata al secondo piano dell'Edificio A nella sede centrale. La **sala server** è composta da una fila di n. 5 armadi rack dove sono installati gli apparati attivi di core del Sistema IT IZSVe: router, switch, server e storage, e tutti i relativi accessori (attestazione linee dati, link in rame / fibra ottica tra apparati, ecc.).

L'alimentazione elettrica degli armadi rack è garantita da un UPS Schneider Electric Symmetra PX 2.

Il raffreddamento della sala server è garantito da due climatizzatori ambientali Daikin.

Attualmente la sala server non è dotata di un sistema specifico di rilevazione e spegnimento incendi.

Il monitoraggio ambientale della sala server (temperatura, umidità, ecc.) è garantito da un sistema di sensori gestito dal modulo APC NetBotz 455.

Una seconda **sala backup** è collocata al primo piano dell'Edificio A ed ospita un armadio rack che contiene gli apparati del sistema di backup (switch, server, storage, libreria nastri), alimentato da un UPS APC Smart-UPS SRT 3000. La sala backup e la sala server principale sono collegate da link in fibra ottica.

e) Sistemi server / storage

Il sistema server / storage di produzione è costituito principalmente da un ambiente virtuale basato su **VMware vCenter Server Ver. 6.7** che è supportato dalla seguente infrastruttura fisica collocata nella **sala server del Data Center** aziendale:

- **Blade Server**:
  - N. 1 Cisco UCS 5100 Blade Server Chassis (8 slot Blade Server)
  - N. 3 Cisco UCS B200 M4 Blade Server (84 CPU, 1 TB RAM)
  - N. 2 Cisco UCS B200 M5 Blade Server (48 CPU, 750 GB RAM)
  - N. 2 Cisco UCS 6324 Fabric Interconnect (link NFS verso core switch)
- **Storage SAN**:
  - N. 1 Storage SAN NetApp FAS-2554 (40 TB su dischi SATA / SAS)
  - N. 1 Storage SAN NetApp AFF-A220 (12 TB su dischi SSD)

Inoltre l'infrastruttura fisica server / storage è integrata dai seguenti dispositivi:

- Data Center / sala server:
  - N. 1 Server DELL PowerEdge R630 (Application Server)
- Data Center / sala backup:
  - N. 1 Server Cisco UCS C240 M4 (Backup server primario)
  - N. 1 Server HP ProLiant DL380e (Backup server secondario)
  - N. 1 Storage SAN NetApp E2812 (Storage di backup: 60 TB su dischi SAS)
  - N. 1 Quantum SuperLoader 3 LTO7 (Libreria nastri)

f) Hypervisor / sistemi operativi

Sulla base della infrastruttura fisica descritta nel precedente paragrafo sono attivi circa 160 server, fisici e virtuali in ambiente basato su **Hypervisor VMware vCenter Server Ver. 6.7**, strutturato in **N. 2 Cluster in High Availability** gestiti da **N. 2 vCenter Server** denominati rispettivamente SRV-IZSV-VCenter (N. 3 host ESXi in HA) e SRV-IZSV-VCenter2 (N. 2 host ESXi in HA).

Oltre ai **server di sistema** (con sistema operativo VMware ESXi, VMware Photon, NetApp Data Ontap, ecc.), i server applicativi hanno principalmente il sistema operativo **Microsoft Windows Server** (Versioni 2008 R2, 2012, 2016 e 2019) e **Linux** (Distribuzioni Ubuntu, Debian, CentOS).

Il sistema client/server dell'IZSVe è basato su un dominio **Microsoft Active Directory** strutturato con 2 Domain Controller situati nel campus della sede centrale a cui fanno richiesta di login tutti i sistemi Windows inseriti in dominio: i Server Windows e i client Windows 7/8/10 della sede centrale (circa 600 postazioni di lavoro) e delle 10 sedi periferiche (circa 300 postazioni di lavoro).

Tutte le principali policy di configurazione sono impostate nei DC centrali e vengono distribuite ai server/client periferici in dominio mediante GPO.

Gli aggiornamenti dei sistemi operativi Windows (Windows Update) sono gestiti e distribuiti mediante un servizio centralizzato Windows Server Update Services (WSUS).

g) Sistema di sicurezza perimetrale

Il sistema di sicurezza perimetrale attivo per la protezione del Sistema IT dell'IZSVe è composto da due appliance firewall **Check Point 5400 Security Gateway** in alta affidabilità.

La gestione del sistema si basa su Security Management Server versione R80.30 su sistema operativo Check Point Gaia.

Nel sistema sono attivi i servizi di sicurezza compresi nel NGTX Security Package che include i servizi di IPS, Anti-Bot, Antivirus, Application Control, URL filtering, IPSec VPN, Email security, Threat Emulation e Threat Extraction.

h) Sistema di sicurezza server

Il sistema che gestisce la sicurezza informatica dei server fisici e virtuali è basato sulla piattaforma **Trend Micro Deep Security** che dispone delle seguenti funzionalità:

- *Anti-Malware*: funzionalità di sicurezza di base con protezione da virus, spyware, trojan e altre minacce informatiche.
- *Web reputation*: funzionalità di content filtering su web browsing per rafforzare la protezione per server e desktop virtuali.
- *IPS (Intrusion Prevention System)*: funzionalità di blocco di attacchi che sfruttano vulnerabilità note mediante virtual patching e analisi del traffico in entrata e in uscita.
- *Firewall*: funzionalità di agent firewall che riduce le possibilità di attacco ai server mediante filtraggio granulare del traffico IP.

i) Sistema di sicurezza client

Il sistema che gestisce la sicurezza informatica dei client / endpoint con sistema operativo Windows 7/8/10 è basato sulla piattaforma **Trend Micro Apex One**.

Il sistema gestisce la sicurezza di 900 client / postazioni di lavoro (600 circa in sede centrale e 300 circa nelle sedi periferiche) e dispone delle seguenti funzionalità:

- *Anti-Malware*: funzionalità di sicurezza di base con protezione da virus, spyware, trojan e altre minacce informatiche.
- *Web reputation*: funzionalità di content filtering su web browsing per rafforzare la protezione nelle varie postazioni di lavoro.
- *Endpoint Application Control*: funzionalità di blocco di esecuzione di software dannoso utilizzando criteri personalizzabili ed elenchi di utenti autorizzati / non autorizzati.
- *DLP*: funzionalità di individuazione, monitoraggio e prevenzione della perdita di dati.

j) Sistema di backup

Il **backup dei dati** relativi ai servizi attivi e supportati dai sistemi server / storage (descritti nel paragrafo 6.5) viene eseguito mediante il software **CommVault** secondo le seguenti backup policy:

- **Livello 1: Backup su disco**
  - Destinazione: dati salvati su SAN (Storage di backup NetApp E2812)
  - Tipo / frequenza: backup completi eseguiti con frequenza settimanale
  - Tipo / frequenza: backup incrementali eseguiti con frequenza giornaliera
  - Retention dati standard: 4 settimane (sovrascrittura dopo 1 mese)
  - Retention dati CIFS: 1 anno
- **Livello 2: Backup su nastro**
  - Destinazione: dati salvati su supporti magnetici (Libreria nastro Quantum LTO7) e successivamente conservati in cassaforte ignifuga
  - Tipo / frequenza: backup completi eseguiti con frequenza mensile
    Retention: dati conservati all'infinito (nessuna sovrascrittura)

Sono sottoposti al sistema di backup i seguenti sistemi:

- Client Windows: 28
- Server Windows: 29
- Server Linux: 1
- VM VMware: 11
- CIFS Volume: 1

Il sistema di backup gestisce complessivamente circa **15 TB di dati** distribuiti come segue:

Agent Type	Data Written	Number of Clients
Windows File System	8.51 TB	64
NDMP	2.17 TB	1
Exchange Database	1.33 TB	3
Windows 2003 32-bit File System	247.21 GB	1
Exchange Mailbox (Classic)	176.93 GB	1
PostgreSQL	146.61 GB	2
Virtual Server	63.56 GB	2
CommServe Management	62.78 GB	1
SQL Server	61.07 GB	8
Big Data Apps	14.81 GB	6
MySQL	1.42 GB	3
Active Directory	655.38 MB	3
Exchange Public Folder	186.67 MB	1

k) Sistema di posta elettronica / antispam

Il **sistema di posta elettronica** istituzionale che gestisce il dominio **@izsvenezie.it** è basato sulla piattaforma **Microsoft Exchange Server** ed ha le seguenti caratteristiche:

- N. 1 Virtual Server Exchange Server 2016
- N. 1 Virtual Server Reverse Proxy
- N. 870 circa mailbox attive
- Servizio di accesso alle mailbox via Microsoft Outlook
- Servizio di accesso alle mailbox via Webmail OWA

La sicurezza del sistema di posta elettronica è gestito mediante il servizio antispam **Trend Micro IMSVA** (Interscan Messaging Security Virtual Appliance) che regola e analizza il flusso dei messaggi secondo le seguenti policy:

- Messaggi in ingresso:
  - Filtro firewall scan dei messaggi in ingresso
  - Servizi di antivirus, DNSBL, sender reputation
  - Blocco degli allegati in base a block list definite
  - Black list e white list dei domini di provenienza
  - Servizio di quarantena e rilascio dei messaggi di spam bloccati
- Messaggi in uscita:
  - Servizio di relay per i messaggi in uscita
  - Servizio di monitoraggio messaggi in uscita (malware, content, mass-mailing, ecc.)
  - Gestione del limite dei destinatari, peso allegati, ecc.

Sono inoltre attivi i seguenti servizi correlati al sistema di posta elettronica:

- Servizio di provider backup/relay in cloud per i messaggi in ingresso
- Servizio di SMTP Relay in cloud (Mailjet.com) per mass-mailing istituzionale in uscita

6. SERVICE LEVEL AGREEMENT (SLA) E INDICATORI DI QUALITÀ DEL SERVIZIO

I **livelli di servizio** (**Service Level Agreement - SLA**) richiesti per il servizio di **NOC** (Incident Management e Request Fullfillment) sono i seguenti:

- **Copertura oraria**: 8:00-12:30, 14:30-18:00; dal lunedì al venerdì.
- **Tempo di richiamata** (inteso come tempo per la presa in carico della segnalazione e la raccolta delle informazioni calcolato dal tempo della richiesta inoltrata al NOC: apertura ticket / allarme per Incident Management; service request per Request Fulfilment): **massimo 2 ore calcolate all'interno della copertura oraria richiesta**.
  - Esempi: una richiesta inoltrata al NOC alle ore 17.00 del lunedì dovrà essere presa in carco entro le ore 9.00 del martedì; una richiesta inoltrata al NOC alle ore 17.00 del venerdì dovrà essere presa in carco entro le ore 9.00 del lunedì; una richiesta inoltrata al NOC alle ore 7.00 del lunedì dovrà essere presa in carco entro le ore 10.00 del lunedì stesso.
- **Tempo di intervento remoto** (inteso come tempo di inizio dell'erogazione dell'intervento che decorre dal tempo di richiamata): **massimo 6 ore calcolate all'interno della copertura oraria richiesta** (livello standard), tranne nel caso di incident classificato come 'critico' per cui il tempo di intervento remoto deve essere di **massimo 2 ore calcolate all'interno della copertura oraria richiesta**.
  - Esempi: l'inizio dell'erogazione di un intervento riferito ad una richiesta inoltrata al NOC alle ore 15.00 del lunedì dovrà avvenire entro le ore 11.00 del martedì, mentre nel caso di incident 'critico' entro le ore 17.00 del giorno stesso.
- **Tempo di risoluzione** (inteso come tempo per il ripristino dell'operatività ordinaria dalla richiesta inoltrata al NOC): **massimo 24 ore calcolate all'interno della copertura oraria richiesta** (livello

standard), tranne nel caso di incident classificato come 'critico' per cui il tempo di risoluzione deve essere entro **8 ore calcolate all'interno della copertura oraria richiesta**.

- Esempi (per incident critico): una richiesta inoltrata al NOC alle ore 10.00 del lunedì dovrà essere risolta entro le ore 10.00 del martedì; una richiesta inoltrata al NOC alle ore 10.00 del venerdì dovrà essere risolta entro le ore 10.00 del lunedì; una richiesta inoltrata al NOC alle ore 7.00 del lunedì dovrà essere risolta entro le ore 18.00 del lunedì stesso.

Il fornitore sarà tenuto al rispetto dei tempi di risoluzione indicati per tutte le attività previste all'interno del perimetro / dominio di intervento.

Non saranno tenuti in considerazione ai fini del rispetto dei livelli di servizio richiesti:

- Le tempistiche di esecuzione degli interventi riconducibili a fornitori terzi;
- Le tempistiche di esecuzione degli interventi di manutenzione ordinaria e programmata delle tecnologie non a perimetro, che comunque con queste si interfaccino;
- Le tempistiche di esecuzione degli interventi di manutenzione straordinaria da effettuarsi con urgenza che dovessero impedire l'intervento di supporto tecnico da parte dell'aggiudicatario (a titolo esemplificativo, il caso in cui un intervento necessario ai dispositivi di networking dovesse interrompere la connettività utilizzata per il collegamento VPN da parte dell'aggiudicatario);
- I fattori al di fuori della sfera di controllo dell'aggiudicatario o fuori dell'ambito dei Servizi, tali da impedire oggettivamente di eseguire i Servizi (a titolo meramente esemplificativo e non esaustivo, fattori inerenti all'infrastruttura esterna di rete e/o ai soggetti deputati alla sua gestione);
- L'inattività dell'aggiudicatario per causa, anche accidentale, imputabile all'ente o a terzi, inclusi, a titolo esemplificativo ma non esaustivo, eventuali interventi all'infrastruttura hardware/software effettuati autonomamente dall'Istituto senza la preventiva autorizzazione dell'aggiudicatario;
- Eventi di forza maggiore (quali a titolo esemplificativo ma non esaustivo incendi, alluvioni, terremoti, ecc).

Viene richiesto di monitorare e rendere disponibili alcuni **indicatori di qualità del servizio** per ogni anno di erogazione del servizio di Incident Management, o comunque quando richiesti dal Servizio Informatica, secondo le seguenti metriche di controllo, rilevate su base mensile e utili alla misurazione delle performance di processo:

- Statistiche aggregate e di dettaglio sulle richieste / ticket aperti: percentuali di ticket risolti e non risolti, classificazione per priorità / tipologia / ambito / tecnologia, ecc.
- Confronto delle statistiche tra diversi anni di erogazione del servizio e analisi della tendenza generale e specifica per tipologia di richieste / ticket.
- Percentuale di incidenti risolti al primo livello di Help Desk, per misurare la qualità della Knowledge Base (richieste non scalate).
- Percentuale di incidenti risolti al momento del contatto, per misurare l'aderenza dell'Incident Management alla situazione ideale (richieste risolte molto velocemente).
- Percentuale di incidenti assegnati in modo non corretto, per misurare la bontà dei processi di assegnazione (richieste erroneamente classificate).
- Percentuale di incidenti risolti entro i livelli di SLA, per misurare la capacità di risolvere gli incidenti secondo gli standard richiesti (richieste evase regolarmente).
- Tempo medio di risoluzione degli incidenti, per misurare la qualità e l'efficienza generale del processo di Incident Management.
- Percentuale di incidenti con categorizzazione non corretta, per misurare l'accuratezza e l'utilizzabilità dei dati prodotti dall'Incident Management.
- Percentuale di incidenti risolti correttamente al primo tentativo, per misurare l'efficienza generale del processo.

I **livelli di servizio** (**Service Level Agreement - SLA**) richiesti per la fase di **Incident Response** del servizio di sicurezza erogato dal **CSIRT** (Computer Security Incident Response Team), in base al relativo *severity level* sono i seguenti:

- **Severity level 1** (**Informational**): notifica incidente al Servizio Informatica / apertura di un ticket di sicurezza al servizio NOC in **massimo 6 ore**; presa in carico in **massimo 24 ore**.
- **Severity level 2** (**Low impact**): notifica incidente al Servizio Informatica / apertura di un ticket di sicurezza al servizio NOC in **massimo 4 ore**; presa in carico in **massimo 12 ore**.
- **Severity level 3** (**Moderate impact**): notifica incidente al Servizio Informatica / apertura di un ticket di sicurezza al servizio NOC in **massimo 2 ore**; presa in carico in **massimo 8 ore**.
- **Severity level 4** (**High impact**): notifica incidente al Servizio Informatica / apertura di un ticket di sicurezza al servizio NOC in **massimo 1 ora**; presa in carico in **massimo 3 ore**.
- **Severity level 5** (**Critical impact**): notifica incidente al Servizio Informatica / apertura di un ticket di sicurezza al servizio NOC in **massimo 1 ora**; presa in carico in **massimo 1 ora**.

7. AVVIO ESECUZIONE DEL SERVIZIO

Entro n. 30 gg. solari decorrenti dalla sottoscrizione del contratto, l'appaltatore dovrà concordare con il Direttore dell'Esecuzione del Contratto l'avvio di tutti i servizi richiesti sul dominio di intervento specificato dandone opportuna evidenza; la verifica e formalizzazione dell'attivazione dei servizi avverrà mediante sottoscrizione di apposito verbale di **collaudo** sulla base delle seguenti evidenze:

Servizio	Evidenze	Esito
Servizi e sistemi di monitoraggio dell'infrastruttura del Sistema IT IZSVe	Disponibilità del portale web di monitoraggio e verifica degli elementi monitorati	
Servizi e sistemi di gestione delle configurazioni	Disponibilità del servizio di gestione delle configurazioni e della sua integrazione con il portale web di monitoraggio	
Servizio di raccolta e conservazione a norma dei log degli amministratori	Disponibilità servizio di consultazione dei log raccolti e sua integrazione con il portale web di monitoraggio	
Servizio di Asset Management e scadenziario	Disponibilità del servizio di Asset Management e scadenziario e della sua integrazione con il portale web di monitoraggio	
Servizi di supporto e assistenza sistemistica tramite NOC (Network Operation Center)	Disponibilità del portale web di gestione dei ticket integrato con il portale di monitoraggio, di un esclalation path e dei relativi contatti e riferimenti per l'apertura e la gestione delle richieste di supporto e assistenza	
Servizio di supporto per la sicurezza IT tramite MDRS (Managed Detection & Response System) e CSIRT (Computer Security Incident Response Team)	Disponibilità del portale web della piattaforma SOAR ed installazione del modulo di detection su almeno 5 dispositivi di test	

Dalla data del positivo collaudo decorreranno i termini contrattuali.

Il Progettista

Dott. Davide Ruzza