AFFIDAMENTO DEL SERVIZIO DI ASSISTENZA SISTEMISTICA PER LA DIREZIONE GENERALE E PER LE SEDI TERRITORIALI ARPAM

CAPITOLATO TECNICO – Allegato B

Il presente Capitolato Tecnico disciplina, in relazione agli aspetti tecnici, il servizio di assistenza sistemistica per l’Agenzia Regionale per la Protezione Ambientale Marche, di seguito “ARPAM”.

Vengono di seguito riportati i requisiti strutturali, funzionali ed operativi minimi a cui deve necessariamente rispondere il fornitore del servizio di assistenza sistemistica, di seguito “fornitore”.

Indice

[1 Descrizione dell’architettura informatica ARPAM 1](#_Toc44054123)

[2 Servizi richiesti 2](#_Toc44054124)

[2.1 Servizi di virtualizzazione …2](#_Toc44054125)

[2.2 Sistemi operativi 2](#_Toc44054126)

[2.3 Sistemi di database 3](#_Toc44054127)

[2.4 Strumenti di sicurezza informatica 3](#_Toc44054128)

[2.5 Servizi di posta elettronica (e-mail) 4](#_Toc44054129)

[2.6 Strumenti di backup 4](#_Toc44054130)

[2.7 Internetworking 4](#_Toc44054131)

[3 Modalità di intervento 5](#_Toc44054132)

[4 Attività sul territorio 5](#_Toc44054133)

[5 Service Level Agreement (SLA) 5](#_Toc44054134)

[5.1 Escalation 6](#_Toc44054135)

[6 Certificazioni di affidabilità 6](#_Toc44054136)

# Descrizione dell’architettura informatica ARPAM

L'informatica dell'ARPAM è dislocata in 7 (sette) sedi territoriali, in relazione alle quali il fornitore dovrà garantire pari condizioni di assistenza per i servizi oggetto di questo capitolato tecnico.

L’elenco delle sedi e delle infrastrutture sotto riportato ha valore indicativo; ARPAM si riserva il diritto di modificarne postazioni e sedi geografiche, anche durante la vigenza del contratto, rimanendo comunque le stesse in ambito regionale:

* **Direzione Generale (Ancona, via Ruggeri 5):**
	+ n.2 hosts fisici di virtualizzazione, circa n.10 VM VMWARE, circa n.5 server fisici, n.1 sistema di backup a nastro, n.1 firewall fortinet fortigate 50b;
* **Sede Regione Marche**:
	+ n.3 hosts fisici di virtualizzazione, circa n.20 VM PROXMOX;
	per questa sede non sono oggetto di questo capitolato l’assistenza per il software di virtualizzazione PROXMOX e l’assistenza in loco;
* **Dipartimento di Ancona (Ancona, via Colombo, 106) attuale**:
	+ n.5 server fisici, n.1 NAS QNAP, sistema di backup a nastro
	futuro: n.1 host fisico di virtualizzazione, n.2 VM HYPER-V, n.1 NAS QNAP;
* **Dipartimento di Fermo (Fermo, via Pompeiana, 158) attuale:**
	+ n.1 server fisico, sistema di backup a nastro;
	futuro: n.1 host fisico di virtualizzazione, n.2 VM HYPER-V, backup a nastro;
* **Dipartimento di Ascoli (Ascoli Piceno, via della Repubblica, 34)attuale:**
	+ n.1 host fisico di virtualizzazione, n.2 VM VMWARE, backup a nastro
	futuro: n.1 host fisico di virtualizzazione, n.2 VM HYPER-V, backup a nastro
* **Dipartimento di Pesaro (Pesaro, via Barsanti, 8)**
	+ n.1 host fisico di virtualizzazione, n.2 VM HYPER-V, sistema di backup a nastro
* **Dipartimento di Macerata (Macerata, via Federico II, 41) Attuale:**
	+ n.2 server fisici, NAS QNAP, terminal server
	futuro: n.1 host, n.2 VM HYPER-V, NAS QNAP, senza terminal server

Inoltre, per ogni sede dipartimentale è presente un server MS WS2008 in rete di connessioni interdipartimentali su server fisico IBM x3400/x3500 M3/M4. Questi server costituiscono una rete dati con database in replica.

In origine ogni dipartimento era intestatario di un dominio Microsoft separato e comunicante in trust non transitivo. ARPAM ha avviato una procedura di unificazione dei domini in corso di realizzazione. Allo stato attuale risultano ancora due domini ws2003 non ancora integrati che lavorano in trust non transitivo.

# Servizi richiesti

Il servizio di assistenza sistemistica in oggetto dovrà coprire, secondo le modalità indicate in seguito i seguenti prodotti software dislocati sul territorio come da architettura descritta. In relazione ai servizi richiesti l’affidamento comprende lo svolgimento dei compiti e delle funzioni di Amministratore di Sistema. Per il mero svolgimento di questi compiti , al fornitore sarà assegnato un account nominale con il ruolo di amministratore di sistema di cui il fornitore assume ogni responsabilità di gestione ( politica delle password, attività non attinenti, divulgazione illecita etc). Tale account sarà reso inattivo a termine contratto. L’esercizio delle funzioni di amministratore di sistema da parte del fornitore verrà consentito solo tramite tale account che ARPAM sottopone a tracciamento e verifica attività.

## Servizi di virtualizzazione

Le piattaforme di virtualizzazione oggetto di questo capitolato sono Microsoft Hyper-V, e VmWare ESXi (dalla versione 4.5) e prodotti correlati.

Il fornitore dovrà essere in grado di indicare ed attuare per i sistemi di virtualizzazione in oggetto le best practices, fornire ed attuare soluzioni ai problemi comuni dei sistemi di virtualizzazione (creazione, accensione, spegnimento, spostamento, ridimensionamento, snapshot, backup delle macchine virtuali, l'installazione dei tools nelle macchine virtuali ed ogni attività attinente alla corretta manutenzione del sistema) e trattare in maniera autonoma e/o collaborativa tutte le richieste di gestione sulle suddette piattaforme.

Il fornitore dovrà anche guidare, su richiesta, i tecnici ARPAM nella gestione in minima autonomia delle piattaforme di virtualizzazione (ad es. tool di gestione Vsphere).

ARPA Marche ha in corso il porting di molte macchine fisiche/virtuali verso server regionali virtualizzati in PROXMOX KVM; il servizio di assistenza su questa piattaforma di virtualizzazione non è oggetto del presente capitolato tecnico.

## Sistemi operativi

I sistemi operativi oggetto del presente capitolato tecnico sono:

* sistemi operativi Microsoft per piattaforme server (windows server);
* sistemi operativi Microsoft per utenze ordinarie Personal Computer.

Entrambe le piattaforme possono essere oggetto di richieste di supporto.

Per quanto attinente ai supporti sistemistici, il fornitore dovrà essere in grado di risolvere i comuni problemi dei sistemi operativi server di Microsoft Windows Server dalla versione 2003 alla versione in attuale rilascio Microsoft durante tutta la durata del contratto, in relazione alle configurazioni di dominio ADDS, applicazioni delle policy, DHCP, DNS, autenticazioni, trust di domini, AAA (computer security), PDC, FSMO, printer server, WSUS, ed ogni altro comune servizio di domino.

I servizi di supporto devono comprendere anche le procedure di installazione e configurazione completa dei sistemi operativi su server fisici o virtuali.

Il fornitore dovrà essere in grado di erogare il supporto sistemistico anche per piattaforme dismesse da Microsoft (WS2003 ad esempio) per i soli fini ordinari/manutentivi, con servizio di troubleshooting senza escalation al vendor.

Per quanto riguarda il supporto ai sistemi operativi lato client (Win10, Win8, Win7, XP), il fornitore dovrà essere in grado di intervenire su tutte le configurazioni di sistema in relazione all’ADDS aziendale e supportare i tecnici informatici ARPAM per gli upgrades, il troubleshooting e le best practices delle utenze sui PC a dominio. Anche in questo caso per le piattaforme dismesse, il fornitore dovrà comunque erogare assistenza per i soli fini ordinari/manutentivi senza richiesta di escalation al vendor.

Non viene richiesto il servizio diretto di installazione dei sistemi operativi client, ma il fornitore dovrà comunque garantire la piena assistenza tecnica in caso di problemi configurativi/gestionali incontrati dai tecnici ARPAM.

## Sistemi di database

Nei server dipartimentali sono in esercizio RDBMS Oracle tipo embedded incluso nel prodotto gestionale e istanze territoriali di MS SQL Server che i tecnici ARPAM gestiscono in autonomia. Con il passaggio alla Regione Marche le istanze MS SQL verranno unificate.

Il fornitore dovrà garantire il supporto e la risoluzione dei problemi, qualora fosse richiesto dai tecnici ARPAM, per le installazioni, l’integrazione e le configurazioni minime dei sistemi MS SQL Server nel contesto del dominio e della rete aziendale. Non vengono richieste al fornitore competenze in merito alle gestioni delle banche dati, alle interrogazioni ed al trattamento dei dati contenuti.

## Strumenti di sicurezza informatica

Gli strumenti di sicurezza informatica oggetto del presente capitolato sono i software nativi Microsoft di Windows (ad es MS Defender) ed i prodotti antivirus di Trend Micro (OfficeScan con potenziale migrazione ad APEX ONE).

ARPAM ha in adozione il servizio antivirus centralizzato OfficeScan, installato su una VM WS 2012 nella sede regionale e dai servizi di Smart Protection Server su una VM linux separata.

Il fornitore dovrà essere in grado di:

* supportare i tecnici ARPAM per le problematiche degli agent locali;
* monitorare in tempo reale gli attacchi virali;
* risolvere in totale autonomia tutte le rilevazioni e le criticità attinenti gli attacchi informatici provvedendo all’attivazione delle relative contromisure;
* controllare periodicamente la salute del sistema (server e client);
* tenere aggiornata tutta la piattaforma;
* gestire il trattamento dei nuovi pattern attuando l’escalation a Trend Micro delle rilevazioni e dei problemi in atto, con trattamento in tempistiche oggetto di SLA dei problemi di compatibilità e dei falsi positivi;
* fornire delle risposte ai tecnici ARPAM in merito ai sospetti positivi trasmessi via e-mail;
* trattare le problematiche comuni dei sistemi antivirus centralizzati.

In caso di rilevazioni di attacchi, il fornitore dovrà in primo luogo procedere alle contromisure urgenti in autonomia operativa, avvisando il personale ARPAM dell'intrusione.

Il supporto antivirus (come ad esempio verifica email sospette) deve essere attivabile anche tramite chiamate esplicite di tutto il personale ARPAM, non limitandosi ad assistere il solo staff informatico.

In caso di danneggiamenti subiti da ARPAM per intrusioni illecite, il fornitore dovrà garantire l’attuazione delle corrette procedure di ripristino in sinergia con in sistemi di backup indicati nel presente capitolato, eventualmente coordinando con i tecnici ARPAM le attività territoriali che ritenesse necessarie.

Tutte le attività di cui sopra, dovranno continuare ad essere erogate al momento di passare il servizio OfficeScan sotto il sistema APEX ONE.

Per quanto attinente ai sistemi di sicurezza del traffico dati si rimanda al punto specifico di questo capitolato tecnico.

## Servizi di posta elettronica (e-mail)

Lo strumento adottato da ARPAM per i servizi di posta elettronica è il servizio MDaemon Email Server con configurazioni accessi tramite web server e tramite comuni clienti (in special modo Outlook, liveMail), anche con strumenti portable in ActiveSync.

Il servizio principale di email di ARPAM è erogato da un server virtualizzato MDaemon on-premise.

Il fornitore dovrà essere in grado di gestire il sistema di posta MDaemon e trattarne eventuali malfunzionamenti con interventi diretti sulla piattaforma server. Dovrà inoltre essere di supporto per tutti gli aggiornamenti del prodotto e per l’applicazione delle patch che dovranno essere attuate in tempo adeguato ed in autonomia operativa.

Si richiede anche la disponibilità per trattare le problematiche della erogazione dei servizi e-mail client sia tramite la piattaforma WEB sia tramite i comuni clienti ove si verificassero malfunzionamenti non risolubili dai tecnici ARPAM.

## Strumenti di backup

Nelle sedi dipartimentali e nella sede della direzione generale, ARPAM ha attuato dei processi di backup tramite unità a cassette di tipo LTO con formati che vanno dalla versione 3 alla versione 6. Il software utilizzato per i servizi di Backup è il prodotto Backup Exec (Symantec/Veritas).

Il fornitore dovrà essere in grado di fornire il supporto tecnico necessario per la configurazione, la schedulazione, il backup ed il ripristino granulare e complessivo di files e macchine virtuali in tutte le sedi ARPAM dotate di unità a nastro LTO.

Viene inoltre richiesta la competenza operativa e gestionale per l’aggiornamento del prodotto, l’installazione delle patch, il troubleshooting e l’esercizio sui nastri LTO e sui NAS QNAP presenti in alcune sedi dipartimentali.

Con il trasferimento della sala server in Regione Marche, ARPAM intende dotarsi del sistema VEEAM per attuare le procedure di backup dipartimentali e centralizzate.

Il fornitore dovrà essere in grado di erogare anche su piattaforma VEEAM il medesimo supporto offerto per il prodotto Backup Exec, collaborando con i tecnici ARPAM per la scelta e l’implementazione delle best practices in relazione all’hardware ed alle configurazioni di rete sul territorio.

## Internetworking

Tutte le sedi ARPAM sono integrate in SPC nelle reti della Regione Marche che supervisiona le connessioni ed effettua servizio di firewalling.

Il fornitore dovrà garantire la collaborazione competente con la Regione Marche per le procedure di internetworking, come filter packet, firewalling, configurazioni di sicurezza perimetrale e controllo reti in fibra.

Per quei dispositivi ARPAM con linee autonome xDSL (in via di dismissione), il fornitore dovrà supportare la gestione delle configurazioni gateway, le procedure di sicurezza, le configurazioni di accesso esterno con gli apparati attualmente disponibili in ARPAM (comuni modem in fibra ed un firewal fortigate presente in Direzione Generale).

In caso di richiesta del personale tecnico ARPAM o della Regione, il fornitore dovrà essere in grado di garantire intervento ed assistenza per il corretto funzionamento degli switch dipartimentali e centrali ARPAM di marca HP e CISCO.

In tal caso ARPAM garantirà al fornitore la raggiungibilità in remoto degli switch tramite interfacce web/telnet/ssh.

# Modalità di intervento

ARPAM si è dotata di uno staff tecnico interno a cui il fornitore può far riferimento per risolvere le chiamate di assistenza. In genere le comunicazioni avvengono tramite questo gruppo di lavoro; ARPAM si riserva comunque il diritto di far aprire chiamate di assistenza anche tramite i referenti informatici dipartimentali o direttamente tramite altro personale interno in servizio.

I servizi di assistenza del fornitore sono erogati in remoto tramite accesso in RDP, VPN o altre soluzioni di assistenza remota concordate. Per tutte le attività risolubili a distanza, una volta stabiliti i canali operativi, il fornitore dovrà essere in grado di agire in autonomia, eventualmente coordinandosi o avvisando i tecnici ARPAM di riferimento.

In caso non fosse possibile intervenire a distanza, parte delle attività può essere concordata in collaborazione/supervisione comune in base alle decisioni dei tecnici ARPAM e con la collaborazione di personale ARPAM locale.

# Attività sul territorio

Nei casi comuni, ove si richieda attività manuale sul territorio, il personale ARPAM si rende disponibile per eseguire gli interventi con istruzioni guidate a distanza.

Per gli interventi sistemistici complessi, reinstallazione di server, reinstallazione di sistemi di virtualizzazione o altro, nella fornitura di assistenza sistemistica devono essere comunque incluse 2 (due) giornate forfettarie di attività sul territorio, eventualmente separabili in mezze giornate ove opportuno, con l’intervento di uno o più tecnici specializzati del fornitore.

È facoltà di ARPAM esercitare la richiesta di intervento sul territorio per il numero di giornate indicate, in programmazione concordata con almeno 7 giorni lavorativi di anticipo qualora non costituiscano evidente urgenza.

# Service Level Agreement (SLA)

Con il termine Service Level Agreement si intendono le metriche dei servizi di supporto che devono essere rispettate dal fornitore.

Nel seguito se ne indicano quelle minime vincolanti:

1. Durante il corso del servizio di assistenza il numero di chiamate consentite deve essere illimitato;
2. L’assistenza deve essere erogata per 5 (cinque) giorni lavorativi settimanali, 8 (otto) ore giornaliere, con eccezione dei festivi infrasettimanali. Durante il corso della mattinata devono essere garantite almeno 5 (cinque) ore di copertura del servizio;
3. Entro gli orari di assistenza, il fornitore deve rispondere ad una chiamata di assistenza tramite un tecnico qualificato entro 2 (due) ore e garantire un tempo di intervento entro 6 (sei) ore. Si considera il tempo a partire da una richiesta ARPAM tramite ogni forma di comunicazione ordinaria messa a disposizione del fornitore, quali e-mail di riferimento, centralino telefonico, contatto diretto operatore o apertura ticketing tramite servizio web.

I servizi di supporto tecnico offerti dovranno coprire i prodotti indicati per tutte le postazioni client e tutti i server in esercizio nelle sedi ARPAM. Viene riportata la dimensione stimata delle installazioni per i singoli prodotti:

* Sistemi Operativi Microsoft: tutti i server fisici e virtuali (n.30), tutte le postazioni client (n.300);
* VmWare: tutte le installazioni ESXi (n.5);
* Trend Micro: tutti gli agent Officescan installati (n.300) e le piattaforme server (n.2);
* Backup Exec: tutti i prodotti installati (n.5)
* VEEAM: da definirsi in fase di allestimento, indicativamente uno per sede;

Tutte le licenze d’uso dei prodotti di assistenza esulano dalla fornitura e si intendono a carico di ARPAM.

Il fornitore si impegna a mettere a disposizione di ARPAM un servizio di accesso web tramite accounting per la gestione dei tickets. Il servizio deve garantire il controllo di tutte le fasi della apertura chiamata, con verifica in tempo reale dello stato della chiamata (tracking), garantendo in oltre tracciature storicizzate da consultare anche in caso di controversie.

## Escalation

Nel caso si renda necessario ricorrere ai relativi vendors per processare la richiesta di supporto ARPAM, il fornitore dovrà obbligatoriamente far ricorso alle proprie partnership garantite da questo capitolato e gestire la chiamata secondo i propri migliori accordi commerciali. Il fornitore è tenuto a rendicontare ad ARPAM, su richiesta dell’Agenzia, le comunicazioni intercorse in escalation e le motivazioni di un eventuale ritardo di intervento che si protragga oltre gli SLA stipulati con ARPAM.

# Certificazioni

Al fine di garantire l’adeguatezza del servizio offerto, ARPAM richiede che il fornitore sia in possesso delle certificazioni di partnership adeguate per i prodotti in oggetto.

In particolare si richiedono i seguenti livelli minimi per specifico prodotto:

* Microsoft: level gold;
* VmWare: level advanced;
* Trend Micro: level gold, officescan XG certified professional, APEXONE certified professional;
* Veritas-Symantec: registered partner.

Il fornitore deve essere dotato di un NOC (Network Operation Center) da cui raggiungere in remoto le sedi di ARPAM e tramite il quale esercitare i servizi richiesti di diagnosi e risoluzione dei problemi.

Il fornitore si impegna ad adempiere con personale specializzato a tutti i servizi di assistenza descritti in questo capitolato, incluso il servizio NOC.