



Affidamento del servizio di manutenzione rete LAN/Wifi per il triennio 2024-2026 e sostituzione Firewall per la rete informatica dell'Istituto degli Innocenti di Firenze - CIG ZF63DC1F97

Specifiche tecniche

L'Istituto degli Innocenti di Firenze (<https://www.istitutodeglinnocenti.it>), una delle più antiche istituzioni italiane dedicate alla tutela dell'infanzia, è un Ente Pubblico (Azienda di Servizi alla Persona) ai sensi della Legge Regionale Toscana n. 43 del 3 agosto 2004 *Riordino e trasformazione delle istituzioni pubbliche di assistenza e beneficenza (IPAB) Norme sulle aziende pubbliche di servizi alla persona. Disposizioni particolari per la IPAB Istituto degli Innocenti di Firenze*, gestisce servizi di accoglienza rivolti a bambini e a famiglie in difficoltà, servizi educativi per bambini e genitori.

Collabora con vari organismi di livello locale, regionale, nazionale e internazionale per la realizzazione di attività di ricerca, formazione, documentazione e promozione sui diritti dell'infanzia e dell'adolescenza. Si occupa della valorizzazione del proprio patrimonio storico-artistico, monumentale e archivistico, della gestione e riqualificazione del suo patrimonio immobiliare. Offre servizi culturali attraverso il Museo degli Innocenti, la Biblioteca Innocenti Library e l'Archivio storico.

La peculiarità delle attività sopra descritte, nonché la sensibilità dei dati trattati nelle stesse, richiede di gestire e mantenere una complessa infrastruttura informatica distribuita in numerosi edifici.

In questo quadro di attività l'Istituto ha quindi necessità di affidare a ditta specializzata nel settore sia la manutenzione della rete LAN che del sistema wi-fi centralizzato, nonché di adeguare il livello di sicurezza con l'acquisto di un Firewall aggiornato come meglio di seguito descritto.

Oggetto del servizio

Oggetto dell'affidamento è:

1) la fornitura del servizio di manutenzione della rete LAN come di seguito descritta:

Assistenza per tutto quanto concerne gli apparati attivi all'interno dei rack dati dell'Istituto e eventuali interventi di ripristino di prese dati, fibra ottica e parti passive. Il servizio di manutenzione deve prevedere un servizio FULL SERVICE on Site comprensivo di interventi e parti di ricambio.

Il livello di servizio (SLA) richiesto è un 8x5xNBD con Presa in carico (PIC) entro 2 ore dalla segnalazione.

La copertura oraria è nei giorni feriali (escluso giorni di festività nazionale) dalle ore 9 alle ore 18.

L'Ente nominerà due referenti che potranno attivare le procedure di intervento; tali nominativi dovranno comprendere nome cognome numero di telefono per reperibilità e indirizzo mail.

Per l'attivazione della procedura di guasto si procederà come segue:

- Il referente invierà segnalazione di guasto alla mail fornita dall'affidatario; oppure per via telefonica oppure tramite sezione nel sito Internet (se prevista);
- entro due ore lavorative la segnalazione dovrà essere presa in carico da un tecnico che invierà l'avvenuta presa in carico;
- seguirà un primo intervento da remoto per verifica e diagnostica degli apparati con tentativo di ripristino;
- se necessario sarà eseguito intervento on-site entro il giorno lavorativo successivo alla lavorazione o in altro giorno concordato con il referente;
- a fine intervento sarà redatto un buono di lavoro con collaudo di ripristino da ritornare firmato per accettazione;

2) Aggiornamento tecnologico firewall

sostituzione dell'attuale Firewall WatchGuard M370 con un NGF di nuova generazione Fortinet Fortigate 60F con licenza UTP per 3 anni.

I Next-Generation Firewall (NGFW) per filtrare il traffico di rete e per proteggere l'Ente dalle minacce interne ed esterne; in questo modo si consente di identificare attacchi, malware e altre minacce e si permette al NGFW di bloccare tali minacce. I NGFW forniscono ispezione SSL, Application Control, Intrusion Prevention e visibilità avanzata su tutta la superficie di attacco.

I NGFW non solo bloccano il malware, ma includono anche percorsi per gli aggiornamenti futuri, garantendo la flessibilità necessaria per evolvere con il panorama delle minacce e mantenere la rete sicura in caso di nuove minacce. I Next-Generation Firewall sono una componente vitale per l'implementazione della sicurezza di rete.

3) Servizi licenza UTP

Application Control

Per migliorare la sicurezza e soddisfare i requisiti di conformità grazie alla facile applicazione delle policy di uso accettabili tramite visibilità senza pari e in tempo reale nelle applicazioni eseguite dagli utenti.

Web Filtering

Per proteggere l'Ente bloccando l'accesso a siti Web dannosi, inappropriati oppure oggetto di attacchi da parte degli hacker.

Antivirus

FortiGuard AntiVirus per proteggere da virus, spyware e altre minacce a livello di contenuti recenti, non a livello di Endpoint, ma a livello di rete. Sfrutta avanzati motori di rilevamento per impedire che minacce nuove e in evoluzione penetrino nella rete e accedano ai suoi preziosi contenuti.

Intrusion Prevention

FortiGuard IPS per proteggere dalle ultime intrusioni di rete rilevando e bloccando le minacce prima che raggiungano i dispositivi di rete.

Servizio di protezione contro gli attacchi di virus

Il servizio FortiGuard di protezione contro gli attacchi di virus (Virus Outbreak Protection Service, VOS) copre gli intervalli tra gli aggiornamenti antivirus con l'analisi sandbox di FortiCloud per rilevare e bloccare le minacce malware individuate tra gli aggiornamenti delle signature prima che possano diffondersi in tutta l'azienda. OS avvia una ricerca in tempo reale nel nostro database di Threat Intelligence globale.

Content Disarm & Reconstruction

Content Disarm & Reconstruction (CDR) rimuove tutti i contenuti attivi dai file in tempo reale, creando un file flat ripulito. Tutti i contenuti attivi vengono trattati come sospetti e rimossi. Eelabora tutti i file in arrivo, li analizza a fondo e rimuove tutti gli elementi che non corrispondono alle policy del firewall.

Sicurezza IP Reputation & Anti-botnet

Il servizio IP Reputation di FortiGuard aggrega dati IP di fonti dannose provenienti dalla rete distribuita Fortinet di sensori di minaccia, CERT, MITRE, concorrenti cooperativi e altre fonti globali che collaborano per fornire threat intelligence aggiornata per fonti ostili. L'intelligence in tempo quasi reale proveniente da gateway di rete distribuiti abbinata alle ricerche di prim'ordine di FortiGuard Labs aiuta a migliorare la sicurezza delle organizzazioni e bloccare gli attacchi in modo proattivo

Dal prezzo dell'affidamento sono escluse la riparazione e sostituzione di terminali telefonici (analogici, digitali, Dect, IP), UPS, Raddrizzatori, Server/PC, parti di consumo in genere (batterie, ecc) e tutto quanto non espressamente citato.

Con la presentazione dell'offerta il fornitore dichiara di avere piena conoscenza della rete e dell'attuale sistema Firewall SPP e dei vari collegamenti operativi nell'Ente è - tuttavia - concessa la possibilità di effettuare un sopralluogo in caso di richiesta;

L'operatore economico si impegna altresì - alla scadenza dell'affidamento e in caso di nuova gara - a garantire continuità del servizio mettendo a disposizione del nuovo eventuale fornitore tutto ciò che è necessario per il proseguo dell'attività senza costi aggiuntivi a carico dell'Ente. (a titolo esemplificativo e non esaustivo, al termine del contratto il contraente si impegna a trasmettere tutta la documentazione tecnica illustrativa, le modifiche effettuate alla rete stessa, i dati di accesso agli apparati fisici e le credenziali di accesso ai pannelli di gestione software..)

Il servizio ha la durata **di 3 anni, ovvero dal 1 Gennaio 2024 al 31 Dicembre 2026**

E' possibile la proroga della scadenza al solo fine di completare l'assistenza necessaria e gli eventuali aggiornamenti previsti dal contratto, senza ulteriori aggravii in termini economici a carico dell'Ente.

Per lo svolgimento del servizio, l'operatore economico può avvalersi delle attrezzature presenti presso la sede dell'Istituto degli Innocenti, Piazza SS. Annunziata 12, 50122 Firenze, dal lunedì al venerdì, dalle ore 9.30 alle ore 18.30.

Gli interventi sono svolti in raccordo con i referenti del servizio competente, appositamente individuati.

Importo presunto e pagamenti

L'importo dell'affidamento è pari ad **€ 18.727,00 IVA inclusa**

La partecipazione è sottoposta alle seguenti condizioni:

Il presente documento "Specifiche tecniche" deve essere firmato digitalmente e ricaricato a sistema da parte dell'operatore economico per accettazione;



L'importo dell'affidamento dovrà essere comprensivo di tutti i servizi indicati;

Si ricorda che ai sensi dell'art. 120, comma 9, del D. Lgs. N. 36/2023, le variazioni entro 1/5 devono essere accettate dal fornitore alle stesse condizioni tecniche ed economiche dell'offerta.

L'Istituto degli Innocenti, per cause di forza maggiore si riserva la possibilità di risolvere il contratto che sarà stipulato con l'aggiudicatario, ai sensi dell'art. 1456 del codice civile.

Note di fatturazione:

E' prevista la fatturazione trimestrale previa verifica dei volumi e della qualità delle attività svolte a cura del Responsabile del servizio competente, con il supporto del personale informatico dell'Ente.

Split payment:

Ai sensi dell'art.1 comma 629 a partire dal 1/1/2015 il fornitore emette regolare fattura con addebito IVA indicando che tale imposta deve essere versata dall'acquirente o committente ai sensi dell'art.17-ter del D.P.R. n. 633/1972; l'Ente Pubblico provvederà a pagare al fornitore quanto indicato in fattura solo nella voce IMPONIBILE, versando direttamente all'Erario la relativa IVA.

Fatturazione elettronica:

A decorrere dal 31 marzo 2015, le fatture sono trasmesse in formato elettronico secondo i requisiti tecnici previsti dal Decreto del Ministero dell'Economia e delle Finanze n.55/2013.

Il codice univoco ufficio da utilizzare per l'invio delle fatture intestate all'istituto degli Innocenti è: **GY7RWO**. Inoltre ai fini di una corretta procedura di liquidazione fatture stesse è necessario indicare correttamente i dati relativi a CIG e numero d'ordine così come forniti dall'Ente.

Il Responsabile del
Procedimento/Responsabile P.O. Servizio
Segreteria generale, sistemi IT e Museo degli
Innocenti
Dott.ssa Antonella Schena