INDAGINE DI MERCATO ESPLORATIVA CON RICHIESTA DI PREVENTIVI PER L'AFFIDAMENTO DELLA FORNITURA DI BENI E SERVIZI RELATIVI AL MONITORAGGIO DELLA SICUREZZA INFORMATICA DI RETE DI FINAOSTA S.P.A.

Ente committente

Finanziaria Regionale Valle d'Aosta - Società per Azioni siglabile FINAOSTA S.p.A., con sede in Aosta Via Festaz n. 22, tel. +390165269267, email acquisti@finaosta.com, pec gare.finaosta@legalmail.it

Premesse

Il sistema informatico di FINAOSTA S.p.A. (d'ora in poi FINAOSTA) opera all'interno di un ambiente di calcolatori interconnessi mediante una rete di trasmissione dati. Questo ambiente, denominato "rete locale", non è isolato rispetto all'esterno, ma è predisposto per poter comunicare, per mezzo della rete internet, con soggetti terzi, allo scopo di scambiare informazioni.

Il passaggio delle informazioni da e verso l'esterno è regolato da un dispositivo di sicurezza, denominato "firewall", il cui scopo è di impedire tutti i flussi non autorizzati in base alle regole predisposte e garantire la riservatezza delle connessioni attivate dall'esterno verso l'interno da parte degli utenti autorizzati.

Oggetto

Oggetto della presente indagine esplorativa di mercato è l'acquisizione di preventivi per la fornitura di beni e servizi per la gestione, internamente al perimetro di rete protetto dal firewall sopra citato, di un sistema di monitoraggio della sicurezza informatica di rete (network intrusion detection (di seguito anche NIDS), vulnerability assessment (di seguito anche VA) e correlazione) di Finaosta S.p.A., attraverso le prestazioni descritte nelle specifiche tecniche allegate alla presente (allegato "A").

L'Affidatario dovrà accettare di essere nominato **Responsabile esterno del trattamento dei relativi dati** ai sensi della vigente normativa di protezione della privacy.

Non è consentito il subappalto.

Durata della prestazione

Le prestazioni richieste dovranno essere attivate entro il termine di 30 giorni dalla data della lettera di affidamento della fornitura inviata da FINAOSTA, fatte salve indicazioni diverse di quest'ultima, e proseguite per i successivi 36 mesi. L'attivazione delle prestazioni si desumerà da un apposito

documento di collaudo sottoscritto dai referenti di Finaosta S.p.A. e dell'operatore economico affidatario.

Corrispettivo

Il valore presunto del contratto ammonta a € 38.000,00 (euro trentottomila/00), omnicomprensivi di tutti gli oneri e le spese che si renderanno necessarie per il trasporto e l'installazione del materiale ed al netto dell'imposta sul valore aggiunto.

Sopralluogo

Al fine di garantire il recepimento di tutte le informazioni necessarie, nei giorni lavorativi compresi tra la data di pubblicazione del presente avviso e il giorno precedente quella di termine per la presentazione del preventivo, Finaosta S.p.A. renderà possibile un sopralluogo nella propria sede, alla presenza e sotto la guida di proprio personale, dalle 8:30 alle ore 12 e dalle ore 14:30 alle 16:30, previo appuntamento telefonico ai numeri 0165-269231 o 0165-269220. Il sopralluogo di cui sopra è facoltativo.

Competenza professionale richiesta e soggetti ammissibili

Possono presentare il preventivo i soggetti indicati all'art. 45 del D.lgs. 50/2016 e successive modificazioni, i quali al momento della presentazione dell'istanza:

a) non si trovino nelle condizioni di esclusione dalla partecipazione previsti dall'art. 80 del D.lgs. 50/2016;
b) non si trovino in situazioni di incompatibilità o conflitto di interessi con FINAOSTA;
c) non si trovino in situazioni, cause di esclusione, che comportino il divieto di contrarre con la pubblica amministrazione;
d) a comprova del livello specialistico richiesto, abbiano svolto per conto di terzi negli anni 2016 – 2017 – 2018 uno o più incarichi aventi ad oggetto attività di:
    - *vulnerability assessment*

      oppure
    - gestione di sistemi informatici di rilevamento delle intrusioni

   per un importo complessivo minimo pari € 38.000,00.

Criterio di selezione

L'affidamento del servizio avverrà mediante affidamento diretto ai sensi dell'art. 36 comma 2, lett. a) del D. Lgs. n. 50/2016.

FINAOSTA S.p.A. affiderà l'incarico mediante il criterio del **prezzo più basso.**

Responsabile Unico del Procedimento

Il Responsabile Unico del Procedimento è Fabio Broccolato.

Contenuti della documentazione richiesta

Il preventivo dovrà indicare il corrispettivo per le attività indicate nell'oggetto comprensivo di tutti gli eventuali rimborsi o spese e non deve essere indicata l'imposta sul valore aggiunto.

FINAOSTA si riserva la facoltà di chiedere ulteriori chiarimenti sulla documentazione presentata.

Modalità di presentazione della domanda e del preventivo

La documentazione dovrà pervenire, via PEC, al seguente indirizzo: **gare.finaosta@legalmail.it** entro le **ore 16.00** del **23 settembre 2019**; l'oggetto dovrà recare la seguente dicitura "MONITORAGGIO SICUREZZA INFORMATICA DI RETE DI FINAOSTA - INDAGINE CON RICHIESTA DI PREVENTIVI"

Occorrerà inserire in allegato la seguente documentazione:

- una dichiarazione, redatta su carta semplice secondo lo schema allegato, corredata di documento di identità in corso di validità del dichiarante;
- un preventivo indicante il compenso omnicomprensivo di eventuali rimborsi, spese e oneri esclusa l'imposta sul valore aggiunto.

Informazioni ulteriori

FINAOSTA ha proceduto a pubblicare, in pari data, un avviso per "L'AFFIDAMENTO DELLA FORNITURA DI BENI E SERVIZI RELATIVI ALLA GESTIONE DEGLI APPARATI DI PRESIDIO DELLA SICUREZZA INFORMATICA PERIMETRALE DI FINAOSTA S.p.A".

Gli operatori economici, in possesso dei requisiti previsti, possono presentare un preventivo per entrambi gli avvisi; tuttavia si informa che la fornitura di cui al presente bando **NON potrà essere affidata all'operatore economico che si trovi in una delle situazioni di cui all'art. 2359 c.c. o in altra situazione di connessione giuridica, desumibile dalla visura camerale, con l'operatore economico affidatario del servizio di gestione sopracitato.**

Trattamento dei dati personali

FINAOSTA S.p.A. garantisce il rispetto delle norme di legge applicabili al trattamento dei dati personali contenute nel Regolamento UE n. 679 del 2016 in materia di protezione dei dati personali.

****

Eventuali chiarimenti sul contenuto del presente avviso possono essere richiesti ai seguenti indirizzi: acquisti@finaosta.com

La presentazione dell'istanza non equivale ad una proposta *ex* art. 1326 del codice civile né comporta l'applicazione degli artt. 1337 e 1338 del codice civile. L'istanza rappresenta per FINAOSTA S.p.A. un'indicazione di mercato, senza effetti o vincoli giuridici.

FINAOSTA S.p.A. si riserva di non affidare l'incarico o di affidare l'incarico, nel rispetto della normativa vigente, attraverso procedure alternative alla presente.

Aosta, 9 settembre 2019

FINAOSTA S.p.A.

Allegati
Allegato A: Specifiche tecniche
Allegato B: Dichiarazione

Allegato A – Specifiche tecniche

INDAGINE DI MERCATO ESPLORATIVA CON RICHIESTA DI PREVENTIVI PER L'AFFIDAMENTO DELLA FORNITURA DI BENI E SERVIZI RELATIVI AL MONITORAGGIO DELLA SICUREZZA INFORMATICA DI RETE DI FINAOSTA S.p.A.

Sommario

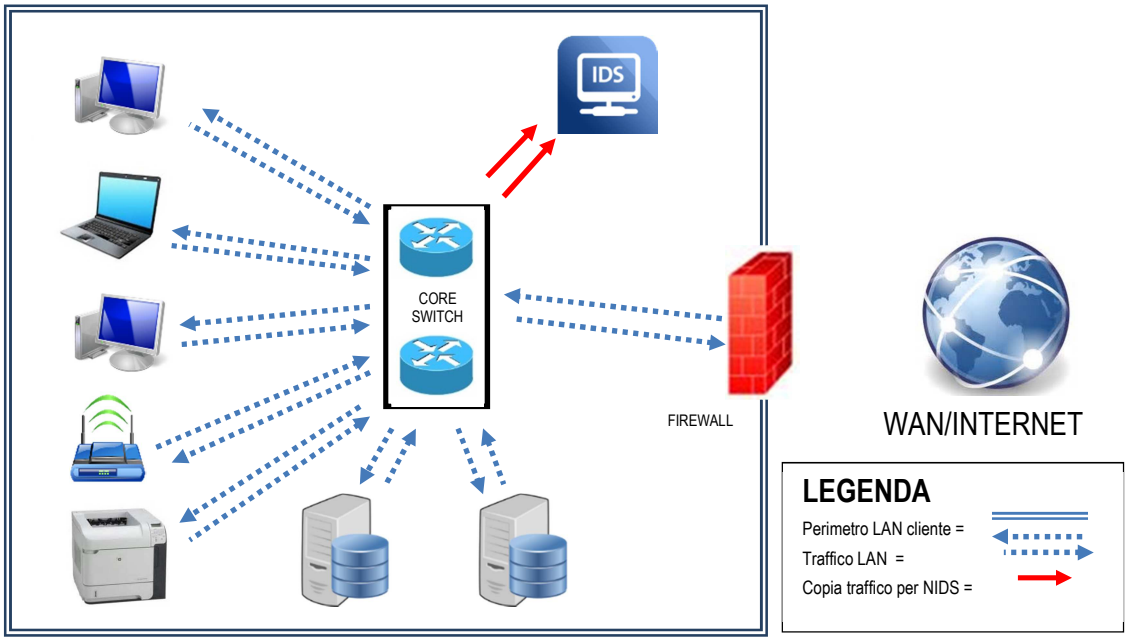
1 Oggetto della fornitura

La piattaforma di cui è richiesta la quotazione per la fornitura è costituita da un insieme di apparati hardware e software più relativi servizi di gestione, necessari per realizzare quanto di seguito specificato.

1.1 Servizio di network intrusion detection

Il servizio di network intrusion detection (d'ora in avanti anche NIDS) deve essere atto a:

a) rilevare ed analizzare il traffico dati in transito per i due core switch della rete locale del cliente (configurati con protocollo Spanning Tree ed una mirroring port ciascuno, velocità 1 Gbit/secondo);



b) segnalare via email o telefono episodi di traffico rilevato di cui al punto che precede, nei casi di maggiore rilevanza quantitativa o qualitativa, qualora possa essere riferito, avuto riguardo ai migliori standard di sicurezza tempo per tempo applicabili:
   - ad attività ostili rivolte contro le risorse informatiche interne alla rete del cliente;
   - ad attività ostili aventi origine da risorse informatiche interne alle rete del cliente.

   Le segnalazioni dovranno avvenire secondo i seguenti livelli di servizio:
   b1) segnalazione automatica entro 15 minuti dalla rilevazione dell'evento critico;
   b2) 1 segnalazione giornaliera anche in caso di assenza di eventi critici rilevati;
   b3) copertura del servizio h24.

c) generare di una reportistica mensile, comprendente suggerimenti su attività possibili per la riduzione del rischio, che includa il numero di attività malevole rilevate nel mese precedente, classificate per:
   c1) punto di origine (interno o esterno al perimetro aziendale);
   c2) giudizio di gravità (in base tipo o estensione dell'danno atteso sui sistemi impattati).

Tutta la reportistica prodotta deve essere depurata dalle segnalazioni che costituiscono notifica di eventi non correlabili con vulnerabilità presenti nella realtà della stazione appaltante.

La trasmissione dei report avverrà utilizzando il formato elettronico pdf con testo ricercabile, inviato previa cifratura protetta da password di almeno 10 caratteri, comunicata mediante un canale concordato diverso da quello utilizzato per l'invio dei documenti. Adeguati ulteriori criteri di protezione delle informazioni sensibili o degli eventuali dati personali potranno essere posti in essere con modalità concordate tra le parti.

Il sistema dovrà essere in grado di operare sul traffico almeno (ma non limitato) dei seguenti segmenti di rete:

- DMZ (ove esistente);
- Segmento di rete che interconnette gli switch di core con i nodi firewall;
- Tutte le VLAN in cui la rete locale è suddivisa (riferimento schema 1 in calce a questo documento), laddove il traffico transiti da uno qualunque degli switch di core.

Sarà cura della stazione appaltante informare preventivamente l'impresa aggiudicataria sull'eventuale attivazione di nuovi piani di indirizzamento o di nuove VLAN.

Il sistema NIDS dovrà avere le seguenti caratteristiche:

- essere dotato di interfacce di rete 10/100/1000 Mbit/s Ethernet rame;
- permettere di registrare ed effettuare una prima analisi in real-time di tutto il traffico dei segmenti indicati;
- disporre di una quantità di memoria sufficiente a conservare per analisi successive una quantità di dati adeguata ad identificare e caratterizzare eventuali anomalie;
- attivare più di un metodo di analisi sul traffico;
- essere in grado di rilevare attacchi di tipo Denial-of-Service (DoS);
- essere in grado di rilevare comportamenti anomali provocati da worm o virus informatici;
- disporre di meccanismi di auto-aggiornamento delle signatures;
- essere in grado di operare in modo non rilevabile dall'esterno (transparent mode);
- permettere di configurare allarmi con notifiche sia all'impresa aggiudicataria gestore del sistema sia alla stazione appaltante per un'immediata analisi dell'evento.

Il produttore del sistema dovrà disporre di una struttura in grado di rilasciare aggiornamenti regolari delle signature.

Il sistema dovrà supportare l'aggiornamento delle signature, ovvero l'introduzione della decodifica di nuovi protocolli e nuove compound signatures, senza la necessità di riavviare il sensore stesso, e senza caduta delle sessioni attive, durante l'aggiornamento.

Il sistema dovrà essere in grado di aggiornare le signature automaticamente, senza l'intervento manuale dell'operatore, in base a programmazione effettuata in precedenza, con frequenza almeno giornaliera.

1.2 Servizio di vulnerability assessment

Il servizio di vulnerability assessment (d'ora in avanti anche VA) consiste nell'analisi non invasiva dell'esposizione al rischio di attacchi delle risorse del sistema informativo del cliente, ove dotate di interfaccia di collegamento cablata (fisica o virtuale) alla rete locale.

Il servizio dovrà essere erogato mediante test a cadenza mensile e con le seguenti finalità:

- identificare gli obiettivi di potenziali attacchi;
- rilevare le installazioni non correttamente protette, e quindi vulnerabili ad eventuali attacchi;
- verificare l'applicazione di tutte le patch rilasciate;

Salvo diverse intese tra i referenti del contratto, l'attività di VA dovrà essere effettuata sui seguenti segmenti di rete (riferimento schema 1 alla fine di questo documento):

- DMZ (ove esistente);
- segmento di rete che interconnette gli switch di core con i nodi firewall;
- tutte le VLAN in cui la rete locale è suddivisa (riferimento schema 1), laddove il traffico transiti da uno qualunque degli switch di core.

Sarà cura della stazione appaltante informare preventivamente l'impresa aggiudicataria sull'eventuale attivazione di nuovi piani di indirizzamento o di nuove VLAN.

Le attività svolte dovranno impattare il meno possibile sulle funzionalità del sistema informatico sottoposto a VA.

I risultati dei test dovranno essere presentati mensilmente in un report che conterrà almeno le seguenti sezioni:

1. analisi globale della sicurezza della rete riguardante topologia della rete ed i flussi informativi ad essa correlati, l'hardware ed i sistemi operativi installati;
2. le vulnerabilità riscontrate, classificate per livello di rischio;
3. per ciascuna vulnerabilità, la soluzione, se esistente, in grado di risolvere il problema.

I report così prodotti devono poter consentire alla stazione appaltante di verificare l'adeguatezza della politica di sicurezza implementata all'interno del proprio dominio di responsabilità e di adottare eventuali adeguamenti.

Tutte le vulnerabilità dovranno essere catalogate secondo un metodo di valutazione quantitativo e qualitativo che permetta una precisa categorizzazione dei risultati e delle contromisure suggerite.

I report saranno trasmessi entro la prima settimana del mese successivo a quello a cui il report si riferisce.

La trasmissione dei report avverrà utilizzando il formato elettronico pdf con testo ricercabile, inviato previa cifratura protetta da password di almeno 10 caratteri, comunicata mediante un canale concordato diverso da quello utilizzato per l'invio dei documenti. Adeguati ulteriori criteri di protezione delle informazioni sensibili o degli eventuali dati personali potranno essere posti in essere con modalità concordate tra le parti.

1.3 Servizio di correlazione

Detto servizio dovrà essere svolto tra le risultanze delle attività di NIDS e di VA, allo scopo di escludere dalle segnalazioni di cui al punto b) del servizio NIDS le attività rivolte a sfruttare vulnerabilità non rilevate nei sistemi interni.

1.4 Servizio di supporto

Il supporto sui sistemi gestiti sarà fornito a cura e spese dell'impresa aggiudicataria, con interventi remoti e/o on-site, in caso di necessità.

Tale servizio dovrà prevedere, per un periodo di 36 mesi effettivi dalla data di sottoscrizione del documento di collaudo e con la formula "8x5" (5 giorni su 7, 8 ore al giorno), anche la sostituzione dei componenti, al massimo entro quattro giorni lavorativi successivi alla comunicazione dell'avaria da parte della stazione appaltante.

La manodopera e le parti di ricambio verranno messe a disposizione dall'impresa aggiudicataria, che si farà carico delle spese accessorie relative agli eventuali interventi, anche presso la sede del cliente senza alcun onere aggiuntivo per quest'ultimo; le parti sostituite verranno ritirate dall'impresa aggiudicataria stessa, previa verifica della garanzia della riservatezza di eventuali dati in esse contenute (esempio: formattazione a basso livello prima del ritiro o rinuncia al ritiro di memorie contenenti dati).

Il servizio di supporto includerà sia la manutenzione preventiva sia quella correttiva, sia quella evolutiva del sistema, così definite:

- Manutenzione preventiva
  L'impresa aggiudicataria si impegna tempo per tempo a proporre e, previo accordo con la stazione appaltante, effettuare regolazioni, controlli, sostituzioni, ecc. finalizzati al mantenimento dell'efficienza e dell'efficacia del sistema.

- Manutenzione correttiva
  La manutenzione correttiva consiste in interventi di analisi e risoluzione di guasti, blocchi o altri inconvenienti che dovessero verificarsi all'infrastruttura gestita sotto il profilo hardware e software; include l'esecuzione delle prove e dei controlli necessari a garantire il ripristino del pieno funzionamento dei sistemi, nonché nella fornitura ed installazione di correttivi di tipo hardware e software. Sono incluse le attività di eventuale roll-back. Il servizio può essere attivato sia su richiesta della stazione appaltante, sia su indicazioni di uno dei costruttori della piattaforma, sia su iniziativa del gestore.

- Manutenzione evolutiva
  Consiste nel periodico e tempestivo aggiornamento della piattaforma a nuove versioni dei software ivi installati, quando rilasciate dal produttore durante il periodo di validità del contratto e per le quantità di licenze che via via si renderanno necessarie, limitatamente alle utenze presenti all'interno della sede di Via Festaz 22. Sono inclusi i test di buon funzionamento della piattaforma e le attività di eventuale roll-back. In tali occasioni non saranno addebitate ulteriori somme, in quanto assorbite dal canone previsto per il servizio di supporto.

La copertura del servizio sarà di tipo "8x5" (5 giorni su 7, 8 ore al giorno).

Le comunicazioni avverranno, a scelta delle parti, a mezzo piattaforma CRM, email, telefono.

I livelli di servizio richiesti per il supporto sono:

- 4 ore lavorative dalla chiamata per la presa in carico e la prima analisi del problema;
- 1 giorno lavorativo dalla chiamata per l'inizio dell'intervento ed una stima dei tempi di risoluzione in caso di guasto bloccante;
- 3 giorni lavorativi dalla chiamata per l'inizio dell'intervento ed una stima dei tempi di risoluzione in caso di guasto non bloccante.

La stazione appaltante rende disponibile nel proprio datacenter, ove di interesse per ospitare la soluzione oggetto del presente capitolato, il seguente sistema hardware:

- HP ProLiant DL 385 G7, 2 CPU AMD Opteron 6180SE 12 core 2,5GHz, RAM 64Gbyte, HD 2TB circa, 6 interfacce Gigabit Ethernet, senza sistema operativo.

Detto sistema hardware, ove utilizzato per espletare i servizi richiesti, dovrà essere coperto, con oneri a carico dell'impresa aggiudicataria, dalla fornitura delle licenze d'uso dei software necessari e dai servizi di supporto più sopra illustrati.

A corredo della fornitura di quanto precedentemente descritto, sono richiesti, ove necessari, i lavori di installazione, configurazione personalizzata, attivazione operativa delle soluzioni e dei servizi forniti.

L'impresa aggiudicataria è tenuta a fornire ed installare materiali vari e ad eseguire i lavori eventualmente necessari e complementari in aderenza alle finalità previste dalla presente commessa. Dovrà essere, quindi, fornito ed installato tutto quel materiale di minuteria non espressamente indicato nella presente specifica tecnica, necessario al completamento dell'installazione, che dovrà essere effettuata secondo le migliori tecniche ed a regole d'arte.

La stazione appaltante consentirà al personale incaricato dall'aggiudicatario, sotto la direzione e piena responsabilità di quest'ultimo, l'accesso ai locali ed alle apparecchiature necessarie per effettuare le attività previste, e fornirà tutte le informazioni di sua conoscenza che dovessero risultare utili per raggiungere le finalità di progetto.

Fatto salvo il caso di guasti bloccanti, l'accesso da remoto ai sistemi gestiti dovrà avvenire da una delle loro interfacce interne al perimetro della LAN del cliente, dopo instaurazione di una sessione VPN con uso del software client Cisco® AnyConnect.

Nel caso di interventi particolarmente critici (ad esempio: firmware update, sostituzione hardware) sarà cura del gestore dell'infrastruttura concordare preventivamente ogni attività con il personale della stazione appaltante.

2 Trattamento dei dati

Tenuto conto della natura del servizio, che può comportare il trattamento di dati personali, la sua esecuzione comporta l'obbligo, per l'aggiudicatario, di accettare la nomina a responsabile esterno del trattamento di dati di cui Finaosta è titolare ai sensi della vigente normativa di protezione della privacy.

3 Incontri periodici tra i referenti

Durante tutta la durata del contratto, l'impresa aggiudicataria dovrà prendere parte, su sollecitazione della stazione appaltante, ad un massimo di 6 incontri di verifica e controllo dell'andamento del servizio gestito. Tali incontri potranno avvenire anche mediante l'uso di tecnologie di audio o video conferenza, e vi prenderanno parte i referenti della stazione appaltante e del fornitore, competenti nella gestione del servizio oggetto dell'appalto.

4 Comunicazioni del fornitore alla stazione appaltante

Il fornitore dei servizi informerà per iscritto la stazione appaltante di qualsiasi evento che dovesse incidere sulla sua capacità di svolgere il servizio affidato in maniera efficace e in conformità con la normativa tempo per tempo vigente; inoltre, comunicherà tempestivamente il verificarsi di incidenti di sicurezza nell'ambito del perimetro dei processi gestiti per conto della stazione appaltante, anche al fine di consentire la pronta attivazione delle relative procedure di gestione o di emergenza.

Schema 1

Di seguito è riportato lo schema delle VLAN attualmente presenti sugli switch di core HP 5406-zl.

VLAN ID	Name	Status	Voice	Jumbo
1	Old_Vlan	Port-based	No	No
5	VL_Guest	Port-based	No	No
8	VL_Logon	Port-based	No	No
9	VL_Server	Port-based	No	No
10	VL_Internet	Port-based	No	No
11	VL_MGMT	Port-based	No	No
20	VL_AUTH	Port-based	No	No
30	VL_SysAdmin	Port-based	No	No
40	VL_Printer	Port-based	No	No
80	VL_Domotica	Port-based	No	No
105	VL_IntGuest	Port-based	No	No
150	VL_Telefonia	Port-based	No	No

Allegato B - Dichiarazione

Oggetto: INDAGINE DI MERCATO ESPLORATIVA CON RICHIESTA DI PREVENTIVI PER L'AFFIDAMENTO DELLA FORNITURA DI BENI E SERVIZI RELATIVI AL MONITORAGGIO DELLA SICUREZZA INFORMATICA DI RETE DI FINAOSTA S.p.A.

Il sottoscritto _____ nato il _____
a _____ (_____) codice fiscale _____
in qualità di _____
dell'operatore economico _____
con sede legale in _____ (_____) Via _____
Codice fiscale _____ Partita IVA _____
Telefono _____ Telefax _____
e-mail _____ PEC _____

dichiara

ai sensi degli artt. 47 e 77-bis del Decreto del Presidente della Repubblica (D.P.R.) 28 dicembre 2000, n. 445, consapevole delle sanzioni penali previste dall'art. 76 del detto D.P.R. per le ipotesi di falsità in atti e dichiarazioni mendaci:

A) di non trovarsi nelle condizioni di esclusione dalla partecipazione indicate nell'avviso;

B) di essere in possesso dei requisiti di carattere professionale richiesti;

C) di acconsentire al trattamento dei dati personali ai sensi della vigente normativa;

D) di acconsentire preventivamente all'esecuzione, da parte di FINAOSTA S.p.A., ad ogni idoneo controllo per accertare la veridicità delle dichiarazioni sostitutive fornite.

Data _____ Firma del Legale Rappresentante _____

Allegati: n. 1 copia fotostatica del documento di identità in corso di validità del dichiarante