**CSI PIEMONTE**

**Piattaforma di Network Security Policy Management - NSPM**

**REQUISITI TECNICO - FUNZIONALI**

**E MODALITÀ DI FORNITURA**

**[***Indicare qui il nome dell’operatore economico partecipante***]**

# INTRODUZIONE

Il CSI Piemonte intende dotarsi di una soluzione per la gestione integrata e centralizzata di *Network Security Policy Management* (di seguito NSPM)

Attualmente il CSI dispone di una soluzione (sviluppata in casa su piattaforma Remedy) che implementa esclusivamente il flusso di “change” di una policy di sicurezza.

Obiettivi principali cui la nuova soluzione è funzionale sono:

* evolvere verso una moderna soluzione di NSPM
* semplificare le modalità di richiesta e gestione Policy (anche su base utente e/o applicazione)
* supportare le attività di *governance* e di controllo della sicurezza.

Si evidenziano di seguito alcune caratteristiche importanti della soluzione desiderata:

* **Firewall rules management:** la soluzione deve consentire la gestione centralizzata delle policy di sicurezza in un ambiente “multivendor” (sia per la parte firewall che di dispositivi di rete/bilanciatori) evidenziando situazioni di overlapping, shadowing e di conflitto policy.
* **Centralized policy management and visibility**: la soluzione deve permettere di avere una visione ed un controllo centralizzato della sicurezza della rete compreso anche *private cloud* e *public cloud*.
* **Automated change management**: la soluzione deve garantire la gestione automatica di tutto il flusso autorizzativo di richiesta di creazione/modifica/dismissione di una policy
* **Topology mapping and path analysis:** la soluzione deve fornire una mappa “virtuale” della rete dando visibilità delle connessioni
* **Audit and compliance management/reporting of security policies:** la soluzione deve poter gestire diversi profili di “compliance” a linee guida di sicurezza
* **Vulnerability and risk assessment:** la soluzione deve poter effettuare un risk assessment della rete e sistemi identificando le diverse vulnerabilità riscontrate e suggerendo le azioni da intraprendere al fine di eliminare/ridurre il rischio.

Il presente documento - che costituisce l'allegato all’*Avviso di indagine di mercato nell’ambito dell’analisi comparativa finalizzata all’individuazione di una soluzione software Network Security Policy Management ai sensi dell’art. 68 del D. Lgs. 82/2005 e s.m.i. - Codice dell’Amministrazione Digitale (CAD)”* - ha l'obiettivo di verificare la presenza sul mercato di soluzioni dotate – in tutto o in parte - di caratteristiche funzionali e tecniche, funzionali a soddisfare le esigenze del CSI-Piemonte, conoscendone anche le relative modalità di fornitura/distribuzione oltre che le stime di massima su costi e tempi di messa a disposizione.

# Nota bene: In considerazione della natura dell’Indagine in corso e dei relativi fini di analisi comparativa ai sensi dell’art. 68 CAD – è richiesto di omettere ovvero di non inserire tra le informazioni, elementi protetti da segreto industriale, know-how, proprietà intellettuale e/o industriale o analoga normativa (si veda anche quanto al riguardo precisato nell’avviso cui il presente documento costituisce allegato).

# RIFERIMENTI

Art. 68 CAD - Circolare 6 dicembre 2013 n. 63 – Linee guida per la valutazione comparativa prevista dall’art. 68 del D. Lgs. 7 marzo 2005, n. 82 “Codice dell’Amministrazione digitale”.

#

# DESCRIZIONE IN SINTESI DELLA SOLUZIONE PROPOSTA

*Inserire qui una breve descrizione (max 1 pagina) della soluzione proposta e delle tecnologie di riferimento adottate dalla soluzione (system software, linguaggi di sviluppo e middleware).*

# SODDISFACIMENTO DEI REQUISITI

Nel seguito sono elencati i requisiti individuati per la soluzione sulla base delle esigenze espresse da Città di Torino e dagli altri attori interessati.

Si distinguono in tabelle separate:

* i requisiti funzionali (RF),
* i requisiti non funzionali (RNF),
* la modalità di fornitura del software (MF)

Nel seguito si descrive il significato delle colonne:

* **Gruppo di requisiti**: descrive il raggruppamento logico del requisito. (NON MODIFICARE)
* **ID**: descrive il codice univoco del requisito (NON MODIFICARE)
* **Requisito:** descrive il singolo requisito individuato (NON MODIFICARE)
* **Obbligatorio (O) Premiale (P):** i requisiti contrassegnati con la
	+ **O** sono considerati essenziali/imprescindibili. La loro assenza non permette di prendere in considerazione la soluzione proposta;
	+ **P** sonoconsiderati importanti. Pur in loro assenza la soluzione sarà presa in considerazione.;
* **Requisito soddisfatto:** indica la disponibilità del requisito da parte della soluzione proposta nella versione attualmente disponibile (COMPILARE). La disponibilità/non disponibilità deve essere indicata con “SI/NO”.
* **Note** (DA COMPILARE OPZIONALMENTE): spazio da utilizzare per fornire precisazioni esplicative rispetto al soddisfacimento del requisito.

**Requisiti funzionali**

| **Gruppo requisiti funzionali** | **ID** | **Requisito funzionale (RF)** | **Obbligatorio (O) Premiale (P)** | **Requisito soddisfatto****(SI/NO)**  | **Note** |
| --- | --- | --- | --- | --- | --- |
| **Funzionalità Generali** | **RF1** | Il prodotto deve poter disporre di una console di amministrazione integrata che consenta di gestire graficamente la piattaforma e le funzionalità a disposizione | **O** |   |   |
| **RF2** | Il prodotto deve poter “profilare” amministratori diversi che possono operare su ambiti diversi | **O** |   |   |
| **RF3** | Il prodotto deve restituire statistiche sull’utilizzo e sul carico del sistema | **O** |   |   |
| **RF4** | Il prodotto deve mantenere e rendere visibile l’informazione della persona che ha richiesto il change, di chi l’ha approvato e del tecnico che ha preso in carico il task. | **O** |   |   |
| **RF5** | Il prodotto deve interagire con apparati in ambiente rete/sicurezza “multivendor” (principalmente Palo Alto, Cisco e Juniper con diverse versioni di sistema operativo e con router/switch Cisco e bilanciatori Alteon/f5) | **O** |   |   |
| **RF6** | Il prodotto deve poter generare dei report personalizzabili | **O** |   |   |
| **RF7** | Il prodotto deve poter effettuare controlli (audit) di compliance delle policy rispetto ad una “baseline” aziendale o di standard internazionali | **O** |   |   |
| **Funzionalità Generali** | **RF8** | Il prodotto deve avere anche funzioni di “SLA management” su tutte le fasi del change | **O** |  |  |
| **RF9** | Il prodotto deve evidenziare le policy create/modificate senza ticket associato | **O** |  |  |
| **RF10** | Le richieste di change (policy) oltre che per “IP/porta” devono poter essere richieste “per utente” e “per applicazione” | **O** |  |  |
| **RF11** | Il prodotto deve poter simulare l’applicazione di una policy (what-if) | **O** |   |   |
| **RF12** | La funzionalità di what-if deve anche evidenziale eventuali rischi di sicurezza che si presentano con l’applicazione della policy | **O** |  |  |
| **RF13** | Il prodotto deve poter evidenziale le “shadow policies” | **O** |   |   |
| **RF14** | Il prodotto deve poter evidenziare le policy che non hanno “match” da un periodo configurabile | **O** |   |   |
| **RF15** | Il prodotto deve poter evidenziare le vulnerabilità dei devices | **P** |   |   |
| **RF16** | Il prodotto deve poter indicare le policy da inserire, su quale apparato ed in quale posizione  | **O** |   |   |
| **RF17** | Il prodotto può (se configurato) implementare direttamente la policy sugli apparati.  | **O** |   |   |
| **RF18** | L’utente deve poter verificare se la sua richiesta è già soddisfatta da una policy più generale | **O** |  |  |
| **RF19** | L’utente deve poter richiedere change di policy non solo su base “IP/porta” ma anche per utente ed applicazione | **O** |  |  |
| **RF20** | L’utente deve poter vedere se una propria richiesta “viola” una policy aziendale  | **O** |  |  |
| **RF21** | L’utente deve poter vedere in ogni momento lo “stato” della sua richiesta (all’interno del workflow autorizzativo) | **O** |  |  |
| **Vulnerability assesment** | **RF22** | Il prodotto offre funzionalità di vulnerability assessment | **P** |   |   |
|  **RF23** | Il prodotto ha “on board” un motore di vulnerability scanner | **P** |   |   |
|  **RF24** | Il prodotto deve poter integrare i contenuti di vulnerabilità da almeno 20 “feed” esterni | **P** |   |   |
|  **RF25** | Il prodotto può verificare che l’applicazione di una policy non generi una vulnerabilità su un servizio  | **P** |   |   |
|  **RF26** | Il prodotto è in grado di individuare vulnerabilità anche per device IOT | **P** |  |  |
|  | **RF27** | Il prodotto è in grado di fornire anche una prioritizzazione delle vulnerabilità  | **P** |  |  |
|  |  |  |  |   |   |

**Requisiti non funzionali**

I requisiti “non funzionali” includono requisiti tecnici o di servizio.

| **Gruppo requisiti non funzionali** | **ID** | **Requisito tecnico, architetturale, infrastrutturale e non funzionale (RNF)** | **Obbligatorio (O) Premiale (P)**  | **Requisito soddisfatto**  | **Note**  |
| --- | --- | --- | --- | --- | --- |
| **Messa a disposizione** | **RNF1** | Il fornitore ha una presenza tecnica sul territorio italiano | P |   |  |
| **RNF2** | Il fornitore dispone di tecnici certificati dal produttore | P |  |  |
| **RNF3** | Il produttore ha una presenza commerciale in Italia  | P |   |  |
| **RNF4** | Il produttore ha una presenza tecnica (pre-sales) in Italia | P |  |  |
| **RNF5** | Il fornitore può erogare giornate di formazione e training on the job | P |   |  |
| **Deployment** | **RNF6** | La Soluzione adotta un sistema di traceability delle attività degli utenti, assicurando il monitoraggio attraverso la fruizione dei log | P |  |  |
| **RNF7** | Il software può essere messo a disposizioneattraverso modalità Cloud computing (SaaS). | P |   |   |
| **RNF8** | Il software può anche essere in modalità **multi-tenan**t. | P |   |   |
| **RNF8** | La soluzione deve poter operare in ambiente virtuale VMware | O |  |  |
| **RNF10** | La soluzione **può** operare in ambiente virtuale OpenStack | **P** |  |  |
| **Identity & Access Management** | **RNF11** | La soluzione di autenticazione e autorizzazione interna è totalmente compliant ai vincoli di sicurezza applicativa in aderenza alla legge D.lgs.196/2003, al Regolamento UE 679/2016 (di seguito, anche GDPR Privacy) e relativo decreto di attuazione e successivi aggiornamenti ed al Codice della Amministrazione Digitale. | O |   |   |
| **RNF12** | La soluzione prevede al suo interno la gestione dei profili degli utenti con accesso multiutente, con profilazioni differenziate, | O |   |   |
| **RNF13** | La profilazione deve essere garantita in funzione delle attività che gli utenti devono espletare sul sistema attraverso appositi ruoli che permettano di operare in maniera differenziata sulle funzionalità. | O |  |  |
| **RNF14** | Il prodotto deve avere la gestione delle utenze integrata con Active Directory | O |   |   |
| **RNF15** | L’utente deve essere in grado di accedere al sistema utilizzando i più comuni Internet browser (Internet Explorer, Chrome, Firefox) | **O** |  |  |
| **RNF16** | Interfaccia utente in HTML5 | **P** |  |  |
| **RNF17** | L’utente deve potersi autenticare al sistema tramite le proprie credenziali di Dominio | **O** |  |  |
| **Interoperability** | **RNF18** | L’interoperabilità con i sistemi esterni è basata su protocolli di comunicazione a Web Services di tipo SOAP o RESTful per l’implementazione dell’architettura SOA. | P |   |   |
| **RNF19** | La soluzione espone API Web per l'interoperabilità con altre applicazioni esterne. | P |   |   |
| **Performance & Availability**  | **RNF20** | Il fornitore garantisce l’import dell’attuale DB (su Remedy 8) dei ticket del CSI al fine di salvaguardare lo storico dei change richiesti e ne garantisce l’integrazione con la piattaforma | O |  |  |
| **RNF21** | La Soluzione continua ad essere disponibile indipendentemente dalla quantità di accessi, senza soluzione di continuità né decadimento apprezzabile delle prestazioni. | O |   |   |
| **RNF22** | Il prodotto deve disporre di una soluzione di HA (High Availability)  | **O** |  |  |
| **RNF23** | Aggiornamento software e patching in continuità di servizio per l’utente (almeno per le minor release) | **O** |  |  |
| **Backup** | **RNF24** | Sono previste delle procedure di backup dei dati e dei sistemi. | O |   |   |

**Modalità di fornitura della soluzione**

| **ID** | **Modalità di fornitura (MF)** | **Obbligatorio (O) Premiale (P)** | **Requisito soddisfatto**  | **Note** |
| --- | --- | --- | --- | --- |
| **MF1** | Le licenze sono fornite in modalità “perpetual” | P |   |   |
| **MF2** | Le licenze sono fornite in modalità “subscription” | P |   |   |
| **MF3** | La soluzione non deve limitare il numero degli utenti fruitori né prevedere metodi di licencing basati sul numero di utenti che vi accedono | O |   |   |
| **MF4** | La licenza non prevede limiti relativi alla **tipologia di soggetti** autorizzati alla fruizione del software (ad esempio, solo dipendenti, oppure terzi che a qualsivoglia titolo operino nell’interesse del licenziatario, ecc.). | O |   |   |
| **MF5** | La licenza e/o il prodotto non prevedono **dipendenze da elementi di terze parti** eventualmente integrati nel prodotto in oggetto e/o da cui lo stesso dipenda per il relativo funzionamento. Nelle note fornire l'elenco dettagliato corredato dagli annessi vincoli d'uso di qualsivoglia natura e con quali modalità verranno trasferiti al fornitore del servizio IaaS. | P |   |   |
| **MF6** | È disponibile con licenza di diritto d'uso nel perimetro definito a Capitolato. | O |  |  |
| **MF7** | È riconosciuto il diritto di ispezionabilità del codice sorgente, garantendone pertanto la relativa disponibilità ed accessibilità a mezzo deposito presso notaio. | P |  |  |
| **MF8** | È riconosciuto il diritto di ispezionabilità del codice sorgente, garantendone la relativa disponibilità ed accessibilità direttamente al Committente. | P |  |  |
| **MF9** | È riconosciuto anche il diritto di modificabilità del codice sorgente, anche ai fini di creazione di opere derivate ed eventuale diritto di redistribuzione (specificare con le relative condizioni, nel caso). | P |  |  |
| **MF10** | La soluzione è rilasciata con licenza di software libero / Open Source. | P |  |  |
| **MF11** | I diritti di cui sopra si estendono ad ogni patch, aggiornamento e/o release eventualmente rilasciate sul prodotto in continuità. | P |  |  |
| **MF12** | I diritti di cui sopra possono essere esercitati per il tramite di propri enti in house strumentali. | P |  |  |
| **MF13** | Con riferimento al profilo di licenza di cui alle precedenti righe, è prevista la possibilità di estendere l’utilizzo della soluzione anche ad altre amministrazioni locali del territorio e strutture private accreditate convenzionate, oltre il perimetro previsto dal Capitolato. | P |  |  |
| **MF14** | La licenza non prevede limitazioni a metrica associata. Ad es.: numero di utenti e/o processori e/o accessi contemporanei o loro assenza; numero di dispositivi collegabili (come ad esempio stampanti, scanner, ecc.) o loro assenza; eventuale numero massimo di processori o core su cui il software può essere eseguito; numero di elaborazioni da effettuare nell'arco di validità della licenza superato il quale occorre corrispondere un controvalore maggiore. | P |  | Se ad oggi sono presenti limitazioni, indicare le metriche di licensing, le fasce di upgrade e i relativi prezzi per ogni funzionalità |
| **MF15** | Per quanto riguarda gli "sviluppi ad hoc" richiesti e finanziati dall’Amministrazione la stessa può acquisire la titolarità del software così realizzato, ovvero acquisire i diritti di proprietà intellettuale (diritti di sfruttamento economico) e/o di diritto industriale; detti diritti nel caso riguardano tutto quanto realizzato dal fornitore (anche tramite eventuali subappaltatori in esecuzione della fornitura), comprensivo ad es. di codici binari e sorgenti, materiali preparatori, documentazione e ogni altro materiale e/o documento creati, inventati, modificati, predisposti o realizzati dal fornitore o dai suoi dipendenti nell’ambito o in occasione dell’esecuzione della fornitura, in modo che il Committente possa esercitare senza restrizione alcuna di condizioni e/o di tempo i relativi diritti di titolarità previsti dalla normativa di riferimento (uso, redistribuzione, pubblicazione, cessione, anche parziale, modifica ed evoluzione, etc.) | P |  |  |
| **MF16** | È prevista la disponibilità del fornitore a mettere a disposizione dell’Amministrazione, a titolo gratuito (o eventualmente ricompreso nel costo delle licenze d’uso) il servizio di assistenza all’uso del software, di segnalazione malfunzionamenti e della correzione degli stessi. | O |  |  |
| **MF17** | Sono previste delle Garanzie e i relativi limiti, in base alla legge vigente. | P |  |  |
| **MF18** | Non sono previste eventuali ulteriori clausole da valutare attentamente e prendere in considerazione che potrebbero limitare l'uso delle licenze così come desunto tramite le risposte alle domande precedenti.  | O |  |  |
| **MF19** | Il software è messo a disposizioneanche attraverso modalità Cloud computing o "SaaS" (software as a service, in cui il software viene erogato come servizio da remoto). |  |  | Indicare se è disponibile o meno  |
| **MF20** | È incluso nella licenza il diritto di ricevere gli aggiornamenti per la durata del contratto. | O |  |  |
| **MF21** | È previsto l'ampliamento dei giorni e dell'orario di attività dell'assistenza applicativa minima richiesta nel Capitolato tecnico. | P |  |  |
| **MF22** | Il software è messo a disposizione "on-premises" o mediante concessione di licenza, tramite fornitura di una o più copie del software per l'installazione ed esecuzione su una o più macchine del licenziatario. | P |  |  |

**Nota bene**: Alcune voci relative alla modalità di fornitura indicate in tabella sono alternative fra loro (es. soluzione SaaS o *on premise*, licencing perpetual o a subscription, etc.), non costituiscono un requisito, ma sono funzionali solo alla migliore comprensione delle caratteristiche della soluzione proposta. Fanno eccezione le voci contrassegnate con la O (obbligatori) in quanto imprescindibili.

**DIMENSIONAMENTO DELLA SOLUZIONE**

Per consentire al fornitore una stima dei costi e dei tempi si riportano di seguito alcuni dati di dimensionamento:

| **ID** | **Descrizione** | **Q.tà** |
| --- | --- | --- |
| **1** | Numero di utenti abilitati all’utilizzo della soluzione | **>1000** |
| **2** | N. di firewall CED (compresi i virtuali) | **30** |
| **3** | N. di firewall remoti (branch office) | **20** |
| **4** | Numero di nodi di rete (L3) – compresi bilanciatori | **100** |
| **5** | Numero di device (FW, server, router ecc.) per cui si richiede un controllo delle vulnerabilità  | **500** |
| **6** | N. di giornate di supporto specialistico **remoto** (mail o telefono) da erogarsi a consumo all’interno della durata contratto di manutenzione  | **5** |
| **7** | N. di giornate di supporto specialistico **on-site** da erogarsi a consumo all’interno della durata del contratto di manutenzione | **5** |

**COSTI E TEMPI INDICATIVI DELLA MESSA A DISPOSIZIONE DELLA SOLUZIONE**

Si richiede di compilare le seguenti tabelle relative a costi e tempi per la messa a disposizione e per la gestione della soluzione desiderata. Si ricorda che si tratta di stime di massima, non impegnative (non costituiscono offerta), ma utili a definire la base d'asta e il capitolato per una eventuale gara finalizzata all’acquisizione della soluzione dal mercato.

In particolare, le stime riguardano:

* i requisiti funzionali e non funzionali;
* la messa in esercizio della soluzione.

Requisiti funzionali e non funzionali

**Costo delle componenti già disponibili**: costo complessivo delle componenti funzionali e non funzionali, già disponibili, della soluzione proposta che contribuiscono a soddisfare i requisiti obbligatori (O). L’eventuale costo di licenza per l’uso della soluzione è incluso in queste stime

**Stima costo aggiuntivo per il completo soddisfacimento:** stima del costo aggiuntivo necessario all’eventuale soddisfacimento dei requisiti Premiali (P). Al riguardo, si precisa che parte dei requisiti premiali costituiscano già una implementazione prevista dal Fornitore nella propria roadmap di sviluppo, si fornisca una stima complessiva dell’incremento di costo ipotizzato per la soluzione nel suo complesso. Per i requisiti premiali (P), invece, non altrimenti già previsti dal fornitore a proprio investimento, si fornisca per difetto una stima ipotizzata dei giorni uomo necessari per una integrazione ad hoc.

| **ID** | **Voci di costo** | **Stima costo (Euro) //GG UOMO**  | **Stima tempi (GG)** |
| --- | --- | --- | --- |
| 1 | Costo per le componenti “Obbligatorie” (O) |  |  |
| 2 | Costo per le componenti “Premiali” (P) \* |  |  |
| 3 | Messa a disposizione di un “manuale d’uso utente” in formato elettronico da mettere a disposizione di tutti gli “end-user” per le richieste di change |  |  |
| 4 | Costi di upgrade delle licenze |  |  |
|  | **TOTALE** |  |  |

\*il costo delle componenti Premiali va suddiviso per singola tipologia dei RF e RNF

Messa in esercizio della soluzione.

| **ID** | **Voci di costo** | **Stima costo (Euro)** | **Stima tempi (GG)** |
| --- | --- | --- | --- |
| 1 | Installazione e configurazione del software finalizzata alla messa in esercizio (deploy, configurazioni, integrazioni, collaudo.) |  |  |
| 2 | Formazione ai sistemisti per la gestione e configurazione della piattaforma |  |  |
| 3 | Messa a disposizione di un “manuale d’uso utente” in formato elettronico da mettere a disposizione di tutti gli “end-user” per le richieste di change |  |  |
|  | **TOTALE** |  |  |

Supporto Specialistico

| **ID** | **Voci di costo** | **GG** | **Stima costo (Euro)** |
| --- | --- | --- | --- |
| 1 | N. di giornate di supporto specialistico **remoto** (mail o telefono) da erogarsi a consumo all’interno della durata contratto di manutenzione  | **5** |  |
| 2 | N. di giornate di supporto specialistico **on-site** da erogarsi a consumo all’interno della durata del contratto di manutenzione | **5** |  |
|  | **TOTALE** |  |  |

**COSTO INDICATIVO ANNUO DI GESTIONE DELLA SOLUZIONE**

| **ID** | **Attività di gestione della soluzione**  | **Stima costo 3 anni (Euro)** |
| --- | --- | --- |
| 1 | “Support & Maintenance” comprensivo fornitura minor e major release e assistenza con SLA “*next business day”* - **per requisiti Obbligatori** |  |
| 2 | “Support & Maintenance” comprensivo fornitura minor e major release e assistenza con SLA “*next business day”* - **per requisiti Premiali** |  |
|  | **TOTALE** |  |