Allegato 2.2 – Specifiche tecniche (minime) del lotto n.5 ("Implementazione 'chiavi in mano' di un sistema centralizzato per la rilevazione degli Asset sia fisici che virtuali e per la gestione degli accessi, basato su protocollo di rete 802.1x (o equivalente) e autenticazione a più fattori")

La Ditta dovrà provvedere all'implementazione del sistema in oggetto all'interno della server-farm comunale fornendo tutto il materiale hardware e software necessario incluse le eventuali licenze d'uso (per entrambe le componenti) di tipo perpetuo e illimitato (ovviamente laddove l'hardware e/o il software non fossero di tipo proprietario). Tale sistema dovrà essere conforme alle specifiche tecnico funzionali di cui alla circolare Agid n.2/2017 sulle misure minime di sicurezza (in particolare leggasi ABSC_ID: 1.4, 1.5, 1.6, 5.6) e raggiungere i seguenti obiettivi:

a) limitare e controllare quali dispositivi possono essere connessi alla rete informatica;
b) implementare un sistema di autenticazione a più fattori per gli utenti standard e "privilegiati" (alias "amministratori di rete e/o di sistema") dell'Ente;
c) fornire un accesso di rete altamente sicuro sia agli utenti che ai dispositivi dando visibilità di informazioni ad esempio su chi è connesso;
d) implementare una unica console per la gestione, rilevazione e censimento di tutti gli asset (sia di tipo fisico che virtuale) informatici posseduti dall'Ente;

Il sistema dovrà altresì:

a) prevedere un sistema di autenticazione in tecnologia Cisco per essere perfettamente integrato con la tecnologia LAN (wireless e fonia) in uso presso l' Ente, supportando il protocollo 802.1x (o equivalente);
b) implementare l'autenticazione utenti (come sopra definiti) a più fattori anche per l'accesso all'ambiente Citrix in uso presso l'Ente;
c) condividere dati contestuali vitali, quali identità di utenti e dispositivi, in modo da poter identificare, contenere e correggere più rapidamente le minacce e gli accessi;
d) adottare un sistema di profiling in grado di fornire informazioni dettagliate sugli asset informatici - sia di tipo fisico che virtuale - in uso presso l' Ente e connessi alla rete informatica comunale, adottando per essi una console di gestione, rilevazione e censimento unica;
e) essere in grado di supportare e gestire immediatamente tutte le utenze e gli asset (fisici e/o virtuali) informatici in uso presso l'Ente, senza alcuna limitazione né di numero né di tipologia, al fine di poter soddisfare in futuro nuove esigenze e configurazioni organizzative dell'Ente, senza che ciò comporti ulteriori costi per l'Ente stesso;
f) sfruttare e integrarsi quanto più possibile con le tecnologie (Cisco, Vmware, Microsoft, MS SQL, ecc) già presenti all'interno dell'infrastruttura IT comunale eventualmente aggiornandole e potenziandole – laddove necessario - al modello di licensing opportuno: ciò al fine di non indurre ulteriori oneri - a livello tecnico ed economico - sull'Ente derivanti dall'adozione di nuove tecnologie che potrebbero far aumentare in modo incontrollato la complessità dell'infrastruttura IT comunale e quindi i relativi costi di gestione;
g) presentare le seguenti caratteristiche/funzionalità di tipo "evoluto":

- **Gestione Centralizzata delle identità e delle policy aziendali**
  - Creazione Policy basato su regole e su attributi quali l'identità dell'utente e dell'endpoint, i protocolli di autenticazione, l'identità del profilo e altri attributi esterni per attuare politiche di controllo degli accessi;
  - Capacità di integrazione con più archivi di identità esterni come Microsoft Active Directory, LDAP (Lightweight Directory Access Protocol), RADIUS, RSA One-Time Password (OTP), autorità di certificazione per autenticazione e autorizzazione e Open Database Connectivity (ODBC);
- **Controllo centralizzato degli accessi**

Il sistema dovrà:

- essere in grado di fornire una vasta gamma di opzioni di controllo degli accessi, tra cui, a titolo di esempio, elenchi di controllo degli accessi scaricabili (dACL), assegnazioni di LAN virtuale (VLAN), reindirizzamenti URL, ACL denominati e gruppi di sicurezza (SG);

- garantire l'accesso sicuro alla rete in base al ruolo aziendale per fornire una policy di accesso alla rete coerente per gli utenti finali, sia che essi si connettano attraverso una rete cablata, wireless o VPN;

- permettere la creazione di una policy di segmentazione definita dal software per contenere le minacce della rete al fine di implementare il controllo degli accessi basato su ruoli a livello di routing e switching. Dovrà inoltre essere in grado di segmentare dinamicamente l'accesso senza la complessità di più VLAN o la necessità di riprogettare la rete.

- **Identificazione precisa dei dispositivi**

  - Il sistema dovrà garantire la visibilità e l'identificare dei dispositivi in modo accurato grazie alla gestione dei profili dei dispositivi e al servizio di feed dei profili stessi;

- **Autenticazione utenti**

  - Il sistema dovrà implementare per gli utenti (standard e privilegiati) un' di autenticazione a più fattori (ex. Smart card, Token fisico, One Time Password (OTP), biometria), l'accesso unico delle utenze alle Management Console necessarie per la gestione e manutenzione di tutta l'infrastruttura IT dell'Ente (ad esempio SQL Management Studio, VMware Virtual Center, Citrix Studio, ecc).

- **Rilevazione degli asset fisici e virtuali**

  - Il sistema dovrà essere in grado di rilevare automaticamente tutti gli asset (fisici e virtuali) presenti nell'infrastruttura IT comunale, consentendone il censimento e/o la gestione attraverso un'unica console in grado di esportare i dati acquisiti nei formati documentali e testuali più diffusi (es. pdf, excel, xml, txt, ecc) facendo riferimento a un modello di report altamente configurabile in relazione alle esigenze dell'Ente;