

ALLEGATO A

CAPITOLATO TECNICO E RELATIVE APPENDICI

CLASSIFICAZIONE CONSIP PUBLIC

APPENDICE 3 AL CAPITOLATO TECNICO - Lotto 2

Servizi di monitoraggio (SOC)

Indice

1	<i>PREMESSA</i>	3
2	<i>SERVIZI DI MONITORAGGIO</i>	4

1 PREMESSA

In aggiunta ai servizi richiesti nel Capitolato Tecnico, il Fornitore ha facoltà di offrire i servizi di monitoraggio in ambito sicurezza da erogare in modalità “as a service” attraverso un Security Operating Center (SOC) operante presso il Centro Servizi.

Il Fornitore in un documento separato dall’Offerta Tecnica (e pertanto non concorrerà al calcolo delle pagine dell’Offerta tecnica) dovrà descrivere:

- o le infrastrutture tecnologiche e le architetture a supporto dei servizi di monitoraggio;
- o le modalità operative e gli strumenti che intende adottare per la realizzazione delle attività di monitoraggio erogate dal SOC al fine di supportare da remoto le Amministrazioni nelle attività di rilevazione di incidenti e/o attacchi ostili;
- o le modalità operative e gli strumenti che intende adottare per le eventuali azioni preventive da svolgere e delle modalità da adottare per la comunicazione;
- o le metriche e le eventuali fasce per la determinazione del prezzo dei servizi offerti.

Il Fornitore nell’apposito foglio di lavoro fornito con la documentazione di gara dovrà indicare i relativi prezzi offerti per l’erogazione del servizio.

Si precisa che sia la soluzione tecnica offerta sia la relativa quotazione economica non saranno oggetto di valutazione né tecnica né economica. AgID/Consip si riservano l’eventuale inserimento del servizio all’interno del Contratto Quadro, mediante specifica approvazione del Comitato di Direzione Tecnica.

Se i servizi di monitoraggio offerti saranno inseriti da Consip nel Contratto Quadro, il Fornitore assume sin d’ora l’obbligo di prestare detti servizi in ambito sicurezza in favore delle Amministrazioni che ne faranno richiesta nei Contratti Esecutivi.

Ai servizi di monitoraggio si applicheranno i seguenti indicatori di qualità (vedi Appendice 1 del Capitolato Tecnico):

- indicatori IQ01 e IQ02 in ambito “Governo della fornitura e servizi professionali”;
- indicatori IQ07, IQ08 e IQ09 in ambito “Centri Servizi”;
- indicatori IQ10, IQ11, IQ12 e IQ13 in ambito “Help Desk”;
- indicatori IQ14, IQ15, IQ22 e IQ23 in ambito “Qualità di erogazione dei servizi”;
- indicatori IQ24, IQ25 e IQ26 in ambito “Collaudo dei servizi”.

2 SERVIZI DI MONITORAGGIO

Descrizione del servizio

1. I servizi di monitoraggio devono consentire alle Amministrazioni l'individuazione e la prevenzione dei rischi derivanti dagli attacchi informatici.
2. I servizi di monitoraggio sono erogati dal Fornitore attraverso un Security Operating Center (SOC) operante presso il Centro Servizi che si farà carico degli oneri di monitoraggio dei servizi di sicurezza, mantenendo la segregazione degli utenti, dei ruoli e dei dati delle Amministrazioni.

Il SOC deve anche supportare le Unità Locali di Sicurezza, per la gestione degli aspetti relativi alla sicurezza.

3. Il Fornitore, nell'ambito dei servizi di monitoraggio deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:
 - monitoraggio di apparati IDS/IPS e di apparati Firewall;
 - monitoraggio delle piattaforme di autenticazione forte comprendente la modalità di gestione delle policy, degli utenti e dei loro privilegi;
 - raccolta delle informazioni provenienti dai diversi servizi di sicurezza in ambito e segnalazione tempestiva di eventuali problemi;
 - attività di troubleshooting;
 - archiviazione dei log nel rispetto delle normative vigenti, in archivi immutabili e inalterabili;
 - notifica di eventi/allarmi a fronte del superamento di soglie prefissate e a seguito del verificarsi di eventi critici che impattano sulla sicurezza dell'ambiente informatico.

Tipologia del servizio

I servizi di monitoraggio saranno erogati in modalità continuativa di tipo "as a service".