SISTEMA SANITARIO REGIONALE

AZIENDA OSPEDALIERA
SAN GIOVANNI ADDOLORATA

REGIONE LAZIO

DELIBERAZIONE DEL DIRETTORE GENERALE 740 del 09 AGO. 2022
Numero data

Oggetto: Contratto Quadro CONSIP SPC Lotto 2 – ditta Leonardo S.p.a. - Adesione fino al 31/12/2022 dei servizi di sicurezza per le pubbliche amministrazioni per un importo pari a € 113.153,37 IVA esclusa - CIG 5518849A42- CIG Derivato 9355004983

Esercizio 2022 Conto 502020119
Macro _____ Sub _____

Centro di Costo _____

Sottoconto n° _____

Budget:
- Assegnato € _____
- Utilizzato € _____
- Presente Atto € 138.047,11
- Residuo € _____

Ovvero schema allegato ■

Il Direttore della UOC Economico Finanziaria e Patrimoniale
p. 8/8/22

Struttura proponente

UOSD ICT

Estensore Monica Simeoni

Data 03/08/2022 Firma _____

Responsabile del Procedimento
Ing. Gabriele Rinonapoli

Data 03/08/22 Firma _____

Il Dirigente della UOSD ICT
Ing. Gabriele Rinonapoli

Data 03/08/22 Firma _____

Proposta n° 799 del 05 AGO. 2022

PARERE DEL DIRETTORE SANITARIO

Favorevole

Data 9/8/2012

IL DIRETTORE SANITARIO
Patrizia Magrini

PARERE DEL DIRETTORE AMMINISTRATIVO

FAVOREVOLE

Data 9/8/12

X IL DIRETTORE AMMINISTRATIVO
Alberto Fiore

Gli estremi della registrazione e della data di pubblicazione sono riportati nell'ultimo foglio allegato alla presente delibera.

Il Responsabile della U.O.S.D. I.C.T.

VISTO il Decreto Legislativo n. 50/2016 e successive modificazioni ed integrazioni;

il Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale)

il Decreto Legge n.50/2022 del 17/05/2022 relativo a "Misure urgenti in materia di politiche energetiche nazionali, produttività delle imprese e attrazione degli investimenti, nonché in materia di politiche sociali e di crisi ucraina"

l'articolo I della legge 28 dicembre 2015, n.208, che, al comma 512, prevede che "*Al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, provvedono ai propri approvvigionamenti esclusivamente tramite Consip SpA o i soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti*"

VISTA la deliberazione n.184/CS del 26/03/2019 "Attivazione delle Unità operative centrali e degli Uffici amministrativi di cui all'Atto Aziendale adottato con deliberazione n. 88/DG del 29 gennaio 2019, di parziale modifica della deliberazione n. 582/DG del 27 giugno 2018, e approvato con DCA n. U00117 del 18/03/2019" con cui è stata attivata l'unità operativa centrale UOSD I.C.T. come prevista dall'Atto Aziendale;

la Deliberazione di Giunta Regionale n. 589/2022 avente a oggetto: "Approvazione del Bilancio Economico Preventivo (BEP) per l'esercizio 2022 degli Enti del S.S.R rientranti nel perimetro di consolidamento, della GSA e del Consolidato S.S.R. ai sensi dell'art. 32, c. 5 del D.Lgs 118/2011";

la deliberazione n. 269/DG del 29.03.2022, con la quale è stata affidata la Responsabilità della U.O.S.D. I.C.T., dal 01/04/2022, all'Ing. Gabriele Rinonapoli, Dirigente Analista;

RICHIAMATO l'art. 51 del Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) relativo alla "Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni";

l'art. 49, comma 2 del Decreto Legge n.50 del 17/05/2022, per cui: *L'articolo 31-bis del decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120, è sostituito dal seguente: «Art. 31-bis (Proroga di accordi quadro e convenzioni delle centrali di committenza in ambito digitale) -1. In conseguenza dell'ampia adesione delle pubbliche amministrazioni e tenuto conto dei tempi necessari all'indizione di nuove procedure di gara, gli accordi quadro, le convenzioni e i contratti quadro di cui all'articolo 3, comma 1, lettere cccc) e dddd), del codice dei contratti pubblici, di cui al decreto legislativo 18 aprile 2016, n. 50, aventi ad oggetto le categorie merceologiche indicate all'articolo 16-bis, comma 7, del decreto-legge 21 ottobre 2021, n. 146, convertito, con modificazioni, dalla legge 17 dicembre 2021, n. 215, che siano in corso alla data del 28 febbraio 2022 sono prorogati, con i medesimi soggetti aggiudicatari, fino al 31 dicembre 2022, al fine di non pregiudicare il perseguimento, in tutto il territorio nazionale, dell'obiettivo di transizione digitale previsto dal Piano nazionale di ripresa e resilienza.»*

PREMESSO che la società Consip S.p.A. ha stipulato con l'RTI composto dalle aziende Leonardo-Finmeccanica S.p.A, IBM Italia S.p.A., FASTWEB S.p.A. e Sistemi Informativi S.r.l., il Contratto Quadro relativo al lotto 2 (*"Servizi di gestione delle identità digitali e sicurezza applicativa"*) della procedura ristretta per l'affidamento dei servizi di Cloud Computing, di Sicurezza, di Realizzazione di Portali e Servizi on-line e di Cooperazione Applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403);

che il Lotto 2 della procedura comprende le seguenti tipologie di servizi:

- servizi per la gestione delle identità digitali, erogati in modalità "as a service", in conformità anche all'art. 64 del CAD;
- servizio di firma digitale remota comprensiva della fornitura di certificati e servizio di timbro elettronico, erogati in modalità "as a service", volti a favorire la dematerializzazione dei documenti e la digitalizzazione dei processi amministrativi;
- servizi di sicurezza, erogati sia in modalità "as a service" attraverso i Centri Servizi del Fornitore sia in modalità "on premise", atti a garantire la sicurezza applicativa e a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi; i servizi di sicurezza includono anche servizi professionali a supporto delle attività erogati presso i centri delle Pubbliche Amministrazioni.

che, in applicazione di quanto stabilito nel Contratto Quadro stipulato dalla Consip S.p.A. con l'RTI aggiudicatario, ciascuna Amministrazione che scelga di aderire al citato Contratto Quadro, procede alla stipula di Contratti Esecutivi;

che con delibera n.126 del 14.03.2019, l'Azienda Ospedaliera San Giovanni Addolorata ha aderito al Contratto Quadro, stipulando con l'RTI aggiudicatario, un Contratto Esecutivo, per l'erogazione dei servizi di sicurezza dal 01/04/2019 al 31/07/2021, per un importo complessivo pari a € 437.047,36 Iva esclusa – CIG derivato 74264070EE;

che con delibera n.782 del 24.12.2021, l'Azienda Ospedaliera San Giovanni Addolorata ha nuovamente aderito al Contratto Quadro, stipulando con l'RTI aggiudicatario un nuovo Contratto Esecutivo per l'erogazione dei servizi di sicurezza, fino alla scadenza del Contratto Quadro, prevista per il 20/07/2022 e per un importo complessivo pari a € 118.256,63 Iva esclusa – CIG derivato 8982185D89;

VISTO che il Contratto Esecutivo di cui alla deliberazione n.782 del 24.12.2021 è scaduto in data 20/07/2022;

CONSIDERATO che, in termini di servizi di sicurezza, sono state evidenziate nuove esigenze rispetto a quanto previsto con il Progetto dei fabbisogni identificato con GOVM-210321 v.1, di cui alla delibera n.782 del 24.12.2021;
che in particolare, i servizi di monitoraggio devono essere estesi ad ulteriori sistemi informatici, tra cui i firewall interni e i domain controller, non compresi nella attuale configurazione;

che inoltre, anche a seguito degli eventi che hanno determinato l'attacco hacker del settembre 2021, è necessario mettere in atto azioni in coerenza con il Framework Nazionale Cyber Security e Data Protection ed in particolare procedere con un assessment puntuale delle infrastrutture, al fine di valutare l'attuale postura di sicurezza aziendale e prevedere eventuali azioni correttive;

che pertanto in data 25/07/2022 la UOSD ICT ha trasmesso a mezzo PEC alla società Leonardo-Finmeccanica Spa il nuovo Piano dei Fabbisogni, di cui al prot. 25675/22, comprensiva del SERVIZIO DI MONITORAGGIO CONTINUATIVO DEGLI EVENTI DI SICUREZZA, del SERVIZIO MANAGED DETECTION & RESPONSE, di SERVIZI DI CONSULENZA relativi al Framework Nazionale Cyber Security e Data Protection e di eventuali SERVIZI DI SUPPORTO PER INTERVENTI DI ADEGUAMENTO;

VISTA la nota di riscontro inviata via PEC (Ns Prot. LDO/CYS/P/0033719/22) dalla società Leonardo-Finmeccanica Spa il giorno 02/08/2022 contenente il Progetto dei Fabbisogni;

ACQUISITO il Progetto dei Fabbisogni trasmesso dalla società Leonardo-Finmeccanica Spa in data 02/08/2022 e identificato con GOVM-220272 Rev. 01;

VISTO che in base a quanto previsto dall'art. 49, comma 2 del Decreto Legge n.50 del 17/05/2022 il Contratto Quadro SPC Cloud lotto 2 è stato prorogato fino al 31.12.2022;

che il costo complessivo dei servizi inclusi nel Progetto dei Fabbisogni GOVM-220272 Rev. 01 è pari ad € 113.153,37 Iva esclusa;

RITENUTO necessario, per quanto sopra rappresentato, dover procedere ad una nuova adesione al Contratto Quadro SPC Cloud lotto 2, fino al 31.12.2022, in favore del RTI aggiudicatario Leonardo-Finmeccanica S.p.A, IBM Italia S.p.A., FASTWEB S.p.A. e Sistemi Informativi S.r.l., per un importo complessivo pari ad € 113.153,37 IVA esclusa - CIG derivato 9355004983;

RILEVATO che l'onere complessivo derivante dal presente provvedimento, pari a € 138.047,11 IVA inclusa, trova copertura per l'anno 2022 sul conto 502020119 (Altri servizi non sanitari da privato) secondo il seguente prospetto:

che l'importo di € 138.047,11 iva inclusa, non comporta uno scostamento rispetto alla scheda BEP 2022, approvata con Deliberazione 589/2022, cui afferisce il sotto-conto di imputazione;

ATTESTATO che il presente provvedimento risulta necessario ed improcrastinabile;

che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e successive modifiche ed integrazioni, nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1 della legge 241/90 e successive modifiche ed integrazioni;

PROPONE

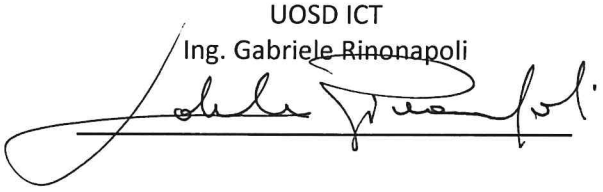
per i motivi in narrativa esposti che formano parte integrante e sostanziale del presente provvedimento:

1. di approvare il progetto dei fabbisogni prot. GOVM-220272 Rev. 01, allegato alla presente deliberazione;
2. di aderire al Contratto Quadro SPC Cloud lotto 2, con la sottoscrizione di un nuovo Contratto Esecutivo con scadenza al 31.12.2022, in favore del RTI aggiudicatario Leonardo-Finmeccanica S.p.A, IBM Italia S.p.A., FASTWEB S.p.A. e Sistemi Informativi S.r.l., per un importo complessivo pari ad € 113.153,37 IVA esclusa - CIG derivato 9355004983;
3. di confermare quale RUP dell'affidamento l'ing. Gabriele Rinonapoli, Dirigente della struttura proponente;
4. di confermare quale DEC dell'affidamento il Dott. Michelangelo Baglioni, Collaboratore Tecnico della UOSD ICT;

5. di far gravare gli oneri derivanti dal presente atto, pari a € 138.047,11 iva inclusa, sul sotto conto 502020119 "altri servizi sanitari da privato" per l'anno 2022;
6. di dare atto che il presente provvedimento risulta necessario e improcrastinabile al fine di garantire la sicurezza dei sistemi informativi aziendali;

La U.O.C. Economico Finanziaria e Patrimoniale curerà la registrazione contabile del valore economico riferito agli esercizi di competenza

Il Dirigente
UOSD ICT
Ing. Gabriele Rinonapoli



IL DIRETTORE GENERALE

VISTO il D.L.vo 30.12.1992, n. 502 e successive modifiche ed integrazioni;

IN VIRTU' dei poteri conferiti con Decreto del Presidente della Regione Lazio n. T00025 del 25 febbraio 2021;

PRESO ATTO che il Dirigente proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della Legge 20/94 e successive modifiche ed integrazioni, nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1 della L. 241/90 e successive modifiche ed integrazioni;

VISTO il parere favorevole Direttore Amministrativo e del Direttore Sanitario;

ritenuto di dover procedere

DELIBERA

di approvare la proposta così come formulata, rendendola disposto.

La U.O.C. Affari Generali e gestione amministrativa ALPI curerà tutti gli adempimenti relativi alla registrazione ed alla pubblicazione della presente deliberazione.

La presente deliberazione è composta da n.____6__ pagine, compreso il frontespizio, di n. 1 foglio di registrazione e pubblicazione, nonché di N. 1 allegato così composto:

- Allegato 1 – Progetto dei Fabbisogni - composto da n. 24 pagine.

Il Direttore Generale
Dott.ssa Tiziana Frittelli

Identificativo: GOVM-220272 Rev. 01

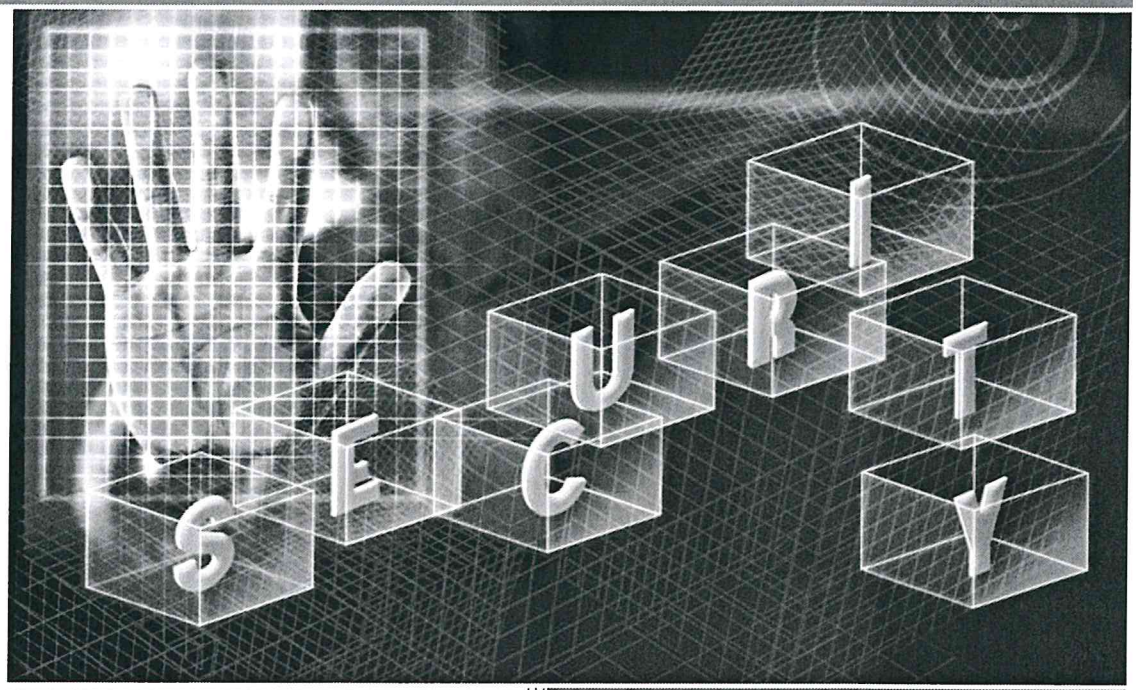
Data: 01/08/2022

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403)

LOTTO 2

Azienda Ospedaliera San Giovanni

Progetto dei fabbisogni



LEONARDO
IBM
SISTEMI INFORMATIVI
An IBM Company
FASTWEB

Costituito
Raggruppamento Temporaneo di Imprese
composto da:
Leonardo S.p.A. - Cyber & Security Solutions division
IBM SpA
Sistemi Informativi srl
Fastweb SpA

	Nome e Ruolo	Firma
Autore		
	Giorgio Castrucci	
Verifica		
	Germano Matteuzzi	
Approvazione		
	Mauro Pucciarini	
Autorizzazione		
	Claudio Rando	

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
01	Vedi data di copertina	AO San Giovanni	

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
01	Vedi data di copertina	Prima emissione	RTI

Il Progetto dei fabbisogni si compone dei seguenti documenti:

Volume principale	Documento nel quale si intende raccogliere e dettagliare le richieste dell'Amministrazione contraente contenute nel Piano dei Fabbisogni e formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro e nei relativi allegati.
Appendice A, Progetto di attuazione	Per ciascun servizio richiesto dal Piano dei fabbisogni, l'appendice contiene i seguenti dettagli: identificativo del servizio; configurazione (ove applicabile); quantità; costi; indirizzo/i di dispiegamento (nel caso di servizi centralizzati si riporterà il solo indirizzo della sede centrale); data prevista di attivazione; impegno delle eventuali risorse professionali previste; descrizione della struttura funzionale ed organizzativa del centro servizi, completa dei nomi e dei ruoli delle figure responsabili per ciascuno dei servizi.
Appendice B, Piano di lavoro	Appendice che contiene l'elenco delle attività/fasi previste con le relative date di inizio e fine. Tutte la fasi previste dal piano indicano gli obiettivi, i tempi necessari comprensivi delle date da garantire, i deliverable prodotti e le date di consegna.
Allegato 1, Modalità di presentazione e approvazione degli Stati di avanzamento mensili	Documento che definisce nei modi e nei tempi come sarà presentato lo stato di avanzamento dei Lavori (SAL). Da consegnarsi in fase di avvio dei lavori.
Allegato2, Documento programmatico di gestione della sicurezza dell'Amministrazione	Da consegnarsi su richiesta dell'Amministrazione
Allegato 3, Piano della qualità	Vedere piano di qualità generale, Documento [DA-7]

= questo documento

SOMMARIO

LISTA DELLE TABELLE

1 INTRODUZIONE

1.1 Ambito

Nel dicembre 2013 CONSIP ha bandito una procedura ristretta, suddivisa in quattro lotti, per l'affidamento dei "servizi di Cloud Computing, di Sicurezza, di Realizzazione di Portali e Servizi on-line e di Cooperazione Applicativa per le Pubbliche Amministrazioni - (ID SIGEF 1403)" nota come Gara SPC Cloud. Il Lotto 2, inerente i Servizi di Identità Digitale e Sicurezza Applicativa, è stato assegnato al Raggruppamento la cui mandataria è Leonardo S.p.A. e le società mandanti sono IBM, Sistemi Informativi e Fastweb.

La durata del contratto è di cinque anni. Nell'arco di tale periodo ogni Pubblica Amministrazione potrà acquisire i servizi offerti dalle "Convenzioni" tramite la stipula di "Contratti Esecutivi" dimensionati tecnicamente in un Piano dei fabbisogni prodotto in base alle proprie esigenze.

In virtù dell'Addendum nr. 4 al Contratto Quadro DA.[1] sottoscritto tra CONSIP ed il RTI in data 26/3/2021 il Contratto Quadro è stato prorogato di ulteriori 12 (dodici) mesi sino alla scadenza al 20 luglio 2022.

Infine in virtù del DL 17 maggio 2022, n. 50 (GU Serie Generale n.114 del 17-05-2022) Art. 31-bis (Proroga di accordi quadro e convenzioni delle centrali di committenza in ambito digitale) il Contratto Quadro è stato prorogato fino al 31 dicembre 2022.

Il presente documento costituisce il progetto dei fabbisogni che comprende l'insieme di servizi e di infrastrutture tecnologiche dedicate alla sicurezza dei sistemi informativi preposti al trattamento dei dati della Pubblica Amministrazione (PA), in conformità alle esigenze dell'Amministrazione stessa espresse attraverso il proprio piano di fabbisogni. Esso raccoglie e dettaglia le richieste dell'Azienda Ospedaliera San Giovanni (indicata nel documento come Amministrazione contraente) contenute nel proprio Piano dei fabbisogni [DA-5] e descritte sinteticamente in §1.2. Successivamente si formula una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" e nei relativi allegati.

1.2 Richieste dell'Amministrazione contraente

In questa sezione del Progetto dei fabbisogni l'RTI intende raccogliere e dettagliare le richieste dell'Amministrazione contraente espresse tramite la redazione del Piano dei fabbisogni [DA-5] e da incontri successivi in cui meglio si sono definite le esigenze.

2 RIFERIMENTI

2.1 Documenti Applicabili

Tabella 1: Documenti applicabili.

Rif.	Codice	Titolo
DA-1.	--	Capitolato Tecnico – Parte Generale "Procedura ristretta, suddivisa in 4 lotti, per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)"
DA-2.	--	Capitolato Tecnico – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)"
DA-3.	--	Offerta Tecnica – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)" del 22 Dicembre 2014
DA-4.	--	Contratto Quadro – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)" del 20/07/2016
DA-5.		"Piano dei Fabbisogni" – *AO San Giovanni* del 24/07/2021 Prot. N. 25675/2022
DA-6.		Allegato 1 – Listino prezzi - http://www.spc-lotto2-sicurezza.it/
DA-7.	EP4A56001Q01	Piano di Qualità Generale – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)"
DA-8.		Capitolato Tecnico – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)" – Appendice 3 – Capitolato Tecnico Servizio di Monitoraggio
DA-9.		Offerta Tecnica – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)" del 22 Dicembre 2014 - Appendice

2.2 Documenti di Riferimento

Tabella 2: Documenti di riferimento.

Rif.	Codice	Titolo
DR-1.		Guida al Contratto Quadro "Servizi di gestione delle identità digitali e sicurezza applicativa" - http://www.spc-lotto2-sicurezza.it/
DR-2.		Allegato 3 – Schema Progetto dei fabbisogni - http://www.spc-lotto2-sicurezza.it/

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

La seguente Tabella 3riporta tutte le definizioni adottate nel presente documento.

Tabella 3: Definizioni valide per il presente documento.

Amministrazioni	Pubbliche Amministrazioni.
Amministrazione aggiudicatrice	Consip.
Amministrazione/i Contraente/i	Pubbliche Amministrazioni che hanno siglato un Contratto di Fornitura con il Fornitore per l'erogazione di uno dei servizi in ambito dell'Accordo Quadro.
Fornitore	Vedi Raggruppamento
Modalità "As a Service"	Servizio erogato da remoto attraverso i Centri Servizi dell'RTI.
Modalità "On premise"	Servizio erogato presso le strutture dell'Amministrazione contraente o altre strutture indicate dalla stessa.
Raggruppamento	Raggruppamento Temporaneo di Impresa Leonardo S.p.A. - Cyber & Security Solutions division (nel seguito Leonardo), società mandataria, IBM S.p.A. (mandante), Sistemi Informativi srl (mandante) e Fastweb S.p.A. (mandante).

3.2 Acronimi

La seguente Tabella 4 riporta tutte le abbreviazioni e gli acronimi utilizzati nel presente documento.

Tabella 4: Lista degli acronimi.

ACL	Access Control List
AgID	Agenzia per Italia Digitale
API	Application Programming Interface
BI	Business Intelligence
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale
CE	Contratto Esecutivo
CED	Centro Elaborazione Dati
CQ	Contratto Quadro
CRL	Certificate Revocation List
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Testing
DLP	Data Loss Prevention
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System

HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IAM	Identity & Access Management
LDAP	Lightweight Directory Access Protocol
MAST	Mobile Application Security Testing
OCSP	Online Certificate Status Protocol
PA	Pubblica Amministrazione
PC	Personal Computer
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
RFC	Request for Comments
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Imprese
RTO	Recovery Time Objective
SAL	Stato Avanzamento Lavori
SAST	Static Application Security Testing
SPC	Sistema Pubblico di Connettività
SPID	Sistema Pubblico di Identità Digitale
URL	Uniform Resource Locator
VA	Vulnerability Assessment
WS	Web Service
XML	eXtensible Markup Language

4 DATI ANAGRAFICI AMMINISTRAZIONE CONTRAENTE

Nelle seguenti tabelle si riportano i dati anagrafici dell'Amministrazione contraente (cfr. Tabella 5) e del suo referente (cfr. Tabella 6).

Tabella 5: Dati anagrafici dell'Amministrazione contraente.

Ragione sociale Amministrazione	Azienda Ospedaliera Complesso Ospedaliero San Giovanni - Addolorata
Indirizzo	Va dell'Amba Aradam, 9
CAP	00184
Comune	Roma
Provincia	Roma
Regione	Lazio
Codice Fiscale	04735061006
Codice IPA	azos_sga
Indirizzo PEC	ao.sga@pec.hsangiovanni.roma.it

Tabella 6: Dati anagrafici del referente dell'Amministrazione contraente.

Referente Amministrazione	Ing. Gabriele Rinonapoli
Ruolo	Responsabile UOSD I.C.T.
Telefono fisso	06/77055415
Indirizzo mail	grinonapoli@hsangiovanni.roma.it
PEC (SÌ/NO)	ao.sga@pec.hsangiovanni.roma.it

5 PROPOSTA TECNICO-ECONOMICA

Nel presente capitolo vengono descritti gli ambiti di offerta identificati al momento della stesura del presente Progetto dei Fabbisogni.

L'esigenza dell'amministrazione si traduce nel seguente catalogo di servizi:

Id Servizio	Titolo	Descrizione
L2.S3.10	RTSM.1	Servizi di monitoraggio della sicurezza
L2.S3.9	SP.01	Servizio Maneged Detection & Response
L2.S3.9	SP.02	Servizio di Consulenza per Adeguamento al FNSC
L2.S3.9	SP.03	Servizio Supporto per Interventi di Adeguamento

5.1 Servizi di monitoraggio L2.S3.10 (RTSM.1)

Alla luce delle crescenti minacce informatiche per le organizzazioni diviene fondamentale rivedere l'approccio alla gestione del rischio e individuare strategie per ridurre la vulnerabilità delle infrastrutture informatiche. Quindi l'individuazione preventiva e la gestione real time degli incidenti di sicurezza sono fattori di primaria importanza per garantire alle aziende un adeguato livello di protezione delle reti, dei dati e dei servizi.

In tale ottica il seguente Servizio di Monitoraggio effettua attività di monitoraggio real time, per mezzo di un SOC messo a disposizione dal RTI presidiato 24 ore su 24 per 365 giorni l'anno e composto da un team di specialisti (analisti, system engineer, security tester e malware specialist).

Per il Servizio di Monitoraggio (SOC) si utilizza una piattaforma centralizzata di Security Information and Event Management (SIEM). Tale piattaforma consiste in un sistema che associa eventi, minacce e rischi per fornire un potente sistema di intelligence per la sicurezza, risposte rapide in caso di necessità, una ininterrotta gestione dei log. La soluzione è intrinsecamente scalabile e modulare e si presenta sotto forma di appliance, con alcune componenti virtualizzabili. In questo modo è possibile far fronte fin da subito alle necessità di gestione della sicurezza informatica in uno scenario multicloud, che può evolvere nel tempo mediante la pubblicazione di servizi su altre piattaforme cloud, inizialmente non previste in fase di attivazione del servizio. L'architettura prevista si articola nelle seguenti componenti:

- *console di gestione*, la quale costituisce il livello di application e presentation installato presso il Centro Servizi ad uso del team specialistico di monitoraggio;
- *sistema di correlazione e log management*, il quale costituisce il livello di data collecting and storage installato presso il Centro Servizi;
- *sistema di raccolta log* (collettori), il quale costituisce il livello di data collecting and forwarding e che sarà installabile «on premise» previo accordo con l'Amministrazione contraente.

5.1.1 Obiettivi del servizio RTSM.1

Il servizio di monitoraggio si pone i seguenti obiettivi:

Fornire un servizio efficiente per la raccolta ed elaborazione dei log relativi al tracciamento delle attività svolte sui sistemi;

- Controllare in maniera attiva l'infrastruttura di sicurezza delle reti e dei sistemi attraverso l'attività di monitoring real-time e supervisione degli apparati di sicurezza prevenendo efficacemente gli incidenti di sicurezza;
- Contribuire al governo ed alla gestione della sicurezza dell'Amministrazione fornendo servizi di installazione, configurazione e manutenzione sia on-site che presso le proprie strutture dei sistemi hardware e software necessari per l'erogazione dei servizi di sicurezza;

- Generare allarmi e reportistica per l'auditing sugli eventi raccolti e garantire la conservazione sicura delle evidenze. I risultati di tale attività saranno resi disponibili all'Amministrazione contraente su una piattaforma condivisa al termine delle attività di triage da parte degli analisti di sicurezza.

Il servizio è stato progettato per anticipare il più possibile il verificarsi di tentativi di attacco, identificando prontamente asset o eventi potenzialmente impattanti. Il servizio fornisce un monitoraggio continuo in tempo reale e la correlazione di eventi di sicurezza sulla rete (ad es. comportamenti non autorizzati, tentativi di attacco, interruzioni di servizio) ed analisi delle anomalie e dei trend. Analisi di dettaglio ed eventuali attività di miglioramento dell'infrastruttura di sicurezza (remediation) sono in carico al cliente.

5.1.2 Architettura di erogazione del Servizio RTSM.1

La soluzione si articola nelle seguenti componenti:

- presenti presso il Centro Servizi del RTI:
  - console di gestione, la quale costituisce il livello di application e presentation installato presso il Centro Servizi del RTI ad uso esclusivo del team specialistico di monitoraggio. In ogni caso l'RTI mette a disposizione un sistema di *ticketing* sviluppato internamente, denominato NGS (Next Generation SOC), sul quale il cliente potrà verificare lo stato degli *incident* ed avere informazioni sugli stessi;
  - sistema di correlazione e log management, il quale costituisce il livello di *data collecting and storage* installato presso il Centro Servizi del RTI;
- presenti presso l'Amministrazione contraente:
  - sistema di raccolta log (collettori), il quale costituisce il livello di *data collecting and forwarding* installato «on premise» su infrastrutture dell'Amministrazione contraente.

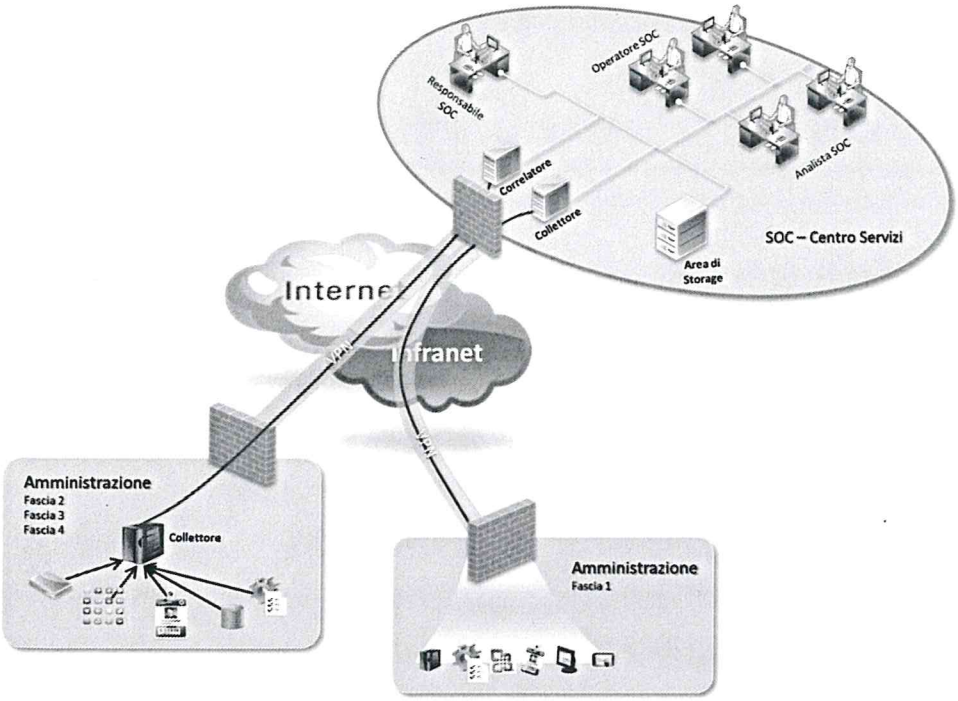


Figura 1: Architettura di riferimento del Servizio di Monitoraggio

Il sistema di *ticketing* visibile all'Amministrazione mostrerà una sezione di Incident handling secondo quanto di seguito rappresentato:

- Sezione Incident Handling dove vengono visualizzati
  - Incident reali (analizzati)
  - Falsi positivi (analizzati)

- Azioni in carico al cliente su allarmi notificati

All'interno delle segnalazioni vengono allegate le schede incidente in formato PDF

Operativamente gli eventi vengono raccolti «on premise» da un collettore VLC (Virtual Log Collector) che integra anche la funzione di *caching dei LOG ricevuti*. Limitatamente all'istanza virtualizzata VLC l'installazione e la manutenzione sono a carico dell'Amministrazione, con il supporto dell'RTI. In caso di indisponibilità della connettività verso la console di gestione centrale, il virtual *collector* è in grado di *mantenere* i LOG in modo da evitarne la perdita definitiva.

La raccolta degli eventi tipicamente avviene in modalità *agentless* e prima di effettuare qualunque elaborazione dei log, il collettore li firma digitalmente, li comprime, ne effettua un hash e li invia verso l'infrastruttura del Centro Servizi dell'RTI, che ha il compito di mantenere i file di log in formato raw inalterati per il tempo di *retention* specificato, che può essere diverso e configurato ad hoc a seconda dei casi da gestire, o più precisamente a seconda delle normative a cui rispondere. La piattaforma effettua l'archiviazione dei log *raw* sullo *storage*. In seguito i log vengono analizzati localmente, normalizzati, indicizzati ed inviati alla piattaforma di analisi. È possibile effettuare copie dei dati indicando una frequenza limite (ad es. una volta al mese) e utilizzando supporti messi a disposizione dal cliente via VPN.

Nel fare questo, i log vengono anche aggregati: questa fase consente di raggruppare più eventi uguali tra loro verificatisi in un intervallo di tempo prefissato, in modo da ridurre lo spazio occupato da essi all'interno del database. Come conseguenza dell'operazione di aggregazione, nel database saranno conservate le seguenti informazioni: time-stamp del primo evento aggregato, numero complessivo di eventi verificatisi nell'intervallo di aggregazione, time-stamp e dati contenuti nell'ultimo evento aggregato. Si ribadisce che le elaborazioni effettuate dal collettore sui log sono successive al loro processing (firma digitale, compressione ed hashing) per l'invio ai successivi moduli che devono mantenere i raw log «originali ed inalterabili nel tempo».

5.1.3 Descrizione del servizio RTSM.1

Il servizi di monitoraggio in ambito di sicurezza informatica sono erogati in modalità «as a service» dal SOC dislocato all'interno del Centro Servizi e includono il monitoraggio, la correlazione, la classificazione e l'analisi, nonché la notifica degli eventi di sicurezza relativi all'infrastruttura dell'Amministrazione contraente. Le componenti di servizio sono:

- monitoring & alerting;
- reporting;
- log management.

5.1.3.1 Monitoring & Alerting

L'elemento di servizio ***monitoring & alerting*** – erogato in modalità H24, per 365 giorni all'anno – prevede:

- *Identificazione*, ossia la fase in cui un attacco o una presunta violazione viene individuata. In particolare, gli eventi rilevati dai dispositivi di sicurezza (firewall, IDS, antivirus ecc.) sono analizzati al fine di determinare, attraverso la correlazione, se si è effettivamente in presenza di potenziali eventi anomali ed incidenti di sicurezza.
- *Classificazione* degli incidenti in cui viene determinato il livello di severità (conformemente a quanto definito nel Lotto 2 della Gara SPC) e l'impatto del potenziale incidente qualora siano stati forniti in fase di Information Gathering da parte dell'Amministrazione la valorizzazione degli Asset. I parametri considerati comprendono la tipologia/categoria di attacco (ad esempio DoS, malicious code, misuse, ecc.) e la valutazione delle criticità che riguardano i target coinvolti.
- *Notifica* di eventuali incidenti e altre anomalie. Stabilita la tassonomia dell'anomalia viene comunicato alle opportune strutture lo stato di allarme (con le informazioni necessarie a qualificarlo) affinché si attivi il processo vero e proprio di contrasto degli incidenti (incident response).

5.1.3.2 Reporting

È prevista, a seguito della rilevazione di un incidente classificato come reale, l'invio di un *technical report* che contenga tutte le informazioni utili risultanti dall'analisi dell'evento e una descrizione ad alto livello di una *remediation* applicabile.

5.1.3.3 Log Management

L'elemento di servizio *log management* prevede:

- la raccolta dei dati registrati nei log dei dispositivi controllati (cfr. § 5.1.4);
- la conservazione dei file di log nel formato RAW;
- la conservazione dei log relativi ad eventi correlati in modo da preservarne la disponibilità e l'integrità, in accordo ai requisiti imposti dal testo unico sulla privacy e successive modificazioni;
- la conservazione dei dati delle Amministrazioni contraenti per almeno 180 giorni, con conseguente applicazione delle politiche di rotazione e cancellazione sicura dei dati anteriori al periodo definito;
- l'attività di gestione della piattaforma (configuration & change management, fault management);
- un insieme standard di report.

E' possibile effettuare copie dei dati indicando una frequenza limite (ad es. una volta al mese) e utilizzando supporti messi a disposizione dal cliente via VPN. Le estrazioni non sono soggette a SLA.

5.1.4 Vincoli e assunzioni del servizio RTSM.1

Affinché l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Per l'erogazione delle attività del servizio è necessaria quindi anche la creazione di una VPN tra il Centro Servizi del Fornitore e l'Amministrazione Contraente, in mancanza della quale potrebbero non essere erogate alcune attività specifiche.

La configurazione oggetto dei servizi di monitoraggio fa riferimento al perimetro dell'Amministrazione contraente. Il dimensionamento dell'architettura utilizzata sarà in grado di gestire fino a 2000 EPS di picco o 125 Device Equivalenti. In caso di ampliamento del perimetro/sistemi oggetto di servizio SM è necessario prevedere un adeguamento dell'offerta economica al fine di coprire gli EPS aggiuntivi. Il SOC è in grado di operare una verifica giornaliera della media EPS del cliente.

Il RTI garantisce esclusivamente l'accesso ad un sistema di ticketing (NGS) sviluppato internamente sul quale il cliente potrà verificare lo stato degli incident ed avere informazioni sugli stessi.

In relazione all'integrazione dei datasource, il protocollo/formato preferibile è syslog/CEF per tutte le log source. Qualora questo non sia utilizzabile (vedi sistemi Windows) si renderanno necessarie alternative quali la configurazione di WinRM oppure l'installazione di un agent indipendente (come Snare in versione free ad esempio) oppure di un agent dedicato dipendente dal SIEM (alcuni esempi: RSA NetWitness Endpoint Insights, Splunk Universal forwarder). Non sono previste integrazioni di sorgenti e/o servizi che non sono nativamente supportati dal sistema SIEM in termini di connettori

5.1.5 Componenti del servizio RTSM.1 da installare presso l'Amministrazione contraente

Il servizio prevede il deployment della componente di raccolta dei log (collettore) deputato alle funzioni di *data collecting and forwarding* «on premise» c/o l'Amministrazione contraente.

Ciò è infatti necessario al fine di veicolare verso il SIEM gli eventi di sicurezza che provengono dal data centre del cliente. Sarà dunque predisposto un *virtual log collector* (VLC), in formato di *virtual appliance*, che collezionerà e inoltrerà i log provenienti dalle sorgenti verso il SIEM. I log e il contenuto descrittivo verranno archiviati in formato di metadati a servizio delle attività di investigazione e di *reporting*.

La predisposizione delle risorse virtuali necessarie all'implementazione del VLC è a carico dell'Amministrazione; il VLC dovrà essere ospitato presso il *data centre* del cliente (o in alternativa su un server fisico, sempre presso i CED dell'Amministrazione) e disporre delle risorse qui di seguito elencate in tabella. E' esclusa la fornitura di risorse HW da parte del RTI.

Contestualmente si cercherà di mantenere inalterata l'attuale erogazione di servizio di monitoraggio esistente, fino a completamento dell'attivazione del presente SM.1 che avverrà entro max 60 gg dalla data disponibilità perimetro di monitoraggio. (come da riferimento Appendice **Errore. L'origine riferimento non è stata trovata.**)

Tabella 1: Requisiti per il VLC presso il data centre del cliente

nr. CPU	Specifiche CPU	RAM	Memoria di massa
8	Intel Xeon CPU @ 2.00 GHz	8 GB	150 GB

5.1.6 Modalità di erogazione del servizio RTSM.1

Il servizio sarà erogato in modalità «as a service», come previsto da capitolato tecnico e relativa proposta tecnica.

Di seguito viene riportata una tabella relativa alle finestre di servizio.

Tabella 2: Finestre di servizi

Attività	Disponibilità
Help Desk (telefonico)	9:00–18:00 dal lunedì al venerdì (escluso festività nazionali)
Help Desk (telematico)	H24
Monitoraggio di sicurezza delle piattaforme	H24
Monitoraggio di disponibilità delle piattaforme	H24

5.1.7 Quantità e prezzi del servizio RTSM.1

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

5.1.8 Attivazione del servizio RTSM.1

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1.

5.2 Servizi professionali

In questa sezione si descrivono le attività richieste dall'Amministrazione contraente e svolte come servizi professionali. In tale ambito il fornitore s'impegna a erogare tutti i servizi descritti nel presente documento

e assicura la disponibilità delle risorse indicate per supportare l'Amministrazione contraente alla loro erogazione.

Nei successivi paragrafi si fornisce l'elenco delle attività e le relative descrizioni per ciascuno dei servizi professionali richiesti.

5.2.1 SP.01 - Servizio Managed Detection & Response

Nel presente paragrafo è descritto il servizio professionale di supporto alle attività definite nel servizio MDR e di seguito rappresentate:

- Ridurre al minimo le possibili finestre d'esposizione a eventuali attacchi informatici per gli endpoint in perimetro
- Remediation automatica per gli incident riconosciuti come "veri positivi" ed a criticità massima
- Endpoint protetti anche in assenza momentanea di connessione ad internet
- Possibilità di isolare dalla rete un endpoint compromesso conservandone il controllo dalla piattaforma in cloud
- Protezione in tempo reale dagli attacchi conosciuti e non che utilizzano metodologie e/o indicatori noti;

5.2.1.1 Descrizione del Servizio SP.01

Il servizio MDR è erogato in completo outsourcing dal SOC di Leonardo ed include le licenze e la gestione di una degli Endpoint, la cui distribuzione ed installazione tuttavia rimane a carico del cliente. La gestione viene fatta attraverso una piattaforma centrale presente su cloud, che raccoglie tutte le informazioni di telemetria (metadati) inoltrate dagli agent installati sugli endpoint dell'Amministrazione. Per la corretta erogazione del servizio è necessaria la visibilità continuativa tra agent e piattaforma di management tramite una connettività con Internet messa a disposizione dall'Amministrazione, sulla quale comunque le informazioni transiteranno in modo cifrato secondo i più elevati standard di sicurezza.

Il servizio sarà erogato as a service col monitoraggio continuativo nella finestra di servizio H24 per 365 giorni con notifica degli eventi ritenuti di interesse per l'Amministrazione attraverso il portale di Leonardo NGS che garantisce discrezionalità nelle comunicazioni e negli accessi, nonché le capacità di reportistica e dashboarding in merito alle statistiche generali del servizio.

5.2.1.2 Vincoli e assunzioni del Servizio SP.01

Affinchè l'Amministrazione contraente possa usufruire del servizio è necessario che sia interconnessa direttamente alla rete del Sistema Pubblico di Connettività (SPC) — o altre strutture equivalenti individuate da Consip S.p.A. e/o dell'Agenzia per l'Italia Digitale (AgID) — attraverso uno o più Fornitori di connettività, o attraverso Enti autorizzati, in modo tale che il traffico tra il Centro Servizi e l'Amministrazione contraente avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Per l'erogazione delle attività del servizio è necessaria quindi anche la creazione di una VPN tra il Centro Servizi del Fornitore e l'Amministrazione Contraente, in mancanza della quale potrebbero non essere erogate alcune attività specifiche.

Il servizio prevede l'installazione agent software a livello Endpoint, la cui distribuzione ed installazione è a carico dell'Amministrazione.

5.2.1.3 Modalità di erogazione del Servizio SP.01

Il servizio sarà erogato in modalità as a service dal centro servizi del fornitore.

5.2.1.4 Quantità e prezzi del Servizio SP.01

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5].

L' RTI si impegna a erogare tutti i Servizi descritti nella presente offerta e la disponibilità delle risorse per supportare l'Amministrazione contraente per gli scopi sopra dichiarati.

Si rende noto che non sono previsti e definiti specifici livelli minimi di servizio da garantire e/o meccanismi di penalizzazione da applicare al fornitore, salvo quanto disciplinato in materia di responsabilità contrattuale dalla vigente normativa.

Coerentemente a quanto previsto nel succitato Contratto si precisa che la modalità di remunerazione di tali servizi è "a canone".

La valorizzazione dell'effort dell'item di progetto è nel seguito riepilogata in Appendice A.

La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente al piano lavori e verrà riconosciuta bimestralmente come previsto nell'**Allegato 4B - Schema Contratto Esecutivo - Lotto 2.**

5.2.1.5 Attivazione del Servizio SP.01

Si prevede l'avvio del servizio secondo i tempi definiti nell'A.3.1.

5.2.1.6 Deliverable del servizio SP.01

Come deliverable del servizio è previsto il rilascio di un documento:

- Documento riassuntivo di alto livello che riassume le informazioni raccolte sui sistemi presenti nel perimetro di analisi;
- Report di dettaglio, in caso di rilevazione di eventi ritenuti di interesse.

5.2.2 Servizio di Consulting - Assessment Framework Nazionale Cyber Security (FNSC) - SP.02

L'esigenza dell'Amministrazione è quella di avvalersi di servizi professionali finalizzati alla fornitura del supporto specialistico per lo svolgimento di un assessment, basato su Framework Nazionale Cyber Security, in modo da:

- indicare il grado di adeguamento dell'Amministrazione ai livelli standard di sicurezza;
- individuare le possibili azioni correttive e soluzioni rispetto agli standard vigenti nell'organizzazione.

5.2.2.1 Descrizione del servizio SP.02

Il presente servizio è finalizzato ad eseguire un'assessment per indicare la copertura e maturità dei controlli di sicurezza inerenti i seguenti ambiti:

- Governance, che indirizza l'insieme delle pratiche volte a definire le politiche e l'organizzazione necessarie per poter reagire e prevenire, in maniera efficace, alle minacce di sicurezza, in modo da minimizzare l'impatto di possibili danni alle finalità istituzionali dell'Amministrazione dovuti ad incidenti di sicurezza di natura informatica.
- Prevent, che esprime la capacità di attuare pratiche e misure di sicurezza per la protezione delle informazioni, delle infrastrutture e dei servizi digitali presso l'Amministrazione.
- Detect, che esprime la capacità di individuare tempestivamente potenziali violazioni o eventi che possono influenzare o compromettere la sicurezza dell'Amministrazione.

- Respond & Recovery, che esprime la capacità di rispondere efficacemente ad un incidente di sicurezza e possibilmente di ripristinare i servizi impattati dallo stesso.

Nella definizione dei suddetti controlli si prenderanno in considerazione i requisiti previsti dal Framework Nazionale sulla Cyber Security (FNCS) e dalla normativa europea sul General Data Protection Regulation (GDPR).

La Figura contiene una rappresentazione grafica dell'attività progettuale che sarà condotta per l'Amministrazione e si svilupperà nelle seguenti fasi:

- **Avvio del progetto e pianificazione**: In avvio di progetto si procederà alla composizione di un gruppo di lavoro misto formato da personale specialistico dell'RTI e personale dell'Amministrazione, al fine di individuare le figure da coinvolgere nell'esecuzione dell'assessment e procedere ad una pianificazione di dettaglio (fasi 1 e 2). Dette figure dovranno essere in grado di fornire informazioni in ordine allo stato di implementazione dei controlli di sicurezza presi in considerazione e che potranno essere di tipo logico, fisico e organizzativo.
- **Esecuzione dell'assessment:** La presente attività consiste nella raccolta delle informazioni rilevate mediante gli incontri con i responsabili e all'analisi della documentazione ottenuta (fase 3).
- **Elaborazione dei risultati dell'assessment**: A seguito degli incontri/interviste verranno analizzati, gestiti ed elaborati i dati acquisiti, che avranno particolarmente valore e qualità, in quanto aggiornati allo stato dell'arte. Tutte le informazioni acquisite saranno riportate in un documento, che conterrà i risultati dell'assessment e che sarà condiviso con i referenti dell'Amministrazione (fasi 4 e 5).

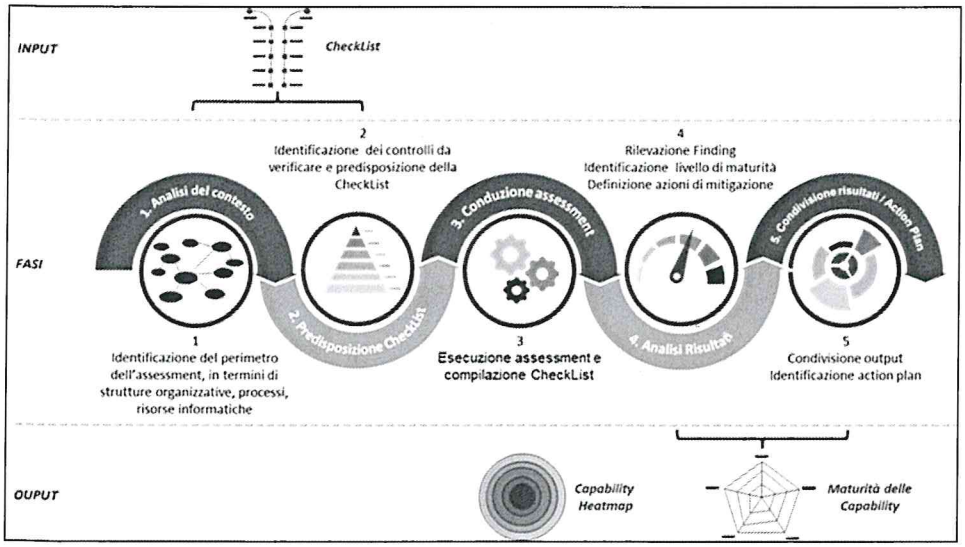


Figura 1: Diagramma di sintesi delle fasi progettuali per l'assessment sui processi di sicurezza

5.2.2.2 Vincoli e assunzioni del servizio SP.02

Il perimetro delle attività descritte è da intendersi limitato alle attività del presidio di sicurezza ICT operativo presso il cliente Azienda Ospedaliera San Giovanni.

5.2.2.3 Modalità di erogazione del servizio SP.02

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2"

5.2.2.4 Quantità e prezzi del servizio SP.02

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, calcolati secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni.

5.2.2.5 Attivazione del servizio SP.02

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

5.2.2.6 Deliverable del servizio SP.02

Come deliverable del servizio è previsto il rilascio di un documento che conterrà i risultati dell'assessment e che sarà condiviso con i referenti dell'Amministrazione. Verrà prodotta inoltre una presentazione di sintesi sulle attività svolte.

5.2.3 Servizio Supporto per Interventi di Adeguamento (SP.03)

Al fine di soddisfare le richieste dell'Amministrazione, il RTI predispone un basket di giornate da utilizzare a consumo per implementare eventuali interventi di adeguamento risultanti in seguito alle analisi svolte durante il task di consulenza.

5.2.3.1 Modalità di erogazione del servizio SP.03

Coerentemente a quanto previsto nel Contratto per i servizi professionali (rif. Capitolato Tecnico [DA-2] par. 1.3.9 Servizio L2.S3.9 – Servizi professionali, pagg. 48–49), si precisa che la modalità di remunerazione di tali servizi è "a task". Per gli SLA, dove applicabili, si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2"

5.2.3.2 Quantità e prezzi del servizio SP.02

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati in Appendice A, calcolati secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni.

5.2.3.3 Attivazione del servizio SP.03

Si prevede l'avvio del servizio secondo i tempi definiti nell'Appendice B.

5.2.3.4 Deliverable del servizio SP.02

Nella fase di attivazione del task relativo agli interventi, saranno definiti in accordo con l'Amministrazione sia l'effort necessario che l'eventuale predisposizione di un deliverable specifico..

6 RISERVATEZZA

Per l'erogazione della fornitura, il Fornitore non ha necessità trattare e/o accedere a informazioni o materiale classificato ma è comunque tenuto alla sicurezza e alla riservatezza dei dati e della documentazione di cui viene a conoscenza.

APPENDICE A PROGETTO DI ATTUAZIONE

A.1 Struttura organizzativa

La struttura organizzativa completa è descritta nella proposta tecnica (cfr. documento [DA-3]).

Le figure professionali coinvolte nella gestione e conduzione dei servizi oggetto del presente Progetto dei fabbisogni per lo specifico contratto esecutivo sono riassunte nella seguente Tabella 7.

Tabella 7: Figure professionali.

Ruolo	Caratteristiche e responsabilità
Responsabile Contratto Quadro	È il rappresentante del fornitore verso Agid/Consip, garantisce l'omogeneità e l'uniformità di interfaccia verso le parti interessate a livello di Governo del Contratto Quadro vigilando sull'osservanza di tutte le indicazioni operative, di indirizzo e di controllo, che a tal scopo potranno essere predisposte da Consip e/o da AgID, per quanto di rispettiva competenza. Rappresenta, insieme al Responsabile del Centro Servizi, il RTI nel Comitato di Direzione Tecnica.
Responsabile Contratto Esecutivo	Costituisce l'interfaccia unica verso il Responsabile del Procedimento dell'Amministrazione Beneficiaria. È responsabile dell'erogazione dei servizi acquistati dall'Amministrazione e della rendicontazione e dei meeting di stato avanzamento lavori. Costituisce l'interfaccia unica verso il Responsabile Unico del Procedimento dell'Amministrazione beneficiaria.
Responsabile Tecnico	È il Responsabile unico delle attività tecniche e del raggiungimento degli obiettivi dei servizi oggetto del Contratto. Costituisce l'interfaccia unica verso il Direttore Esecuzione nominato dall'Amministrazione. Ha la visione complessiva e integrata di tutte le attività tecniche legate all'attivazione, all'erogazione e al rilascio dei servizi della fornitura e ne garantisce la qualità.
Responsabile del Centro Servizi	È responsabile del Centro servizi da cui vengono erogati i servizi nella modalità "as a service".
Responsabile Servizi 'on premise'	Coincide con il Responsabile Tecnico
HELP DESK	Primo punto di contatto a disposizione dell'Amministrazione per l'avvio delle attività di acquisizione del servizio. Supporta inoltre i referenti dell'Amministrazione contraente nelle attività di risoluzione di eventuali problematiche di utilizzo del servizio. L'Help Desk è contattabile: - per contatti di natura commerciale e informativa al numero verde 800 894 590. - per contatti di natura tecnica e di problemi di utilizzo del servizio al seguente indirizzo e-mail **sccd@spc-lotto2-sicurezza.it** Ulteriori informazioni sono reperibili al seguente URL: http://www.spc-lotto2-sicurezza.it presso il quale è presente il Portale di Governo e Gestione della Fornitura.

I nominativi delle figure presenti nella tabella soprastante saranno forniti all'Amministrazione entro 10 giorni dalla stipula del contratto.

A.2 Specifiche di collaudo

N.A.

A.3 Quantità e costi

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati di seguito nelle Tabelle successive, secondo le esigenze espresse dall'Amministrazione contraente nel proprio Piano dei fabbisogni [DA-5]. I prezzi tengono conto di quanto riportato nel listino prezzi SPC lotto 2 [DA-6]. In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5].

A.3.1 Riepilogo Economico

Servizio L2.S3.10 - Servizio di Monitoraggio (5 mesi remoto H24x7)		Valore max	2022		
Metrica	Fascia	Prezzo unitario	Nun.tà	Mesi	Prezzo
Device/anno	Fascia 1 50 Device (max 300 eps)	€ 313,82	0	0	€ 0,00
	Fascia 2 100 Device (max 700 eps)	€ 564,85	0	0	€ 0,00
	Fascia 3 200 Device (max 1.600 eps)	€ 544,30	0	0	€ 0,00
	Fascia 4 500 Device (max 5.000 eps)	€ 508,10	200	5	€ 42.341,67
	Fascia 5 oltre 500 Device (oltre 5.000 eps)	€ 470,00	0	0	€ 0,00
TOTALE					€ 42.341,67

Servizio L2.S3.9 - Servizi professionali Servizio Maneged Detection & Response			Valore max	2022	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo
giorno/uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	9	€ 2.700,00
		Security Architect	€ 372,90	73	€ 27.221,70
		Specialista di tecnologia/prodotto Senior	€ 295,00	0	€ 0,00
		Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00
giorno/uomo	Orario continuativo H24	Specialista di tecnologia/prodotto Senior	€ 1.180,00	0	€ 0,00
		Specialista di tecnologia/prodotto	€ 930,00	0	€ 0,00
TOTALE					€ 29.921,70

Servizio L2.S3.9 - Consulenza in ambito FNCS				2022	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo
giorno/uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	8	€ 2.400,00
		Security Architect	€ 372,90	75	€ 27.967,50
		Specialista di tecnologia/prodotto Senior	€ 295,00	0	€ 0,00
		Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00
giorno/uomo	Orario continuativo H24	Specialista di tecnologia/prodotto Senior H24	€ 1.180,00	0	€ 0,00
		Specialista di tecnologia/prodotto H24	€ 930,00	0	€ 0,00
TOTALE					€ 30.367,50

Servizio L2.S3.9 - Servizi a consumo - SP.4				2022	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo
giorno/uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	4	€ 1.200,00
		Security Architect	€ 372,90	25	€ 9.322,50
		Specialista di tecnologia/prodotto Senior	€ 295,00	0	€ 0,00
		Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00
giorno/uomo	Orario continuativo H24	Specialista di tecnologia/prodotto Senior H24	€ 1.180,00	0	€ 0,00
		Specialista di tecnologia/prodotto H24	€ 930,00	0	€ 0,00
TOTALE					€ 10.522,50

Il valore totale dell'iniziativa è pari a 113.153,37 € (IVA esclusa).

A.3.2 Fatturazione L2.S3.9

A valle delle verifiche dell'Amministrazione (art 15 dell'Accordo Quadro), i servizi professionali L2.S3.9 saranno fatturati bimestralmente (art.19 dell'Accordo Quadro), in ragione dei servizi effettivamente prestati nel rispetto del Progetto dei Fabbisogni, ovvero secondo lo stato di avanzamento dei lavori, e nelle misure che si concorderanno ad inizio delle attività o nel piano di lavoro.

APPENDICE B PIANO DI LAVORO

In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5] la tabella riporta la pianificazione per i servizi contenuti all'interno del presente documento.

ID	Nome attività	Inizio	Fine	Vincoli
RTSM.1	Servizi di monitoraggio della sicurezza	T0	31 Dicembre 2022	-
SP.01	Servizio Maneged Detection & Response	T0	31 Dicembre 2022	-
SP.02	Servizio di Consulenza per Adeguamento al FNSC	T0	31 Dicembre 2022	-
SP.03	Servizio Supporto per Interventi di Adeguamento	T0	31 Dicembre 2022	-

PROVVEDIMENTO DEL DIRETTORE GENERALE

N. PROPOSTA DEL	799 DEL 05.08.2022
N. DELIBERAZIONE DEL	**740 DEL 09.08.2022**

Il dott. Pasquale Ferrari, Direttore *pro tempore* della U.O.C. Economico Finanziaria e Patrimoniale, ha formale delega di funzioni vicarie di Direttore Amministrativo Aziendale da svolgersi nei periodi di astensione delle funzioni del titolare, giusta deliberazione 494/DG del 25 maggio 2022, pertanto sottoscrive il presente provvedimento in ragione della funzione svolta.

La dott.ssa Patrizia Magrini, Direttore Sanitario Aziendale *pro tempore*, ha formale delega di funzioni vicarie di Direttore Generale da svolgersi nei periodi di astensione delle funzioni del titolare, giusta deliberazione n. 494/DG del 25 maggio 2022, pertanto sottoscrive il presente provvedimento in ragione della funzione svolta.

La presente Deliberazione viene pubblicata per esteso nell'Albo Pretorio on-line Aziendale in data **10.08.2022** ai sensi dell'art. 31 L.R. Lazio 45/1996, come previsto dall'art. 32 L. 69/2009 e dall'art. 12 L.R. Lazio 1/2011.

Il Direttore della U.O.C. Affari Generali e
gestione amministrativa ALPI o
Funzionario incaricato