LDO/CYS/P/0011187/21
11 marzo 2021

Identificativo: PRO_GOVM_170241_IOC Rev. 6

Data: 10/03/2021

Agenzia per l'Italia Digitale

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

CIG 7550544A03

Progetto dei fabbisogni

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo SpA Divisione Cyber Security

IBM SpA

Sistemi Informativi srl

Fastweb SpA

	Nome e Ruolo	Firma
Autore		
	Maurizio Gatti	
Verifica		
	Germano Matteuzzi	
Approvazione		
	Giuseppe Nicastro	
Autorizzazione		
	Claudio Rando	

Approvazioni Aggiuntive

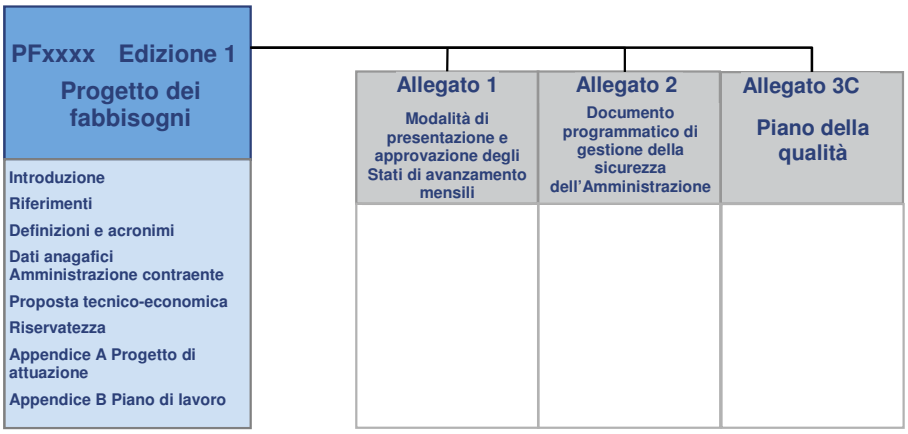
Azienda	Nome e Ruolo	Firma

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
1	19/02/2018	Amministrazione contraente	RTI
2	27/04/2018	Amministrazione contraente	RTI
3	01/06/2018	Amministrazione contraente	RTI
4	18/07/2018	Amministrazione contraente	RTI
5	01/02/2021	Amministrazione contraente	RTI

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
1	19/02/2018	Prima edizione	RTI
2	27/04/2018	Progetto dei fabbisogni per i soli servizi professionali L2.S3.9 identificati come A, B, C, F (oltre al servizio a listino L2.S3.7)	RTI
3	01/06/2018	Compilazione della sezione 4 con i dati anagrafici dell'amministrazione contraente	RTI
4	18/07/2018	Aggiornamento tabelle in appendice A.4 e del piano di lavoro in appendice Appendice B	RTI
5	01/02/2021	Rimodulazione Progetto a fronte richiesta AgID - Prot. Uscita N.0016080 del 15/12/2020	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'lenco 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 deliverables 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).
Allegato2, Documento programmatico di gestione della sicurezza dell'Amministrazione	Da consegnarsi su richiesta dell'Amministrazione
Allegato 3, Piano della qualità	Documento che descrive in maniera dettagliata gli obiettivi di qualità relativi al servizio erogato, mentre dà una descrizione sintetica dei processi di controllo della qualità.

= 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.

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'Agenzia per l'Italia Digitale - AgID (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

Il presente *Progetto dei Fabbisogni* costituisce il documento tecnico economico in cui il fornitore (RTI) descrive le modalità e i tempi delle fasi di acquisizione, configurazione e gestione (erogazione) dei servizi proposti.

Tale documento è in risposta al documento *Piano dei Fabbisogni* (cfr. doc [DA-5]), in cui l'Amministrazione contraente ha espresso le proprie esigenze ed elencato, in termini di servizio e quantità, i propri fabbisogni.

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 (IS 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 (IS 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 – "AgID progetto CERT-PA", Agenzia per l'Italia Digitale del 22/05/2018 e rimodulazione del 15/12/2020 (prot. AgID N.0016080)
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)"

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.
CERT di prossimità	Costituisce la rete di tutti i CERT «vicini» alle Amministrazioni sia in senso geografico (CERT regionali) sia in senso funzionale (CERT settoriali) e che operano secondo un modello organizzativo comune.
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 Divisione Sistemi per la Sicurezza e le Informazioni S.p.A. (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
CE	Contratto Esecutivo
CERT-PA	Computer Emergency Response Team Pubblica Amministrazione
CQ	Contratto Quadro
DNS	Domain Name System
GPG	GNU Privacy Guard
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IDS	Intrusion Detection System

IOC	Indicator of compromise
IPS	Intrusion Prevention System
MVC	Model-View-Controller
NAT	Network Address Translation
NGFW	Next Generation Firewall
NVD	National Vulnerability Database
ODBC	Open DataBase Connectivity
PA	Pubblica Amministrazione
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
RDBMS	Relational Database Management System
REST	REpresentational State Transfer
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Imprese
RTO	Recovery Time Objective
SAL	Stato Avanzamento Lavori
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SOC	Security Operation Centre
SPC	Sistema Pubblico di Connettività
SPID	Sistema Pubblico di Identità Digitale
SQL	Structured Query Language
SSL	Secure Sockets Layer
ULS	Unità Locale di Sicurezza
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAF	Web Application Firewall
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	Agenzia per l'Italia Digitale
Indirizzo	Via Liszt 21
CAP	00144
Comune	Roma
Provincia	Roma
Regione	Lazio
Codice Fiscale	97735020584
Nominativo referente Contratto Esecutivo	Francesco Tortorelli
Indirizzo mail	protocollo@pec.agid.gov.it
PEC (SÌ/NO)	SÌ

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

Nome	Francesco
Cognome	Tortorelli
Telefono fisso	06 85264435
Indirizzo mail	tortorelli@agid.gov.it
PEC (SÌ/NO)	NO

5 PROPOSTA TECNICO-ECONOMICA

Di seguito la Tabella 7 mostra la lista dei servizi previsti nella fornitura.

Tabella 7: Elenco dei servizi offerti

Id Servizio	Titolo	Descrizione
L2.S3.7	Web application firewall / Next generation firewall management	Il servizio consente all'Amministrazione avere una visione completa e in tempo reale di tutte le attività, con funzionalità avanzate di reporting.
L2.S3.9	Servizi professionali	
SP-A	Definizione e sviluppo di una piattaforma di aggregazione dati	Nell'ambito dello sviluppo per le PP.AA. del progetto INFOSEC, servizi di progettazione e supporto allo sviluppo di una piattaforma di aggregazione di dati.
SP-B	Servizi per la piattaforma P.A. per la trasmissione automatizzata degli IoC	Servizi di progettazione per la definizione degli standard per la condivisione degli IOC e la relativa gestione dell'infrastruttura operativa.
SP-C	Adeguamento della piattaforma di infosharing riservato CERT-PA	Servizi di progettazione e sviluppo delle componenti di sicurezza della piattaforma di infosharing riservata del CERT-PA.
SP-F	Supporto al modello d'ingaggio delle Regioni per il CERT-PA	Servizio per la definizione delle linee guida da seguire nella costituzione dei CERT di prossimità e revisione della procedura di risposta agli incidenti a livello regionale.

5.1 Web Application Firewall e Next generation firewall management L2.S3.7

Il servizio L2.S3.7 di Web Application Firewall e Next Generation Firewall (WAF e NGFW) implementa una soluzione a protezione in tempo reale da tentativi di attacco o intrusione non autorizzati, atti a garantire una più efficace capacità difensiva da minacce informatiche anche particolarmente evolute.

5.1.1 Obiettivi del Servizio L2.S3.7

L'integrazione del servizio WAF e NGFW nell'infrastruttura dell'Amministrazione si pone l'obiettivo di acquisire in tempo reale una efficace capacità di ispezione del traffico di rete per l'identificazione di qualsiasi tipo di anomalia a livello applicativo, utenti e dispositivi informatici in genere. Tale percezione permette quindi una definizione granulare delle politiche di sicurezza adottate dal servizio con un conseguente innalzamento della capacità difensiva della propria struttura e delle proprie risorse di rete.

All'Amministrazione sarà garantita:

- continuità dei servizi offerti;
- aderenza alle best practice di sicurezza e alle relative compliance;
- protezione delle applicazioni web da attacchi esterni agendo da filtro del traffico di rete dello strato applicativo, superando quindi le caratteristiche dei normali intrusion detection system;
- fornitura di un reporting completo ed in tempo reale di tutte le attività di rete, applicazioni, anomalie in genere.

5.1.2 Descrizione del Servizio L2.S3.7

Il servizio prevede la modalità di erogazione centralizzata con elementi costituenti presenti presso il Centro Servizi dell'RTI relativamente alle piattaforme centrali per il management delle politiche di sicurezza e raccolta degli eventi rilevanti:

- Componente di **analisi del traffico**: dedicata all'analisi del traffico ed al reporting per la sicurezza della rete e la valutazione delle vulnerabilità;
- Componente di **gestione centrale**: deputata alle attività di configurazione del provisioning basato su policy, aggiornamenti e monitoraggio della rete. Consente la tempestiva *software distribution* mediante *caching* locale degli aggiornamenti Antivirus/IPS autenticando in modo granulare gli accessi amministrativi (con funzionalità di auditing e configuration history/versioning).

Il servizio di sicurezza Web Application Firewall e Next Generation Firewall Management è erogato secondo opportune fasce in funzione della banda di connettività SPC. È stata individuata una banda <200 Mbps, che corrisponde alla Fascia 2.

5.1.3 Vincoli e assunzioni del Servizio L2.S3.7

Affinché l'Amministrazione possa usufruire del servizio di WAF e NGFW 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 avvenga all'interno di VPN sicure e configurate per supportare destinazioni multiple. In subordine dovrà comunque avere un punto di accesso a Internet.

Affinché il suddetto servizio possa essere erogato è necessaria la raggiungibilità dei componenti del servizio dislocati presso l'Amministrazione da parte del Centro Servizi dell'RTI, con finalità prevalente di gestione e manutenzione dei costituenti funzionali (e.g., aggiornamento di release software ed eventuali *change policy*). A tal fine è prevista:

- la preparazione del sito dell'Amministrazione, cioè l'esecuzione dell'insieme delle attività propedeutiche alla messa in esercizio del servizio presso l'Amministrazione stessa;
- l'implementazione di un canale dedicato verso il Centro Servizi (cifrato e attraverso il quale viene permessa la raccolta degli allarmi). Il canale cifrato è finalizzato all'interconnessione tra il Centro Servizi e le componenti periferiche e viene utilizzato per comunicazioni di tipo bidirezionale. A titolo di esempio, su tale canale sono inviate sia le informazioni relative alle politiche di sicurezza da applicare, sia i log degli eventi rilevati dagli enforcer disposti presso l'Amministrazione.

In fase di prima installazione degli apparati di WAF e NGFW è prevista l'implementazione di configurazioni come da Baseline definita nella specifica di servizio. Ulteriori configurazioni sono da considerarsi fuori ambito e potranno essere realizzate, così come altre attività di configurazione e personalizzazione, tramite l'utilizzo di gg/uu a catalogo SPC (L2.S3.9 - Servizi professionali).

5.1.4 Componenti del Servizio L2.S3.7 da installare presso l'Amministrazione contraente

L'architettura proposta per la realizzazione del servizio non prevede il deployment di componenti presso l'Amministrazione contraente.

5.1.5 Modalità di erogazione del Servizio L2.S3.7

Il servizio sarà erogato in modalità continuativa secondo le finestre di servizio definite nella seguente Tabella 8.

Tabella 8: Finestre di servizio per L2.S3.7

Attività	Disponibilità
Help Desk (telefonico)	9:00-18:00 Lunedì – Venerdì (escluso festività)
Monitoraggio di disponibilità	H24
Monitoraggio di Sicurezza	H24

Per gli SLA applicati si fa riferimento all'Appendice 1 al Capitolato tecnico [4] "Indicatori di qualità della fornitura per il Lotto 2".

5.1.6 Quantità e prezzi del Servizio L2.S3.7

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].

5.1.7 Attivazione del Servizio L2.S3.7

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

5.2 Servizi professionali L2.S3.9

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.

Le attività potranno essere erogate a task in base ad obiettivi prefissati (deliverable e tempistiche) e potranno essere svolte sia presso la sede del cliente sia presso una delle sedi del RTI: ogni task oggetto della presente rimodulazione sarà strutturato e concordato tra RTI e AgID mediante una scheda di attivazione che riporterà le informazioni essenziali per identificare l'attività, quali, ad esempio, descrizione del contesto, deliverable, tempistiche di esecuzione, valorizzazione in termini di profili professionali impiegati e relativa valorizzazione economica. È richiesta l'effettiva presenza presso le sedi di AgID solo per il personale del fornitore che dovrà interfacciarsi direttamente con i referenti di AgID per la raccolta dei requisiti e per le riunioni relative allo stato di avanzamento dei lavori. Il resto delle attività potranno essere erogate dalla sede del fornitore o da altra sede da concordare con l'Amministrazione stessa.

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 corpo". La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito in Appendice B, alla consegna dei deliverabile concordati, previo benestare.

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

5.2.1 Definizione e sviluppo di una piattaforma di aggregazione dati (SP-A)

I servizi professionali offerti prevedono la definizione e lo sviluppo della piattaforma INFOSEC per l'aggregazione di dati. Nella piattaforma si distinguono un sito pubblico raggiungibile da Internet all'indirizzo www.infosec.cert-pa.it e un sito raggiungibile solo dalla rete interna all'indirizzo infosec.lab.

L'obiettivo della piattaforma sarà quello di erogare servizi informativi ed operativi al fine di costituire il National Vulnerability Database (NVD) italiano. L'attività sarà articolata come segue:

- Supporto all'analisi dei dizionari relativi alla costituzione dell'NVD italiano.
- Supporto allo sviluppo dei servizi online:
  - raccolta ed elaborazione di dati significativi ai fini della sicurezza cibernetica,
  - realizzazione e gestione di basi dati informative.
- Supporto allo sviluppo dei processi automatizzati per lo scambio dei dati.

- Supporto alla revisione dell'interfaccia grafica secondo le direttive AgID ed analisi delle problematiche relative all'accessibilità del portale pubblico.
- Supporto alla progettazione e realizzazione di API per l'accesso ai dati da parte di applicativi esterni.
- Reingegnerizzazione dell'architettura software complessiva al fine di ottimizzare le performance globali dell'applicazione.
- Supporto alla misurazione della qualità del codice.
- Supporto alla verifica statica e dinamica della sicurezza del software.
- Porting su RDBMS Postgres e relativo *performance tuning*.
- Porting versione framework ZEND.
- Revisione dell'architettura fisica (virtuale) al fine di ottimizzare il bilanciamento di carico e le prestazioni.
- Integrazione con servizi di Identity and access management / SPID.

Le competenze che saranno garantite al fine di poter realizzazione la piattaforma sono:

- conoscenza dei principi di sicurezza applicativa
- conoscenza delle linee guida per la produzione di codice sicuro
- ottima conoscenza del linguaggio PHP5
- conoscenza del linguaggio PHP7 (nessuna esperienza specifica richiesta)
- esperienza nell'implementazione progettuale con pattern architetturale MVC
- comprovata esperienza pluriennale nell'uso del framework PHP
- profonda conoscenza di SQL e ODBC
- esperienza di sviluppo in ambiente LAMP
- approfondita conoscenza tecnica e progettuale di HTML5, CSS3 e Javascript
- esperienza in progettazione e sviluppo di Web Services (SOAP, XML-RPC, REST)
- esperienza nell'uso dei sistemi di controllo di versione e conoscenza dei sistemi distribuiti Git e Bazaar
- esperienza con Zend Framework, a partire dalla versione 1.10
- conoscenza DBMS Oracle, MySQL, Postgres
- esperienze in progettazione di database con implementazione del modello ER
- esperienza nella progettazione e realizzazione di processi ETL.

5.2.1.1 Vincoli e assunzioni del servizio SP-A

N.A.

5.2.1.2 Modalità di erogazione del servizio SP-A

Il servizio sarà erogato in modalità *as a service* presso le sedi dell'RTI e dell'Amministrazione contraente.

5.2.1.3 Quantità e prezzi del servizio SP-A

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].

5.2.1.4 Attivazione del servizio SP-A

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

5.2.1.5 Deliverable del servizio SP-A

I deriverable saranno concordati con l'Amministrazione contraente all'avvio del servizio.

5.2.2 Servizi per la piattaforma P.A. per la trasmissione automatizzata degli IoC (SP-B)

I servizi professionali offerti sono relativi: (i) all'hosting della piattaforma **MineMeld** di Palo Alto Networks e alla sua gestione (SP-B1), che l'Amministrazione contraente utilizzerà per potenziare le proprie capacità di *information sharing* con le pubbliche amministrazioni e le strutture nazionali di Cyber Security; (ii) allo sviluppo della piattaforma di condivisione IOC (SP-B2).

Le attività previste all'interno della gestione operativa infrastrutturale per l'hosting sono:

- installazione e startup delle componenti infrastrutturali (hypervisor, sistema operativo e reverse proxy ngnix);
- manutenzione ordinaria delle stesse componenti infrastrutturali, inclusi patching, hotfix, update;
- esposizione del servizio su Internet (DNS, NAT, ecc.) e configurazione servizi di protezione perimetrale IDS/IPS;
- possibilità da parte di MineMeld (in particolare da parte dei componenti miner) di accedere a Internet, nel rispetto delle politiche di sicurezza implementate riguardo l'analisi reputazionale degli indirizzi IP in ingresso e in uscita dalla piattaforma di per la trasmissione automatizzata degli IoC;
- predisposizione di un servizio SSL VPN finalizzato:
  - all'accesso da parte dell'Amministrazione contraente all'applicazione MineMeld con i diritti di amministrazione;
  - recuperare i file di log necessari per il calcolo delle statistiche di tipo *web analytics*;
- troubleshooting e gestione straordinaria;
- backup e monitoraggio.
- installazione e manutenzione ordinaria di MineMeld;
- installazione degli aggiornamenti di MineMeld;
- monitoraggio dei processi che concorrono all'erogazione del servizio di trasmissione automatizzata degli IoC;
- gestione della VPN affinché l'Amministrazione contraente abbia la possibilità di accedere con i diritti di amministrazione a MineMeld.

Nell'ambito della presente revisione, per mutate esigenze dell'amministrazione dovute a nuove normative intercorse, in funzione delle pianificazioni richieste e del dettaglio delle funzioni, non sono più richiesti i servizi professionali relativi al supporto Python per lo sviluppo della piattaforma di condivisione degli IOC (SP-B2).

5.2.2.1 Vincoli e assunzioni del servizio SP-B

I servizi di hosting soddisfano i seguenti requisiti minimi riservati al sistema di trasmissione automatizzata degli IoC (MineMeld):

- installazione di una singola VM in ambiente VMware vSphere;
- sistema operativo Linux Ubuntu Server versione 16.04 LTS;
- memoria RAM 32 GB;
- spazio massimo datastore 100 GB (thick provision);
- quattro vCPU;
- massimo 1000 sessioni contemporanee di accesso al portale;

- backup full settimanale;
- backup incrementale giornaliero con retention di almeno tre settimane;
- connettività pubblica con banda minima garantita di 30 Mbit/sec e burst di 100 Mbit/sec;
- disponibilità dei servizi esposti sul server stand alone superiore al 99%; la disponibilità è espressa in termini di system uptime (T_{system_up}) del server di produzione ed è calcolata nel seguente modo:

$$T_{system\_up} = \left(T_{up} - T_{down}\right)/T_{up} \times 100,$$

dove T_{up} sono i minuti di disponibilità contrattuale e T_{down} sono i minuti di downtime imputabili al server.[1]

Per poter gestire l'aggiornamento dell'applicazione MineMeld, le relative richieste di servizio dovranno pervenire all'Help Desk dell'RTI complete dei file di aggiornamento e delle istruzioni necessarie al loro corretto utilizzo. Le stesse saranno evase entro 24 ore.

In riferimento all'indirizzamento IP assegnato per l'erogazione del servizio in oggetto, si evidenzia quanto segue:

L'architettura della piattaforma MineMeld è costituita da componenti in housing presso la sede Leonardo S.p.A. di Chieti Scalo (Via E. Mattei 21 – Chieti Scalo). In particolare le componenti hanno lo scopo di consentire all'applicativo MineMeld di pubblicare ed accedere a servizi esposti sulla rete Internet attraverso l'architettura esposta nel par. 5.2.2 del presente documento.

- Salvo diversa indicazione da parte di AgID, Leonardo S.p.A. procederà alla conservazione dei log delle attività di navigazione, traffico di outbound e amministrazione di tutti i sistemi utilizzati per l'infrastruttura per un tempo di conservazione pari ad un anno solare, attraverso opportune policy di rotazione dei log.
- L'indirizzo IP pubblico assegnato per l'erogazione del servizio è 193.104.223.164. Si fa altresì presente che, al fine di garantire il corretto funzionamento del servizio, potrà essere in futuro necessario assegnare al servizio altri indirizzi IP appartenenti alla subnet di indirizzamento 193.104.223.0/24, previa comunicazione scritta all'Amministrazione contraente.
- Tali indirizzi, inclusi quelli appartenenti alla subnet specificata anche se non ancora assegnati al servizio, sono stati registrati presso le autorità competenti (RIPE) a nome del provider telefonico fornitore, che sarà tenuto, in caso di richiesta dell'Autorità Giudiziaria relativa all'utilizzo dei suddetti indirizzi IP, ad indirizzarla a Leonardo S.p.A.

Qualora ciò dovesse accadere, sarà cura della scrivente reindirizzare la richiesta pervenuta ad AgID in qualità di reale ed esclusiva utilizzatrice della risorsa assegnata. A tal proposito, Leonardo S.p.A. dichiara di non essere responsabile rispetto a eventuali richieste di terzi, di qualunque genere, derivanti e/o connessi ai fatti di cui alla suddetta richiesta.

5.2.2.2 Modalità di erogazione del servizio SP-B

L'RTI si occuperà di redigere, concordare e condividere con l'Amministrazione contraente una specifica di servizio che riporterà tutti i dettagli puntuali legati all'operatività. La specifica di servizio sarà considerata un documento ufficiale per la conduzione del servizio SP-B1. Esso sarà erogato in modalità continuativa secondo le finestre di servizio definite nella seguente Tabella 9.

[1] L'orario di misurazione è esteso a tutta la giornata (H24) e la rilevazione del KPI T_{system_up} dovrà essere su base trimentrale.

Tabella 9: Modalità di erogazione

Attività	Disponibilità
Help Desk (telefonico)	9:00-18:00 lunedì – venerdì (escluso festività)
Help Desk (telefonico)	H24
Monitoraggio di disponibilità	H24
Monitoraggio di sicurezza	H24

5.2.2.3 Quantità e prezzi del servizio SP-B

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].

5.2.2.4 Attivazione del servizio SP-B

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

5.2.2.5 Deliverable del servizio SP-B

Saranno prodotti dei report periodici a cadenza mensile che mostrano le statistiche volumetriche relative al traffico (sia in ingresso sia in uscita) generato dall'applicazione MineMeld. Per le statistiche di accesso all'applicazione MineMeld (web analytics), l'RTI metterà a disposizione i file di log.

Altri deliverable per il progetto e lo sviluppo in ambiente Python della piattaforma di condivisione IOC saranno definiti in accordo con l'Amministrazione contraente in sede di kick-off meeting.

5.2.3 Adeguamento della piattaforma di infosharing riservata del CERT-PA (SP-C)

Al fine di migliorare il livello di sicurezza globale, i servizi professionali che saranno erogati per la revisione della piattaforma di infosharing riservata del CERT-PA fruibile da rete Internet, saranno articolati ne seguenti attività:

- Analisi e specifica dei requisiti
- Sviluppo del *portale* e del *backoffice* di amministrazione dello stesso.

Analisi e specifica dei requisiti

Questa attività deve prevede i seguenti punti:

- Architettura dell'informazione
- Visual design
- Specifica dei requisiti e progettazione per
  - la rapida implementazione di nuovi pattern comportamentali, dovuti a minacce specifiche sul cliente,
  - la gestione contenuti
  - la gestione chiave e protezione documenti
  - il data sharing
  - definizione di gruppi/ruoli
  - la gestione accreditamento
  - la gestione notifiche
  - la ricerca.

Sviluppo della piattaforma di infosharing riservata del CERT-PA

La piattaforma di infosharing riservata del CERT-PA sarà sviluppata in maniera conforme ai requisiti relativi all'accessibilità previsti per legge per rispettare gli usuali canoni di usabilità al fine di raggiungere gli obiettivi prefissati con efficacia, efficienza, soddisfazione da parte dell'utente. Il sito, inoltre, fornirà un'interfaccia responsive che consenta di fruire i contenuti anche da dispositivi mobili (utilizzando framework di sviluppo quali, ad esempio, Bootstrap).

La piattaforma sarà composta dalle pagine descritte di seguito.

- **Home page livello 1**. La Home Page di un utente autenticato di livello 1, mostrerà le *News* e la lista degli ultimi bollettini caricati e sarà organizzata in maniera distinta dalla homepage di un utente di livello 2. La portlet delle news sarà alimentata utilizzando le funzionalità native di Liferay.
- **Home page livello 2**. La Home page di un utente autenticato di livello 2, mostrerà le *News* e la lista degli ultimi bollettini caricati e sarà organizzata in maniera distinta dalla homepage di un utente di livello 1. La portlet delle news sarà alimentata utilizzando le funzionalità native di Liferay.
- **Bollettini**. È la pagina che contiene la lista dei bollettini di sicurezza generici. La pubblicazione di un nuovo bollettino invierà una notifica via email a tutti gli utenti a cui deve essere distribuito il bollettino.
- **Upload chiave GPG**. È la pagina che consente agli utenti di caricare la propria chiave pubblica al fine di ricevere avvisi cifrati specifici per l'ente di appartenenza.
- **Avvisi**. Questa pagina contiene la lista degli avvisi, che saranno cifrati automaticamente dal sistema, utilizzando la chiave pubblica dell'utente accreditato (preventivamente caricata sul portale tramite l'interfaccia preposta). Sarà posta particolare attenzione alla gestione delle chiavi pubbliche degli utenti. Le informazioni presenti sugli avvisi sono specifiche per un insieme di Enti, di ruoli o di utenti.
- **Accreditamento di livello 2**. La pagina che consente a un utente di fare richiesta di accreditamento di livello 2.
- **Data-sharing**. La condivisione di documenti tra CERT-PA e utenti dovrà essere realizzata tramite la funzione di data-sharing. La funzionalità è costituita da tre aree funzionali:
  - menu ad albero di navigazione tra le cartelle di lavoro (posizionato sulla parte sinistra della pagina); la cartella di lavoro radice è denominata "CERT-PA-share";
  - menu di elenco degli elementi del documentale (posizionato sulla parte alta a destra della pagina): elenco degli oggetti che caratterizzano una cartella di lavoro, ovvero: cartelle di lavoro; documenti;
  - menu di dettaglio di un elemento (posizionato sulla parte bassa a destra della pagina): dettaglio dei parametri che caratterizzano l'elemento, in particolare attributi legati al nome e attributi legati ai permessi di visibilità.

  Ogni elemento ha un insieme di attributi, di regole di accesso e di visibilità dello stesso. Le regole di accesso esprimono chi può interagire con l'elemento e quali sono i privilegi su di esso. L'insieme dei privilegi definisce quali sono le azioni permesse dagli utenti sull'elemento specifico:
  - READ: permesso di lettura del documento;
  - EDIT: permesso di modifica e cancellazione sull'elemento.
- **Rubrica: utenti e organizzazioni**. La pagina della rubrica consente di visualizzare la rubrica degli utenti registrati al portale. Sarà prevista una funzione di ricerca. La rubrica è visibile ai soli utenti cui è stata fornita una specifica autorizzazione lato backoffice.
- **Segnalazioni**. Le segnalazioni inviate dagli utenti saranno inviate al sistema di *trouble ticketing* interno al fine di poter essere adeguatamente elaborate. L'invio delle segnalazioni sarà protetto da un opportuno CAPTCHA.
- **Ricerca**. Le pagine pubbliche del sito saranno ricercabili. Le pagine private saranno ricercabili solo dagli utenti che hanno i relativi diritti di sicurezza. Più in generale, quindi, la funzionalità di ricerca rispetterà

i criteri di sicurezza imposti dalle ACL applicate ai documenti. In particolare, non sarà consentita la ricerca di documenti su cui l'utente non ha i permessi.

- **Chi siamo**. La pagina del CERT-PA che fornisce indicazioni sul "Chi siamo".
- **Contatti**. La pagina per contattare il CERT-PA.
- **Pagine di feedback**. Il portale fornirà delle pagine specifiche al fine di fornire opportuni feedback agli utenti:
  - in fase di registrazione
  - in fase di creazione account
  - nel caso di password dimenticata.

Backoffice di amministrazione della piattaforma di infosharing

Il back office della piattaforma prevederà le seguenti sezioni:

- **Gestione bollettini**: la funzionalità di gestione dei bollettini da backoffice.
- **Gestione avvisi**: la funzionalità custom di gestione degli avvisi da backoffice.
- **Gestione accreditamenti**: la funzionalità custom di gestione degli accreditamenti da backoffice.
- **Gestione domini email**: la funzionalità custom di gestione dei domini email autorizzati alla registrazione da backoffice.
- **Gestione rubrica**: Le utenze abilitate a vedere la rubrica sono coloro a cui l'amministratore ha impostato uno specifico flag lato backoffice. Le utenze disattivate non compariranno all'interno della rubrica.
- **Gestione news**: La portlet delle news dovrà essere alimentata utilizzando le funzionalità native di Liferay.
- **Log attività**: la funzionalità "log attività" permette di visualizzare tutti gli eventi applicativi generati dagli utenti del Portale che accedono alle funzionalità custom realizzate per il CERT – PA.
- **Gruppi di utenti**: gestione dei gruppi utenti della piattaforma.
- **Ruoli**: definizione dei ruoli della piattaforma:
  - Amministratore CERT – PA
  - Operatore CERT – PA
  - Referente PA
  - Responsabile della Sicurezza
  - Responsabile gruppo ULS
  - Operatore ULS
  - Utente Registrato
  - Utente Accreditato.

Nell'ambito della presente revisione, per mutate esigenze dell'amministrazione dovute a nuove normative intercorse, in funzione delle pianificazioni richieste e del dettaglio delle funzioni si erogheranno le seguenti attività supplementari in sostituzione di quelle non più richieste:

- autenticazione degli utenti del sistema mediante sistema centralizzato openLDAP
- gestione di un "wizard" di primo accesso con profilazione di secondo livello
- upgrade della piattaforma Liferay Portal Community Edition alla versione 7.3 CE
- modifiche al portale Infosec2 (IOC, BlackList e layout)
- integrazionI al modulo InfoFS.

5.2.3.1 Vincoli e assunzioni del servizio SP-C

L'attuale soluzione utilizza Liferay Portal Community Edition 6.2 CE GA2 in bundle con Tomcat in configurazione standalone. Gli sviluppi esistenti saranno migrati sul nuovo portale Liferay Portal Enterprise Edition solo se non risultassero componenti native che eseguono la stessa funzione; tale approccio consente di minimizzare il numero di bug potenzialmente generati da uno sviluppo custom e quindi, come conseguenza, di aumentare la sicurezza generale del sistema.

Sicurezza

Eventuale codice custom rispetterà stringenti criteri di sicurezza quali:

- verifica statica della sicurezza del codice,
- conformità alle norme OWASP.

Migrazione

Sarà prevista la migrazione di tutti gli utenti, organizzazioni, gruppi e ruoli già presenti sul portale oltre ai seguenti contenuti:

- bollettini
- avvisi.

Le news sono escluse dalla migrazione.

Installazione

Si presuppone l'installazione di Liferay Portal sull'infrastruttura fornita da AgID.

5.2.3.2 Modalità di erogazione del servizio SP-C

Il servizio SP-C sarà erogato in due fasi:

- Fase 1: comprende le attività di analisi, progettazione, sviluppo;
- Fase 2: comprende le attività di:
  - Manutenzione adeguativa/evolutiva: le attività saranno concordate col responsabile di progetto successivamente alla data di collaudo del sistema.
  - Manutenzione correttiva: l'attività sarà erogata secondo le finestre di servizio definite nella Tabella 10 .

Il servizio sarà erogato in modalità as a service presso le sedi dell'RTI e dell'Amministrazione contraente.

Tabella 10: Modalità di erogazione

Attività	Disponibilità
Help Desk (telefonico)	9:00-18:00 lunedì – venerdì (escluso festività)

5.2.3.3 Quantità e prezzi del servizio SP-C

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].

5.2.3.4 Attivazione del servizio SP-C

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

5.2.3.5 Deliverable del servizio SP-C

Le attività svolte attraverso l'erogazione dei servizi professionali prevederanno le seguenti milestone contrattuali:

- analisi dei requisiti di sicurezza,
- collaudo del portale di front end,
- collaudo del portale di back office,
- report analisi di sicurezza,
- installazione,
- migrazione dei contenuti.

5.2.4 Supporto al modello d'ingaggio delle Regioni per il CERT-PA (SP-F)

Nell'ambito del presente servizio professionale saranno svolte attività di prevenzione e monitoraggio delle minacce informatiche e gestione degli incidenti di sicurezza informatica eseguite da AgID attraverso la struttura del CERT-PA. Nello specifico le attività di:

- definizione delle *linee guida da seguire per la costituzione di una rete di CERT di prossimità*;
- revisione della *procedura di risposta agli incidenti da attuare a livello regionale*.

Linee guida per la costituzione di una rete di CERT di prossimità

Per la definizione delle linee guida che dovranno essere seguite in fase di costituzione dei CERT di prossimità saranno svolte le seguenti attività, che concorrono alla definizione di un *modello di riferimento nazionale*.

- Presentazione dell'approccio metodologico per la costituzione dei CERT di prossimità
- Definizione degli ambiti di governance di ciascun CERT di prossimità, in termini di:
  - mandato e ambiti di operatività,
  - constituency di riferimento,
  - modello di interazione con gli altri attori.
- Definizione del catalogo dei servizi offerti dai CERT di prossimità e strategia di rilascio dei servizi.
- Definizione delle capacità da implementare per l'avvio dei CERT di prossimità, che includano:
  - processi (inclusi criteri, modalità e flussi, ruoli e responsabilità, misure di prestazione),
  - struttura organizzativa e risorse,
  - tecnologie,
  - sicurezza fisica.
- Identificazione dei fattori abilitanti, inclusi:
  - strategia di comunicazione verso altri enti locali e/ centrali,
  - principi e modalità di cooperazione e affiliazione.

Procedura di risposta agli incidenti informatici a livello locale

In fase di revisione della procedura di risposta agli incidenti informatici a livello locale le attività da svolgere saranno quelle di seguito elencate.

- Raccolta della procedura esistente di risposta agli incidenti definita a livello centrale e locale e degli ulteriori elementi utili alla comprensione del processo attualmente implementato.
- Analisi e comprensione del processo in termini di:
  - ruoli e responsabilità;

- fasi, sotto-fasi e attività;
- strumenti e tecnologie a supporto;
- indicatori e metriche.

- Identificazione degli elementi di aggiornamento / miglioramento del processo, riconducibili sia alle peculiarità del contesto (locale) che a standard o *leading practices*.
- Condivisione degli elementi di aggiornamento / miglioramento con gli attori chiave identificati e raccolta delle osservazioni.

5.2.4.1 Vincoli e assunzioni del servizio SP-F

N.A.

5.2.4.2 Modalità di erogazione del servizio SP-F

Le attività progettuali saranno condotte (durante il normale orario di lavoro) attraverso una fase di assessment iniziale – svolta con il supporto del personale chiave dell'Amministrazione contraente – e di raccolta d'informazioni e documentazione interna alla stessa, in modo da declinare le attività il più possibile rispetto al contesto organizzativo di riferimento.

5.2.4.3 Quantità e prezzi del servizio SP-F

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].

5.2.4.4 Attivazione del servizio SP-F

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

5.2.4.5 Deliverable del servizio SP-F

Per l'avvio dei CERT regionali saranno definite le linee guida implementative, ovvero un documento contenente indicazione di:

- modello di governance;
- servizi offerti dai CERT regionali;
- capacità necessarie per l'erogazione da parte del CERT di prossimità dei servizi verso le Pubbliche amministrazioni locali;
- fattori abilitanti;
- modalità implementative.

Sarà inoltre fornito il materiale a supporto per la presentazione delle Linee Guida per la costituzione dei CERT di prossimità. Successivamente sarà predisposta e rilasciata la procedura aggiornata di risposta agli incidenti a livello locale, che è un documento contenente indicazione di:

- ambito di applicazione;
- attori coinvolti e responsabilità;
- fasi, sotto-fasi e attività di processo, con rappresentazione dei relativi worfklow (con particolare attenzione al processo di escalation verso il CERT-PA);
- matrice delle responsabilità;
- descrizione degli strumenti operativi a supporto del processo
- requisiti di sicurezza fisica.

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 11.

Tabella 11: 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 Data loss/leak prevention, Database security e Professionali	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 al numero verde: **800 894 590**. 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 Modalità di configurazione

Non applicabile.

A.3 Specifiche di collaudo

Le specifiche di collaudo utilizzate per il collaudo della piattaforma saranno fornite separatamente.

A.4 Quantità e prezzi

La fornitura che seguirà la stipula del contratto esecutivo rispetta le quantità e i prezzi presentati di seguito (cfr. Tabella 12, Tabella 13, Tabella 14, Tabella 15, Tabella 16 e Tabella 17), 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].

Tabella 12: Quantità e prezzi del servizio L2.S3.7

Servizio L2.S3.7 - Web application firewall e Next Generation firewall			2018			2019			2020			2021		
Metrica	Fascia	Prezzo unitario	Nun.tà	Mesi	Prezzo	Nun.tà	Mesi	Prezzo	Nun.tà	Mesi	Prezzo	Nun.tà	Mesi	Prezzo
throughput / anno	Fascia 1: throughput fino a 50 Mbps	€ 2.630,00	0	4	€ -	0	12	€ -	0	12	€ -	0	7,0	€ -
	Fascia 2: throughput fino a 200 Mbps	€ 5.600,00	1	4	€ 1.866,67	1	12	€ 5.600,00	1	12	€ 5.600,00	1	7,0	€ 3.266,67
	Fascia 3: throughput fino a 500 Mbps	€ 8.900,00	0	4	€ -	0	12	€ -	0	12	€ -	0	7,0	€ -
					€ 1.866,67			€ 5.600,00			€ 5.600,00			€ 3.266,67

Tabella 13: Quantità e prezzi del servizio L2.S3.9 (SP-A)

SP-A - Definizione e sviluppo di una piattaforma di aggregazione dati (INFOSEC)				2018		2019		2020		2021	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo
giorno / uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	66	€ 19.800,00	279	€ 83.700,00	15	€ 4.500,00	0	€ -
		Security Architect	€ 372,90	156	€ 58.172,40	800	€ 298.320,00	34	€ 12.678,60	0	€ -
		Spec. di tecnologia/prodotto Senior	€ 295,00	80	€ 23.600,00	353	€ 104.135,00	17	€ 5.015,00	0	€ -
		Spec. di tecnologia/prodotto	€ 235,00	0	€ -	0	€ -	0	€ -	0	€ -
giorno / uomo	Orario continuativo H24	Spec. di tecnologia/prodotto Senior H24	€ 1.180,00	0	€ -	0	€ -	0	€ -	0	€ -
		Spec. di tecnologia/prodotto H24	€ 930,00	0	€ -	0	€ -	0	€ -	0	€ -
					€ 101.572,40		€ 486.155,00		€ 22.193,60		€ -

Tabella 14: Quantità e prezzi del servizio L2.S3.9 (SP-B1, hosting)

SP-B1 - Servizi per Piattaforma di Trasmissione Automatizzata degli IoC (Hosting)				2018		2019		2020		2021	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo
giorno / uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	2	€ 600,00	5	€ 1.500,00	1	€ 300,00	4	€ 1.200,00
		Security Architect	€ 372,90	2	€ 745,80	6	€ 2.237,40	1	€ 372,90	9	€ 3.356,10
		Spec. di tecnologia/prodotto Senior	€ 295,00	2	€ 590,00	6	€ 1.770,00	1	€ 295,00	6	€ 1.770,00
		Spec. di tecnologia/prodotto	€ 235,00	0	€ -	0	€ -	0	€ -	0	€ -
giorno / uomo	Orario continuativo H24	Spec. di tecnologia/prodotto Senior H24	€ 1.180,00	6	€ 7.080,00	17	€ 20.060,00	3	€ 3.540,00	22	€ 25.960,00
		Spec. di tecnologia/prodotto H24	€ 930,00	0	€ -	0	€ -	0	€ -	0	€ -
					€ 9.015,80		€ 25.567,40		€ 4.507,90		€ 32.286,10

Tabella 15: Quantità e prezzi del servizio L2.S3.9 (SP-B2, Python)

SP-B2 - Servizi per Piattaforma di Trasmissione Automatizzata degli IoC (Supporto Phyton)				2018		2019		2020		2021	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo
giorno / uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	0	€ -	0	€ -	0	€ -	0	€ -
		Security Architect	€ 372,90	0	€ -	0	€ -	0	€ -	0	€ -
		Spec. di tecnologia/prodotto Senior	€ 295,00	0	€ -	0	€ -	0	€ -	0	€ -
		Spec. di tecnologia/prodotto	€ 235,00	0	€ -	0	€ -	0	€ -	0	€ -
giorno / uomo	Orario continuativo H24	Spec. di tecnologia/prodotto Senior H24	€ 1.180,00	0	€ -	0	€ -	0	€ -	0	€ -
		Spec. di tecnologia/prodotto H24	€ 930,00	0	€ -	0	€ -	0	€ -	0	€ -
					€ -		€ -		€ -		€ -

Tabella 16: Quantità e prezzi del servizio L2.S3.9 (SP-C)

SP-C - Adeguamento Portale Riservato CERT-PA (InfoSharing)				2018		2019		2020		2021	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo
giorno / uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	47	€ 14.100,00	84	€ 25.200,00	5	€ 1.500,00	48	€ 14.400,00
		Security Architect	€ 372,90	315	€ 117.463,50	577	€ 215.163,30	14	€ 5.220,60	133	€ 49.595,70
		Spec. di tecnologia/prodotto Senior	€ 295,00	156	€ 46.020,00	499	€ 147.205,00	12	€ 3.540,00	420	€ 123.900,00
		Spec. di tecnologia/prodotto	€ 235,00	41	€ 9.635,00	413	€ 97.055,00	21	€ 4.935,00	0	€ -
giorno / uomo	Orario continuativo H24	Spec. di tecnologia/prodotto Senior H24	€ 1.180,00	0	€ -	0	€ -	0	€ -	0	€ -
		Spec. di tecnologia/prodotto H24	€ 930,00	0	€ -	0	€ -	0	€ -	0	€ -
					€ 187.218,50		€ 484.623,30		€ 15.195,60		€ 187.895,70

Tabella 17: Quantità e prezzi del servizio L2.S3.9 (SP-F)

SP-F - Modello di Ingaggio delle Regioni per Cyber Security - CERT				2018		2019		2020		2021	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo
giorno / uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	30	€ 9.000,00	3	€ 900,00	3	€ 900,00	0	€ -
		Security Architect	€ 372,90	192	€ 71.596,80	24	€ 8.949,60	24	€ 8.949,60	0	€ -
		Spec. di tecnologia/prodotto Senior	€ 295,00	145	€ 42.775,00	18	€ 5.162,50	18	€ 5.162,50	0	€ -
		Spec. di tecnologia/prodotto	€ 235,00	0	€ -	0	€ -	0	€ -	0	€ -
giorno / uomo	Orario continuativo H24	Spec. di tecnologia/prodotto Senior H24	€ 1.180,00	0	€ -	0	€ -	0	€ -	0	€ -
		Spec. di tecnologia/prodotto H24	€ 930,00	0	€ -	0	€ -	0	€ -	0	€ -
					€ 123.371,80		€ 15.012,10		€ 15.012,10		€ -

La seguente tabella riepiloga i servizi professionali:

Tabella 18: Quantità e prezzi del servizio L2.S3.9 (Complessivo)

L2.S3.9 - Servizi Professionali				2018		2019		2020		2021	
Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo	Nun.tà	Prezzo
giorno / uomo	Normale orario di lavoro (8 ore)	Capo progetto	€ 300,00	145,0	€ 43.500,00	371,0	€ 111.300,00	24,0	€ 7.200,00	52,0	€ 15.600,00
		Security Architect	€ 372,90	665,0	€ 247.978,50	1.407,0	€ 524.670,30	73,0	€ 27.221,70	142,0	€ 52.951,80
		Spec. di tecnologia/prodotto Senior	€ 295,00	383,0	€ 112.985,00	875,5	€ 258.272,50	47,5	€ 14.012,50	426,0	€ 125.670,00
		Spec. di tecnologia/prodotto	€ 235,00	41,0	€ 9.635,00	413,0	€ 97.055,00	21,0	€ 4.935,00	0,0	€ -
giorno / uomo	Orario continuativo H24	Spec. di tecnologia/prodotto Senior H24	€ 1.180,00	6,0	€ 7.080,00	17,0	€ 20.060,00	3,0	€ 3.540,00	22,0	€ 25.960,00
		Spec. di tecnologia/prodotto H24	€ 930,00	0,0	€ -	0,0	€ -	0,0	€ -	0,0	€ -
					€ 421.178,50		€ 1.011.357,80		€ 56.909,20		€ 220.181,80

A.4.1 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

Di seguito si riporta la programmazione delle attività, espressa in giorni lavorativi a partire dalla data di perfezionamento del contratto esecutivo (T0).

B.1 Attività dei servizi L2.S3.7 e L2.S3.9

In base a quanto richiesto dall'Amministrazione contraente nel Piano dei fabbisogni [DA-5] la Tabella 19 riporta le attività previste per l'erogazione del servizio L2.S3.7.

Tabella 19: Piano di lavoro del servizio L2.S3.7

Nome attività	Durata	Inizio	Fine	Vincoli
Web Application Firewall e Next generation firewall management	35M	T1=T0+45 gg	T0+M35	

L'Amministrazione contraente ha espresso, inoltre, nel proprio Piano dei fabbisogni [DA-5] la necessità di attività di personalizzazione che saranno svolte attraverso l'erogazione di servizi professionali L2.S3.9, i cui dettagli sono descritti in § 5.2.

Tabella 20: Piano di lavoro del servizio L2.S3.9

Nome attività	Durata	Inizio	Fine	Vincoli
Definizione e sviluppo di una piattaforma di aggregazione dati (SP-A)	35M			
Supporto al progetto INFOSEC (3 FTE)	24M	T1=T0+30 gg	T1+M24	
Supporto al progetto INFOSEC (1,5 FTE)	12M	T1+M25	T1+M35	
Servizi per la piattaforma di information sharing (SP-B)	35M	T1=T0+45 gg	T1+M35	
Adeguamento del portale riservato CERT-PA (SP-C)	35M			
Analisi, progettazione, Sviluppo	6M	T1=T0+30 gg	T1+M6	
Manutenzione adeguativa, evolutiva, correttiva	30M	T1+M7	T1+M35	
Supporto al modello d'ingaggio delle Regioni per il CERT-PA (SP-F)	6M	T1=T0+30 gg	T1+M6	