Südtiroler Informatik AG
Informatica Alto Adige SPA

Azienda Sanitaria dell'Alto Adige
Ripartizione Informatica
Via del Ronco, 3 | 39100 Bolzano

a.m.: Ing. Andrea Toniutti
andrea.toniutti@sabes.it
p.c.: Lidia Ferrari
lidia.ferrari@sabes.it

Bolzano, il 10.01.2020

Preventivo: Prev2020.009 Rinnovo servizio di Web Application Penetration Test

Spett.le Azienda Sanitaria dell'Alto Adige,

in riferimento al rinnovo dei servizi già previsti per l'anno 2019 ci pregiamo di comunicarVi con la presente il nostro migliore preventivo.

In attesa di un Vostro cortese riscontro cogliamo l'occasione per porgere

cordiali saluti

SMO/PMO

Il Direttore Generale
STEFAN GASSLITTER

Siemensstraße 29 via Siemens
I – 39100 Bozen Bolzano
Tel. 0471 566000 / Fax 0471 566099
E-Mail: info@siag.it – Web: www.siag.it

Südtiroler Landessparkasse - Sitz Bozen
Cassa di Risparmio di Bolzano - Sede di Bolzano
BBAN: T 0645 11600 000003121300
IBAN: IT95 T060 4511 6000 0000 3121300

SteuerNr., Mwst.Nr. C.Fisc., P.IVA IT 01468500218
Handelsreg. Bozen Reg. Imp. Bolzano 01468500218
Ges.Kap. Cap.Soc. € 8.000.000,00 voll.einge.int.vers.

1. Dati del preventivo

Autore del documento	*Francesco Terracciano*

1.1. Richiesta di preventivo

Priorità del progetto	--
Persone di riferimento Cliente	--

1.2. Dettagli del progetto

Progetto	--
Project Manager	--
Identificativo del progetto (Int. order) nel WM	--
Data inizio progetto	--
Data fine progetto	--
Tipologia di fatturazione	--

1.3. Dettagli del servizio

Service Area	*23. IT-Security, Special Services*
Servizio	*23.01.02 Servizio IT per la esecuzione di un Penetration Test*
Tipo di attività	*Rinnovo servizio IT*
Service Area Manager	*Francesco Terracciano*
Data inizio servizio *(1)* Durata servizio / data fine servizio *(2)*	*15.02.2020* *Annuale*
Tipologia di fatturazione	*A consumo*

(1) Inserire la data di go-live del nuovo servizio o modifica ad un servizio esistente, da tale data il servizio sarà fatturabile.

(2) Il servizio viene rinnovato alla scadenza per lo stesso periodo presente in offerta, a meno di una disdetta esplicita, scritta all'indirizzo shared_orders@siag.it , da parte del cliente, almeno 3 mesi prima della data di scadenza od in seguito ad una sostituzione del servizio.

2. Descrizione generale

Le esigenze di indirizzo strategico aziendale determinano, spesso, la necessità di definire un approccio unificato e strutturato nella gestione della sicurezza. Nell'ottica di mirare ad una riduzione costante del rischio cyber, diventa di fondamentale importanza dotarsi di un servizio che riesca a definire, in una maniera quanto più oggettiva possibile, il grado di sicurezza raggiunto con gli investimenti fatti per, eventualmente, guidare gli investimenti futuri.
Un servizio di Penetration Test mira proprio al raggiungimento di questi obiettivi.

2.1. Dettaglio del progetto e milestones (costi una tantum)

Non è prevista per l'offerta in oggetto una parte progettuale.

2.2 Dettaglio del servizio (costi annuali)

Attraverso il servizio di Penetration Test si vuole offrire una analisi dinamica su uno specifico ambito o applicazione finalizzato ad identificare le vulnerabilità applicative e di sistema e validarne il reale grado di utilizzo simulando un eventuale scenario di attacco e verificando le catene di vulnerabilità utilizzabili e il loro effettivo impatto sui dati e sui servizi.
Il deliverable dell'attività sarà formato da un report complessivo contenente:

a. EXECUTIVE SUMMARY: L'Executive Summary illustrerà i principali rischi a cui l'azienda è sottoposta a causa delle vulnerabilità riscontrate e dovrà fornire un messaggio incisivo allo scopo di provocare un adeguato livello di reazione da parte del management stesso. Nel documento saranno concentrati e riassunti i risultati esposti nel report tecnico, conservandone la sequenza e la struttura concettuale. L'Executive Summary includerà inoltre un piano di azione ad alto livello per illustrare, su specifiche classi di priorità (Breve, Medio e Lungo Termine), le macrocategorie di problemi rilevati sui sistemi oggetto dell'analisi e scandire un opportuno piano di rientro.
b. TECHNICAL REPORT: Il Technical Report sarà articolato in modo da mantenere una separazione logica tra le differenti piattaforme soggette ad analisi. Per ogni piattaforma in esame, oltre a fornire una precisa segnalazione delle varie vulnerabilità riscontrate e/o punti deboli del sistema (in termini di porte, servizi e informazioni del sistema, o circa eventuali analisi condotte in ambito locale) saranno riportate anche indicazioni precise sulle possibili soluzioni (in termini di patch, di configurazioni necessarie e suggerimenti migliorativi) al fine di mitigare i potenziali rischi generati dal loro sfruttamento. Ogni problematica riportata sarà descritta in una sezione specifica di approfondimento tecnico. Tale sezione descrittiva sarà composta almeno da:

1. descrizione di dettaglio della problematica rilevata;
2. riferimenti a documentazione pubblica per ulteriori approfondimenti tecnici;
3. suggerimenti provvisori realizzati dal team di analisi;
4. workaround possibili, qualora applicabili;
5. soluzioni perimetrali di protezione, qualora applicabili;
6. per ogni vulnerabilità tecnica verrà effettuata un'analisi "tecnica" del rischio (basata sullo standard CVSS: Common Vulnerability Scoring System) che prenderà in considerazione popolarità e semplicità dell'attacco commisurata al valore del sistema (laddove disponibile) e al grado di compromissione raggiunto;

Viene altresì fornito, nell'arco dei tre mesi solari successivi alla consegna dei deliverables di cui al punto 1, la possibilità di richiedere una verifica ulteriore sullo stesso applicativo testato e sulle stesse vulnerabilità individuate, al fine di verificare gli effetti del piano di rientro implementato internamente.

Ogni singola attività dovrà essere formalmente autorizzata da SABES mediante apposita firma su Manleva dedicata.

Prestazioni servizio (annuali) in giornate e/o EUR	*Tariffa / Costo*	*Giorni / Unità*	*Importo annuale in EUR (IVA esclusa)*
Prestazioni interne SIAG			
Figure professionali / attività *(inserire sempre la relativa figura professionale prima dell'attività)*			
Service Manager / Service Management	600,00	3	1.800,00
Costi interni			
--	--	--	--
Totale prestazioni interne			1.800,00
Prestazioni esterne (indicare se già coperto da contratto esistente)			
Web application Penetration Test (fino ad un massimo di 8 singole attività)			34.646,00
Totale prestazioni esterne			34.646,00
Totale complessivo senza IVA			36.446,00
IVA 22%			8.018,12
Totale complessivo			44.464,12
Totale costo servizio, senza opzioni, dalla attivazione fino fine anno (e.g. servizio viene attivato a giugno = Indicare i costi da giugno fino dicembre)			44.464,12
Modalità fatturazione			Trimestrale a consumo

Si precisa che verranno fatturate solo le attività effettivamente eseguite e che il costo di una singola attività di Web Application Penetration Test è di 4.330,75 iva esclusa.

2.3 Tariffe applicate

Le tariffe per figura professionale indicate nella tabella sono quelle previste dalla delibera della Giunta Provinciale n° 558 del 12.06.2018:

Classe tariffa	*Figura professionale*	*Importo gg/U in EUR (IVA esclusa)*	*Importo gg/U in EUR (IVA inclusa)*
1	Functional Analyst	525,00	640.50
2	Program, Project Manager	650,00	793.00
3	Software Designer	490,00	597.80
4	Developer, Application Assistance	490,00	597.80
5	Service Manager	600,00	732.00
6	DB Administrator	550,00	671.00
7	System Administrator	425,00	518.50
8	Tecnical & Service Supply	380,00	463.60
9	Formazione	525,00	640,50

3. Tabella riepilogo corrispettivi

Anno Prestazione	2019	2020	2021	2022	2023	Totali
Progetto in EURO	--	--	--	--	--	--
Servizio in EURO	--	36.446,00	--	--	--	36.446,00
Tot annuale	--	36.446,00	--	--	--	
					Tot complessivo senza IVA	36.446,00

4. Obblighi della committente

Il committente si impegna a dare il necessario supporto a Informatica Alto Adige per la corretta esecuzione del progetto/servizio con le seguenti modalità:

- Il committente definisce le persone di riferimento dotandole del necessario potere decisionale;
- Il committente dà tutte le informazioni necessarie in tempi congrui all'esecuzione;
- Il committente garantisce la disponibilità del proprio personale e di quello dei key-user per svolgere le necessarie attività esecutive e di test;
- Il committente approva la necessaria documentazione nei tempi prestabiliti dei risultati di progetto e/o servizio;

- Il committente garantisce l'approvazione della stessa documentazione anche da parte dei key-user finali;

Informatica Alto Adige non risponde del ritardo o del mancato raggiungimento di fine progetto o servizio nell'eventualità in cui il Committente o il key-user finale non abbiano ottemperato ai propri impegni come sopra indicati, né dei relativi eventuali costi aggiuntivi che in tale caso verranno sopportati dal committente stesso.

Nell'eventualità in cui Informatica Alto Adige non ottenga dati e/o informazioni o le ottenga incomplete o in ritardo provvederà a darne tempestiva comunicazione al committente che si impegna a prendere i necessari provvedimenti.

5. Condizioni generali

Modalità di pagamento e fatturazione: al fine del pagamento dei corrispettivi spettanti, Informatica Alto Adige emetterà regolare fattura secondo quanto previsto nel presente preventivo.
Il committente verserà gli importi prestabiliti entro 30 giorni dalla data della fattura.

Validità del preventivo: il presente preventivo ha validità per 30 giorni dopo la sua spedizione, termine oltre il quale Informatica Alto Adige si riserva la facoltà di rivederne i contenuti.

Si dichiara che nell´ambito degli ordinari contatti fra committente, fruitore finale e Informatica Alto Adige, non si sono verificate da parte di chicchessia episodi che anche ipoteticamente appaiano riconducibili o comunque diretti ad atti rilevanti ai sensi del D.Lgsl.231/01 in qualunque forma, finalizzati a compensare il responsabile di illeciti comportamenti, volti a produrre un vantaggio per Informatica Alto Adige.

Il Direttore Generale
STEFAN GASSLITTER