COMUNE DI RIVODUTRI

Provincia di Rieti

Servizio Finanziario

ORIGINALE DI DETERMINAZIONE
DEL RESPONSABILE Servizio Finanziario

N.	DATA	Oggetto:
39	**11-03-2019**	**Affidamento Servizio Sicurezza Cloud alla società Halley anno 2019 - cig Z9A27855AE**

IL RESPONSABILE DEL SERVIZIO

VISTO il decreto sindacale n. 1 del 09-06-2014 con il quale vengono confermate, alla sottoscritta, le funzioni di responsabile del servizio finanziario e tributi e responsabile dell'acquisto di beni e servizi non aventi valutazione di natura tecnica;

Richiamata la deliberazione di Giunta comunale n. 43 del 25-06-2014 avente ad oggetto "*contabilità finanziaria comunale – sostituzione a seguito degli adempimenti previsti dal D.Lgs 118/2011*" con la quale si accetta l'offerta proposta dalla soc HALLEY srl, per l'acquisto di software gestionale in grado di rispondere alle esigenze dettate dalla nuova normativa per gli enti locali relativamente alla "*contabilità armonizzata*".

Richiamata la determinazione n. 102 del 20-07-2018 con la quale si dava l'affidamento alla società Halley per il servizio di sicurezza in cloud per:

-alla corretta esecuzione giornaliera delle copie dati presso il Datacenter di Roma ;
-all' aggiornamento notturno su una infrastruttura di backup;
- all ' aggiornamento da remoto di tutte le procedure

Considerato che l'offerta prevede un canone assistenza annuale dal 2019 230,00 più iva al 22%;
VISTO il bilancio di previsione pluriennale 2019-2021 invia di approvazione;

Vista la proroga al 30-03-2019 per l'approvazione del bilancio di previsione 2019-2021;

Visti i commi 3 e 5 dell'art. 163 del D.lgvo 267/2000 i quale prevedono che nel corso dell'esercizio provvisorio si possono impegnare spese correnti, per ciascun programma, non superiore ad un dodicesimo degli stanziamenti del secondo esercizio del bilancio di previsione deliberato;

Richiamato il D.lgs.vo n. 33 del 14 marzo 2013 circa gli obblighi di trasparenza;
Richiamato il D.lgs.vo n. 241/2016 sulla tracciabilità dei flussi finanziari;
Visto il vigente regolamento di contabilità;
Visto il D.L.vo 18-08-2000 n. 267 e successive modificazioni;

DETERMINA

1) Per quanto esposto in premessa. che qui si intende integralmente riportato e trascritto

2) Di impegnare. per l'affidamento del servizio di sicurezza Cloud (CLOUD sas 1000° alla soc. Halley srl;

3) Di impegnare la spesa di cui al presente atto pari complessivamente ad € 280,60 sul bilancio di previsione 2019-2021 al cap. 101034 codice **01.02-1.03.02.19.005** che presenta la necessaria disponibilità.

Rivodutri, lì **11-03-2019**

Il Responsabile del Servizio
Loredana Rag. Lodovici

CONVENZIONE HALLEY SISTEMI

anno 2019

dal 01/01/2019 al 31/12/2019

stipulata tra:

HALLEY Informatica s.r.l.

Via Circonvallazione, 131 62024 Matelica (MC)
N.Reg.Imp.,Cod.Fisc. e Partita IVA 00384350435
di seguito denominato Halley

e

Comune di Rivodutri

PIAZZA MUNICIPIO 9
Partita IVA 00108820572
di seguito denominato Cliente

La convenzione comprende

- PROTEZIONE DATI

Art. 1 PROTEZIONE DATI

Art. 1.1 SERVIZIO CLOUD SaaS

Art. 1.1.1 - Servizi offerti

1.1.1.1 SPAZIO SU DATACENTER

Halley garantisce uno spazio (hosting) dedicato solo ed esclusivamente alle procedure Halley e adeguato al Cliente sul Datacenter di Matelica con replica nel Datacenter di Roma.

1.1.1.2 COPIE

Halley garantisce la corretta esecuzione giornaliera delle copie dati.
Le copie vengono effettuate automaticamente di notte su una infrastruttura di backup dedicata e separata da dati e programmi Halley.

1.1.1.3 AGGIORNAMENTI

Halley garantisce gli aggiornamenti notturni entro 3 giorni lavorativi dall'inserimento sul sito www.halley.it.
Gli aggiornamenti vengono effettuati da remoto.

Art. 1.1.2 - Impegni Halley

1.1.2.1 SPAZIO SU DATACENTER

Halley si impegna ad offrire uno spazio dedicato adeguato e delle allocazioni di risorse adeguate in termini di CPU, RAM, Hard Disk e quant'altro necessario.

1.1.2.2 COPIE

Halley si impegna ad eseguire backup quotidiani, settimanali, mensili e annuali con archivio storico di 60 giorni consultabile in modo retroattivo ogni giorno.
Halley si impegna a programmare, eseguire e controllare da remoto la corretta effettuazione e l'integrità delle copie; in caso di malfunzionamento, provvederà tempestivamente alla risoluzione del problema.

1.1.2.3 AGGIORNAMENTI

Halley si impegna ad avvisare il Cliente della pubblicazione dell'aggiornamento solo attraverso i banner della procedura.
Nei casi in cui Halley ne ravveda la necessità, avviserà il Cliente tramite PEC o fax indicando, con congruo anticipo, le procedure che verranno aggiornate.
Halley si impegna ad aggiornare le procedure software entro 3 giorni dalla pubblicazione nel sito.

Art. 1.1.3 - Livelli di servizio garantiti (SLA)

- Percentuale di tempo in cui il servizio risulta accessibile e usabile: prossima al 100% su base annua.
- Orario in cui il servizio di supporto tecnico è operativo: assistenza telefonica dal lunedì al venerdì dalle 8.30 alle 17.30 e il sabato dalle 8.30 alle 12.00. In ogni caso è garantito 24 ore su 24 e 7 giorni su 7 il monitoraggio del sistema ed eventuale intervento tecnico in caso di necessità.
- Tempo massimo che intercorre tra la segnalazione di un inconveniente da parte del Cliente e la risposta iniziale alla segnalazione da parte del CSP: 1 ora.

Qualora successivamente all'avvio della fornitura si dovesse rendere necessaria una modifica ai livelli di servizio garantiti, questa sarà preventivamente notificata al Cliente.

Art. 1.1.4 - Impegni del Cliente

1.1.4.1 CONNETTIVITA'

Il Cliente si impegna a munirsi di una connettività adeguata, preferibilmente dedicata ad Halley, con avvertenza che in difetto di una connettività dedicata potrebbero registrarsi dei rallentamenti del lavoro

del Cliente nelle procedure Halley.
Si rimanda a: "*Condizioni Protezione Dati*" art. 2.4.

1.1.4.2 AGGIORNAMENTI

Il Cliente si impegna a scaricare la lettera di aggiornamento attraverso i banner della procedura o dal sito www.halley.it, e a leggerne ed accettarne intrinsecamente tutti i contenuti.

Art. 1.1.5 - Obblighi e limitazioni di responsabilità di Halley

Gli obblighi e le responsabilità di Halley verso il Cliente sono quelli definiti dalla presente convenzione pertanto in qualsiasi caso di violazione o inadempimento imputabile ad Halley, la stessa risponderà nei limiti previsti dallo SLA restando espressamente escluso qualsiasi altro indennizzo o risarcimento al Cliente per danni diretti o indiretti di qualsiasi natura e specie. Il Cliente prende atto ed accetta che in tutti i casi in cui non trova applicazione lo SLA, Halley risponderà esclusivamente nei limiti della somma corrisposta dal Cliente per il servizio Cloud SaaS negli ultimi 12 mesi.

Art. 1.1.6 - Estrazione dati

A fronte di una richiesta scritta del Cliente, Halley si impegna a rendere fruibili e leggibili i dati eseguendo il Dump del database su una struttura Hardware messa a disposizione dal Cliente (Nas, Server, PC).

Art. 1.1.7 - Ottemperanza ai requisiti di legge

1.1.7.1 TRATTAMENTO DEI DATI

In ottemperanza alla vigente normativa in materia di privacy Halley informa il Cliente che i dati saranno trattati esclusivamente per la finalità di erogazione del servizio.
Il servizio è erogato tramite il Datacenter di proprietà di Halley Informatica S.r.l. la quale, in conformità ai requisiti di cui alle circolari Agid n.2 e n.3 del 09/04/2018 è in possesso della certificazione secondo lo standard ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018.

1.1.7.2 PROTEZIONE DEI DATI, MISURE DI SICUREZZA CONTRO INTRUSIONI ED ACCESSI ABUSIVI

In attuazione delle misure di sicurezza di cui al D.lgs 196/2003 e s.m.i. e al Regolamento UE 679/2016, i dati del Cliente contenuti nel/nei Datacenter sono protetti contro il rischio di intrusione ed accessi abusivi mediante l'utilizzo di appositi firewall ridondati di nuova generazione di cui Halley si impegna ad aprire le porte in ingresso (WAN to LAN) esclusivamente agli indirizzi IP del Cliente.
Contro il rischio di intrusioni Halley si impegna altresì ad utilizzare strumenti ragionevolmente sicuri per accedere e svolgere attività sugli apparati ovvero un collegamento criptato con protocolli internazionali di sicurezza, le cui credenziali di accesso sono in possesso ed uso esclusivo degli operatori Halley che ne assicurano la custodia e la segretezza. Dette credenziali non contengono riferimenti agevolmente riconducibili agli operatori e sono modificate da questi ultimi almeno ogni sei mesi.
I trasferimenti dei dati tra i due Datacenter di Matelica e Roma avvengono mediante l'utilizzo di un canale dedicato e crittografato.
L'eventuale accesso da parte di tecnici o operatori Halley a dati contenuti nel/nei Datacenter avviene esclusivamente per provvedere alla manutenzione ordinaria e/o straordinaria da remoto e dunque unicamente per scopi di assistenza tecnica.

1.1.7.3 CONSERVAZIONE DEI LOG

In conformità con la normativa in materia di sicurezza e privacy, Halley garantisce la conservazione in archivi dei LOG (traccia degli accessi e delle attività svolte sull'apparato) per un periodo minimo di 6 mesi.
Tutti i LOG possono essere recapitati al Cliente a seguito di richiesta scritta (pec o fax) da parte di quest'ultimo.

1 1 7.4 SICUREZZA DATACENTER DI MATELICA

Il Datacenter di Matelica in cui sono ospitati i dati Halley è strutturato in modo tale da garantire un adeguato livello di sicurezza.

Il Datacenter è stato realizzato in una struttura edile in cemento armato. La sala dati si affaccia su un piazzale di pertinenza completamente recintato, e sorvegliato che ospita scambiatori di calore e gruppi elettrogeni.

Il cablaggio dati, per garantire la massima sicurezza e continuità operativa, per scongiurare interferenze elettromagnetiche e per facilitare l'ispezione visiva, è aereo e sopra gli armadi che contengono gli apparati.

Porte e finestre dell'infrastruttura interna sono realizzate con materiali certificati REI 60 per un'adeguata protezione passiva contro gli incendi.

Il Datacenter dispone di sistemi di alimentazione ridondanti paralleli. L'alimentazione dell'apparecchiatura UPS è dotata di protezione filtro. Il locale accumulatori che ospita le stringhe del sistema di UPS, per ragioni di sicurezza, è stato realizzato separato dalle sale quadri elettrici e dalle sale che ospitano gli apparati elettronici. Particolare attenzione è stata dedicata all'isolamento tramite contro-tubazione del cablaggio delle stringhe e all'isolamento addizionale dei pianali di supporto, degli accumulatori stessi, tramite l'inserimento di vassoi isolanti addizionali.

La sala del Datacenter è mantenuta a temperatura e umidità controllate mediante impianti di aria condizionata ridondati e monitorati da un sistema di controllo/allarme

Gli impianti tecnologici per l'antincendio sono costituiti da rilevatori laser di fumo, posizionati in modo modulare sopra il pavimento, e collegati al sistema antincendio. Il sistema antincendio può essere attivato in modo manuale o in modo automatico, circoscrivendo soltanto l'area in cui è presente l'incendio.

L'area perimetrale è videosorvegliata h24.

Per raggiungere il Datacenter è necessario oltrepassare la sala di ingresso e una sala server. La porta di accesso alla sala server e al Dataceter è blindata, dotate di sistema di controllo accessi centralizzato, con ingresso consentito esclusivamente alle persone autorizzate tramite lettore di badge.

1.1.7.5 SICUREZZA DATACENTER DI ROMA

Il Datacenter di Roma in cui sono ospitati i dati Halley è strutturato in modo tale da garantire un adeguato livello di sicurezza.

Il Datacenter è stato realizzato in una struttura edile in cemento armato protetta e presidiata. La sala dati è costruita in un luogo seminterrato, con i lati non interrati che si affacciano su un piazzale di pertinenza completamente recintato, allarmato e sorvegliato che ospita scambiatori di calore e gruppi elettrogeni. La recinzione protegge il piazzale da possibili esondazioni in caso di allagamento della sede stradale attigua, e il cancello carrabile è predisposto con paratie elettriche stagne.

Il cablaggio dati, per garantire la massima sicurezza e continuità operativa e scongiurare interferenze elettromagnetiche, è aereo e sopra gli armadi che contengono gli apparati.

Pareti, porte e finestre dell'infrastruttura interna sono realizzate con materiali certificati REI 120 per un'ottimale protezione passiva contro gli incendi.

Il Datacenter dispone di sistemi di alimentazione ridondanti paralleli. L'alimentazione dell'apparecchiatura UPS è dotata di protezione filtro. Il locale accumulatori che ospita le stringhe del sistema di UPS, per ragioni di sicurezza, è stato realizzato separato dalle sale quadri elettrici e dalle sale che ospitano gli apparati elettronici. Particolare attenzione è stata dedicata all'isolamento tramite contro-tubazione del cablaggio delle stringhe e all'isolamento addizionale dei pianali di supporto, degli accumulatori stessi, tramite l'inserimento di vassoi isolanti addizionali.

La sala del Datacenter è mantenuta a temperatura e umidità controllate mediante impianti di aria condizionata ridondati (n+1), in configurazione di load-balancing e automatic failover. Tutti i sistemi di condizionamento, al fine di massimizzare la disponibilità del raffrescamento, sono realizzati con impianti indipendenti collegati in rete-dati tra loro e monitorati da un sistema di controllo/allarme.

Gli impianti tecnologici per l'antincendio sono costituiti da rilevatori ottici di fumo, posizionati in modo modulare sotto e sopra il pavimento sopraelevato, e collegati al sistema antincendio. Il sistema può

essere attivato in modo manuale o in modo automatico, circoscrivendo soltanto l'area in cui è presente l'incendio.
L'area perimetrale è videosorvegliata h24. Tutti i varchi di accesso al Datacenter sono dotati di porte blindate allarmate con lettore di badge e tastierino numerico per accedere e, insieme ai varchi di accesso alle singole sale, sono dotati di sistema di controllo accessi centralizzato. Gli armadi Rack ospitati sono fisicamente chiusi singolarmente con serratura e tutte le stanze in cui si trovano le apparecchiature sono monitorate con telecamere a circuito chiuso dotate di funzionalità motion detection.

1.1.7.6 CONFORMITA' ALLE MISURE MINIME DI SICUREZZA ICT

Il servizio è conforme alla circolare AGID del 18 aprile 2017, n. 2/2017 contenente le "Misure minime per la sicurezza ICT delle pubbliche amministrazioni". In particolare i Server e le Workstation che hanno attivo il servizio:

- Mantengono un inventario del software installato tramite la Dashboard (ABSC 2.3.2 all.1 circolare Agid n. 2/2017);
- Registrano le versioni del sistema operativo e le applicazioni installate (ABSC 2.3.3 all.1 circolare Agid n. 2/2017);
- Utilizzano configurazioni standard per la protezione dei sistemi operativi operativi (ABSC 3.1.1 all.1 circolare Agid n. 2/2017);
- Hanno implementato l'hardening per eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate (ABSC 3.1.2 all.1 circolare Agid n. 2/2017);
- Hanno una configurazione standard definita (ABSC 3.2.1 all.1 circolare Agid n. 2/2017);
- Trasmettono informazioni alle Dashboard in modo sicuro: per i server tramite tunnel crittografato ssh mentre per le workstation tramite protocollo https (ABSC 3.4.1 all.1 circolare Agid n. 2/2017);
- Hanno gli accessi limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi (ABSC 5.1.1 all.1 circolare Agid n. 2/2017);
- Registrano gli accessi effettuati (ABSC 5.1.2 all.1 circolare Agid n. 2/2017);
- Per assistenza e manutenzione vengono usate password amministrative complesse (ABSC 5.7.2 all.1 circolare Agid n. 2/2017);
- Le password vengono sostituite con sufficiente frequenza (ABSC 5.7.3 all.1 circolare Agid n. 2/2017);
- Effettuano una copia locale quotidiana mantenendo uno storico di 60 giorni e dove previsto la stessa copia viene ridondata su storage (ABSC 10.1.1 all.1 circolare Agid n. 2/2017);
- Viene verificata periodicamente l'utilizzabilità delle copie mediante ripristino di prova (ABSC 10.2.1 all.1 circolare Agid n. 2/2017)

1.1.7.7 MISURE DI SICUREZZA IN CONFORMITA' AL REGOLAMENTO COMUNITARIO 679/2016 (GDPR)

Si rimanda a: *"Adeguamento al Regolamento Comunitario GDPR"* art. 2.10.

In particolare:

Contro i rischi di distruzione e perdita dei dati il Servizio Cloud SaaS (Software as a Service) garantisce:

- L'esecuzione di backup quotidiani, settimanali, mensili e annuali con un archivio storico di 60 giorni;
- L'accesso al server consentito solo alle persone autorizzate;
- Il collegamento al Cloud da parte dei sistemisti tramite tunnel criptati con chiavi SSL;
- La trasmissione delle informazioni alle Dashboard in modo sicuro: per i server tramite tunnel crittografato ssh mentre per le workstation tramite protocollo https;
- L'utilizzo di configurazioni standard per la protezione dei sistemi operativi;
- La registrazione degli accessi effettuati,
- L'utilizzo di password amministrative complesse per assistenza e manutenzione;
- La sostituzione delle password con sufficiente frequenza,
- La verifica periodica dell'utilizzabilità delle copie mediante ripristino di prova.

Prospetto economico Protezione Dati			
		Qtà	Canone
Cloud saas 1000a	art. 1.1	1	230,00 €
			Totale 230,00 € IVA esclusa

Note: