GRUPPO FINMATICA

Alla c.a. Dott. Brambati Paolo
Spett.le
COMUNE DI LODI
PIAZZETTA BROLETTO
26900 LODI (LO)

Bologna, 23/05/2018

Prot.: ADS_PV18 944 18200425

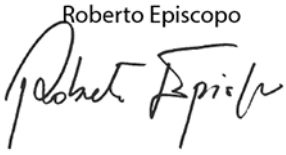
OGGETTO: Migrazione applicazioni ADS su Cloud Gruppo Finmatica

Come da accordi si fornisce offerta per quanto indicato in oggetto.

Restando a disposizione per ogni chiarimento, l'occasione è gradita per porgere i nostri migliori saluti.

ADS automated data systems S.p.A.

Roberto Episcopo



ADS

ADS Automated Data Systems S.p.A. - Via della Liberazione 15 - 40128 Bologna
Tel +39 (0)51 6307411 Fax +39 (0)51 6307498 web www.ads.it e-mail marketing@ads.it

Proposta di migrazione applicazioni ADS su Cloud Gruppo Finmatica

La soluzione proposta da ADS-Gruppo Finmatica Spa prevede la migrazione dell'intera struttura applicativa del cliente, per quanto riguarda gli ambienti software sviluppati da ADS, su di una soluzione di "Software As a Service" (SaaS) ospitata presso la struttura di cloud privato di Gruppo Finmatica Spa.

L'attività di migrazione della struttura applicativa ADS verrà effettuata tramite la configurazione di un nuovo ambiente software, equivalente a quello di produzione del cliente, su di un pool dedicato (tenant) di Virtual Machines (VMs) situato nel cloud; il nuovo "tenant" manterrà le stesse identiche funzionalità applicative dell'ambiente onsite ma, contestualmente alla migrazione, verrà aggiornato alle ultime versioni, certificate per il modo software ADS, di sistema operativo (Red Hat Enterprise Linux, CentOS Linux, Microsoft Windows Server) e middleware applicativo (Oracle DB, Apache e Apache Tomcat).

Una volta implementato, tale ambiente verrà allineato con quello di produzione mediante lo strumento proprietario di Oracle, "Database Export-Import", con due procedure distinte di import ed export dei database, attraverso connessione remota con la struttura Cloud di ADS-Gruppo Finmatica, oppure su supporto esterno rimovibile (NAS) fornito allo scopo: una iniziale per la configurazione e il test delle applicazioni in remoto ed una finale al momento dello "switch off" definitivo del vecchio ambiente applicativo su quello nuovo, situato nel cloud.

L'intera messa in opera della procedura di migrazione sarà assolutamente trasparente, senza downtime non necessari e non concordati con la controparte tecnica del cliente, ed interamente a carico di Gruppo Finmatica per le componenti HW/SW necessarie.

A migrazione avvenuta, l'accesso a tutti gli applicativi da parte degli utenti avverrà utilizzando gli stessi strumenti client impiegati nell'installazione on-premise, reindirizzati però verso un URL pubblico di accesso.

Una volta ospitata presso il cloud privato di ADS-Gruppo Finmatica, alla struttura applicativa del cliente saranno applicate tutte le policies di Backup/Disaster Recovery, Sicurezza e Monitoraggio standard previste dall'offerta e descritte nella documentazione allegata.

Contestualmente alla migrazione dell'ambiente applicativo presso il cloud privato di Gruppo Finmatica, verrà configurata una replica asincrona ("Remote Safe"), con funzionalità di Disaster Recovery, dell'ambiente stesso presso il sito originale del cliente; tale replica impiegherà le due tecnologie certificate, Standby Database e Veeam B&R, per la replica rispettivamente della componente Oracle Database e degli application server.

In alternativa a quest'ultima proposta è stata inserita, all'interno dell'offerta, una proposta alternativa di Disaster Recovery presso il sito secondario della struttura di cloud privato di Gruppo Finmatica.

Prerequisiti necessari:

Collegamento VPN tra sito cliente e struttura di cloud privato di Gruppo Finmatica per allineamento delle credenziali di accesso applicativo (AD4)

Connettività internet simmetrica, a banda larga o ultra larga, verso il cloud privato di ADS-Gruppo Finmatica

Nota:

Le attività verrà svolta interamente da remoto.

Per l'attività di migrazione saranno necessari dei downtime dei servizi applicativi che saranno concordati preventivamente con la controparte tecnica del cliente.

N.	Modulo	Descrizione	Prezzo	Prezzo a voi riservato
1	SY_CON	Configurazione Ambiente	~~5.150~~	2.150*

*Totale offerta € 5.150 **ma come da accordi € 3.000 verranno utilizzati scalando 5 gg residue (da € 600).**

Infrastruttura ICT – Cloud Privato

SITO PRIMARIO (Cloud Privato Gruppo Finmatica – Sito di Produzione)

La struttura di cloud pubblico di Gruppo Finmatica, ospitata all'interno del Data Center Telecom Italia di Bologna (BO), si basa su di un insieme di risorse hardware e software di proprietà, su piattaforma virtuale VMware vSphere, ed è comprensiva di una serie di policies di monitoraggio, alta affidabilità, Backup/DR e sicurezza, interamente gestite dal personale tecnico di Gruppo Finmatica: tali politiche garantiscono la funzionalità delle applicazioni e la disponibilità delle relative basi di dati, H24, 7 giorni su 7. Il Data Center Telecom di Bologna (Via della Centralinista, 3), in classe TIER 3, ha ottenuto il riconoscimento della conformità agli standard ISO 27001 e certifica una disponibilità di servizio maggiore o uguale a 99,995% su base annua; esso è predisposto per una connessione ad Internet attraverso linee multiple per una capacità complessiva di oltre 10 Gbit/s ed è dotato di sistemi di condizionamento, gruppi di continuità, generatori elettrici, sistemi antincendio e monitoraggio attivo 24x7.
Il Data Center è attrezzato con sistemi e procedure di:

a) *Rivelazione fumi e spegnimento incendi*
Tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso FM-200. Gli impianti garantiscono la sola disattivazione della zona oggetto dell'intervento di manutenzione. In particolare l'impianto di spegnimento è stato progettato nel pieno rispetto della normativa UNI 9795 che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente o calamità naturale ed il continuo funzionamento del resto dell'impianto.

b) *Anti allagamento*
Sono previste delle sonde di rivelazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua. Eventuali fuori uscite di acqua saranno opportunamente allontanate mediante convogliamento e scarico verso l'esterno.

c) *Anti intrusione*
E' previsto un sistema di anti intrusione integrato con l'impianto di rivelazione fumi e spegnimento incendi, con il sistema di TVCC, con il sistema di controllo accessi e con gli allarmi tecnologici.
I sensori del sistema allocati all'interno dell'edificio saranno attivati e disattivati da segnali provenienti dal sistema di controllo accessi.

d) *Telecamere a circuito chiuso*
Le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.
Il sistema TVCC sarà soggetto ad attivazione tramite "*motion detection*".

e) *Condizionamento*
Nell'area I/T sono mantenute, sia in estate sia in inverno, le seguenti condizioni ambientali:

- Temperatura 18-24° ±1 °C
- Umidità relativa: controllata (30 – 70 %)
- Ricambi d'aria pari a 0.5 volumi/ora.

f) *Continuità ed Emergenza*
Sono previsti dei gruppi di continuità (UPS) aventi batterie con autonomia di 15-20 minuti a pieno carico; tale intervallo di tempo consente l'attivazione del sistema di emergenza (costituito da 3 gruppi elettrogeni) che a sua

volta garantisce un'autonomia di almeno 36 ore e capacità di asservire tutto il complesso. Gli UPS assicurano la continuità a tutti i dispositivi informatici.

g) Controllo degli accessi fisici all'IDC

Con sorveglianza armata 24 ore su 24, procedure di registrazione degli accessi e identificazione del personale che accede in nome e per conto dei Clienti, accesso alle sale sistemi controllato elettronicamente tramite badge e sistemi di rilevamento di impronte digitali, controllo del perimetro con impianti a raggi infrarossi, test periodici di evacuazione, procedure di sicurezza con identificazione ed assegnazione di responsabilità.

La raggiungibilità degli ambienti in cloud viene garantita da una connessione remota ridondata, attraverso linee multiple, e scalabile secondo le esigenze delle piattaforme applicative dei clienti.
La gestione della sicurezza perimetrale è interamente gestita dai tecnici di Gruppo Finmatica ed è basata su apparati hardware dedicati, in alta affidabilità, in grado di attivare funzionalità di IDS (Intrusion Detection System), IPS (Intrusion Prevention System) ed Antivirus con policies personalizzate per ogni singola piattaforma ospitata.
Tutta l'infrastruttura, nel suo complesso, viene costantemente monitorata utilizzando il sistema di monitoraggio *Zabbix*, di cui il proponente è il principale partner italiano ed uno dei primi al mondo.
Tale sistema di monitoraggio, agendo sia al livello infrastrutturale che applicativo, permette al personale tecnico di Gruppo Finmatica di avere sempre a disposizione lo stato reale di utilizzo dell'infrastruttura complessiva e di quella dedicata ad ogni singolo cliente, potendo così garantire il massimo livello di servizio possibile.
Il cliente a sua volta, avrà la possibilità, tramite portale web, di verificare in tempo reale lo stato di utilizzo della propria infrastruttura informatica e ad intervalli regolari tramite l'invio di un report, gli verrà comunque comunicato il livello di utilizzo della propria infrastruttura cloud in modo da permettere un continuo equilibrio e tuning delle risorse richieste.
Il sito di Produzione del cloud privato di Gruppo Finmatica è composto da un cluster VMware vSphere HA su tre nodi ESXi ed uno storage condiviso con connettività SAN di tipo SAS-2 6 Gbps; la connessione LAN di back-end e front-end è di tipo 1 Gbps.
Il Sito Primario è costituito dalle seguenti apparecchiature principali:

Sito Primario – Componenti Hardware				
Numero	**Tipo**	**Hardware**	**Caratteristiche Principali**	**Funzione**
1	Blade System	HP BladeSystem c7000 Enclosure G3	2 x HP 6125G Blade Ethernet Switch; 2x: HP 6Gb SAS BL SAS Switch	--
3	Hypervisor Server	HP Proliant BL460c	2 x Intel Xeon E5-2680 v2 @ 2.80GHz (10 Cores); 256 GB RAM	VMware ESXi Server 6.x
1	Storage	HP MSA 2040	16 x 900 GB SAS 10k HD	Storage condiviso
1	NAS	HP StoreEasy	16 GB RAM; 12 x 4TB 7.2k NL-SAS	Backup Repository (Short Retention)

Ogni cliente ha a disposizione un pool di risorse dedicato, CPU, RAM, Storage e Network, di tipo esclusivo e non condiviso ("*Tenant*").

SITO SECONDARIO (Cloud Privato Gruppo Finmatica – Sito di Disaster Recovery)

Il Data Center utilizzato per i servizi di DR è situato a Bologna in Via della Liberazione 15 40128 Bologna ed è una struttura altamente industrializzata, dotata dei più moderni sistemi ed impianti e risorse professionali; esso è predisposto per una connessione ad Internet attraverso linee multiple per una capacità complessiva di oltre 1 Gbit/s ed è dotato di sistemi di condizionamento, sistemi antincendio e monitoraggio attivo 24x7.

La progettazione del Datacenter ha tenuto conto dell'Area di Controllo n. 11 "Sicurezza Fisica e Ambientale" della norma ISO/ISC 27002:2013 nella Sezione 11.1 "Aree Sicure", che ha come scopo quello di prevenire l'accesso fisico non autorizzato e i danni sia alle informazioni dell'organizzazione sia alle sue infrastrutture di elaborazione delle informazioni stesse.

Il Data Center è attrezzato con sistemi e procedure di:

a) Rivelazione fumi

Tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio con attivazione dei relativi impianti di spegnimento degli incendi. Gli impianti garantiscono la sola disattivazione della zona oggetto dell'intervento di manutenzione. In particolare l'impianto garantire la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente o calamità naturale ed il continuo funzionamento del resto dell'impianto.

b) Anti intrusione

E' previsto un sistema di anti intrusione ed un sistema di TVCC. Il sistema è collegato via radio ad un Sistema di Vigilanza privata incaricato ad un controllo a distanza h24 x 365 gg con intervento onsite al bisogno.

c) Telecamere a circuito chiuso

Le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.
Il sistema TVCC è sempre attivo.

d) Condizionamento

Nell'area I/T sono mantenute, sia in estate sia in inverno, le seguenti condizioni ambientali:

- Temperatura 18-24° ±1 °C
- Umidità relativa: controllata (30 – 70 %)

e) Continuità ed Emergenza

Sono previsti dei gruppi di continuità (UPS) aventi batterie con autonomia di 90-120 minuti a pieno carico. Gli UPS assicurano la continuità a tutti i dispositivi informatici.

f) Controllo degli accessi fisici all'IDC

Con sorveglianza, procedure di registrazione degli accessi e identificazione del personale che accede in nome e per conto dei Clienti, accesso alle sale sistemi controllato elettronicamente tramite badge, test periodici di evacuazione, procedure di sicurezza con identificazione ed assegnazione di responsabilità.

Il sito di Disaster Recovery del cloud privato di Gruppo Finmatica è composto da un cluster VMware vSphere HA su tre nodi ESXi ed uno storage condiviso con connettività SAN di tipo SAS-2 6 Gbps; la connessione LAN di back-end e front-end è di tipo 1 Gbps.

Il Sito Secondario, ospitato presso il sito di DR della struttura di cloud privato del Gruppo Finmatica, dispone di un'area riservata ("*Tenant*"), su piattaforma virtuale VMware vSphere, destinata alla replica di tutti i dati presenti sul sito primario, con gli strumenti precedentemente descritti.
Il Sito Secondario è costituito dalle seguenti apparecchiature principali:

Sito DR – Componenti Hardware				
Numero	**Tipo**	**Hardware**	**Caratteristiche Principali**	**Funzione**
1	Blade System	HP BladeSystem c7000 Enclosure G3	2 x HP 6125G Blade Ethernet Switch; 2x: HP 6Gb SAS BL SAS Switch	--
3	Hypervisor	HP Proliant BL460c G7	2 x Intel Xeon X56750 @ 3,07GHz (6 Cores); 192 GB RAM	VMware ESXi Server 6.x

1	Storage	NAS Synology RS2414rp+	12 x 2 TB SATA 7.2k HD	Storage condiviso
1	Dedupe Appliance	HPE StoreOnce 3540	15,5 TB Spazio Disco RAW	Backup Repository (Long Retention)

Il Sito secondario ha funzione di Disaster Recovery del primario e pertanto replica a livello di funzionalità l'intera infrastruttura hardware e software disponibile nel sito primario anche se la capacità elaborativa è dimensionata a circa il 50-60% di quella del sito primario.

Networking

Connettività WAN

La pubblicazione dei servizi avviene tramite IP pubblici della rete Telecom su cui sono stati attivati i seguenti accorgimenti di sicurezza:

- Utilizzo di *NameVirtualHost* su un Reverse Proxy
- Utilizzo di un certificato SSL wildcard **.e-pal.it* per i servizi in protocollo HTTPS

In particolare, tutti i servizi pubblicati ai clienti sono host del dominio *.e-pal.it*, la suddivisione per applicativo viene gestita tramite percorso (/gps, /tr4web, ecc.): in caso di accesso protetto viene sempre utilizzato il certificato wildcard **.e-pal.it* che permette di non avere warning per tutti i sottodomini di *e-pal.it*.

Sulla componente network di frontend riservata ai clienti presso la struttura di cloud privato di Gruppo Finmatica sono presenti due Proxy/Firewall *FortiGate* in cluster "*Active-Passive*" e due Reverse Proxy (CentOS Linux 6.9, Apache 2.2) in modalità "*Active-Passive*" con configurazione sincronizzata e load balancing gestito direttamente dagli apparati *FortiGate 100D* con check su pagina web statica sui server.

Tutti i "*virtual host*" sono posizionati sul medesimo Reverse Proxy e da quest'ultimo sono aperte verso la VLAN interna riservata alle VM del cliente solo ed esclusivamente le porte necessarie per l'accesso agli applicativi *Apache Tomcat*.

A livello di DNS i server sono pubblicati direttamente con il loro IP pubblico mentre, per consentire ai client l'accesso diretto tramite la VPN "*site-to-site*", la zona DNS viene direttamente risolta ed instradata sull'IP privato del reverse proxy all'interno VLAN riservata.

Alcuni applicativi client-server richiedono di essere eseguiti in un ambiente Remote Desktop, anche in questo caso si è centralizzato il punto di accesso in un unico server *Remote Desktop Gateway* che incapsuli il traffico RDP in HTTPS e permetta di presentare all'utente una pagina web di scelta degli applicativi a lui assegnati.

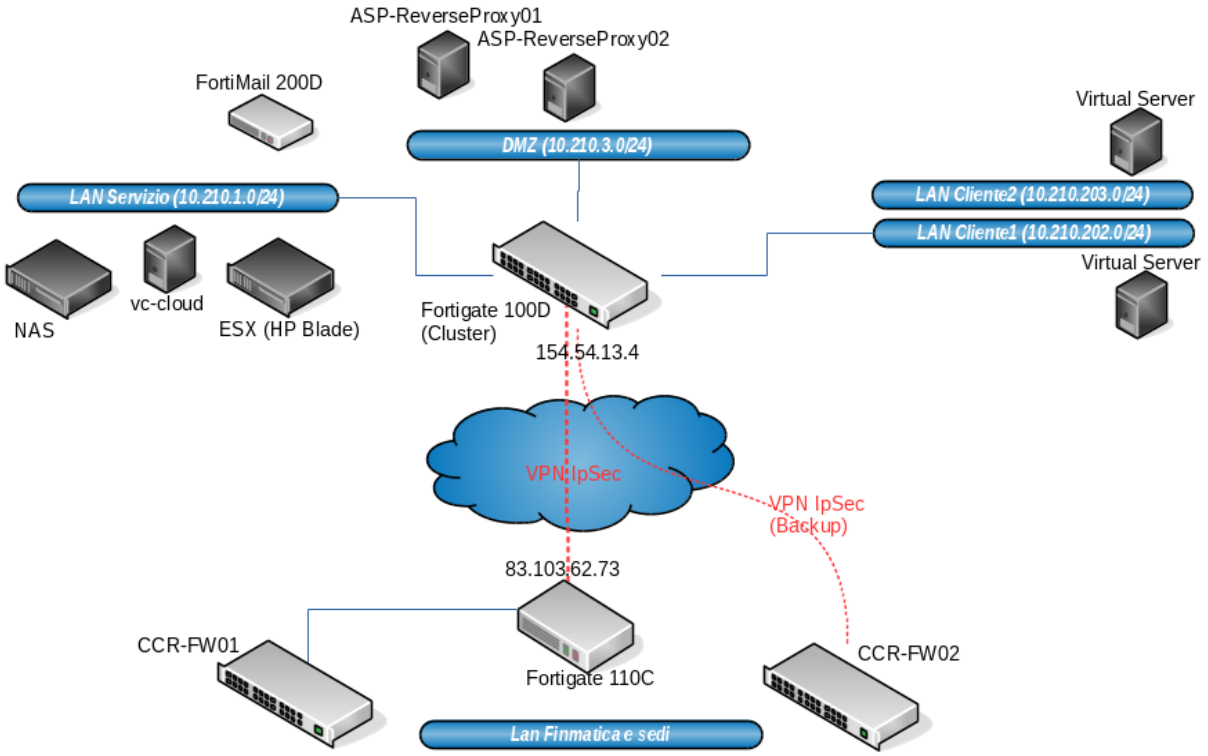
Non sono attualmente presenti filtri per il traffico interno alla VPN dalla rete LAN del cliente verso la VLAN a loro assegnata (e in direzione opposta): questi filtri sul traffico di rete sono direttamente gestiti dall'apparato firewall del cliente.

Connettività LAN

La connettività di backend dell'infrastruttura di cloud pubblico di Gruppo Finmatica è basata su di una serie di subnet a 24 bit delle classi 10.210.x.x (vedi schema di rete).
Tali reti sono suddivise principalmente in "*LAN Servizio*", "*DMZ*" e "*LAN Cliente(n)*", segmentate (ed eventualmente ruotate – vedi tabella "*Routing Policies*") sia a livello di indirizzamento IP che di tag VLAN (*IEEE 802.1Q*) mediante gli apparati *FortiGate 100D* in cluster.

Connettività VPN

L'infrastruttura di cloud pubblico è connessa alla sede principale di Gruppo Finmatica di Via della Liberazione 15 – Bologna (BO), mediante una MAN su linea FTTH dedicata Layer 2 con banda 1 Gbps garantita.



Distanze e Connettività	
Distanza Sito di Produzione – Sito di DR (in Km)	7,2 Km di percorrenza - 4,7 Km in linea d'aria
Connessione Sito di Produzione – Sito di DR (in Km)	FTTH dedicata - 1 Gbps di banda garantita
Connessione Sito di DR - Sedi periferiche	Connessione con sedi Gruppo Finmatica: Legnano → VPN "*Site to Site*" su FTTH dedicata + FTTC Internet Catanzaro → VPN "*Site to Site*" su FTTC internet ridondata Catania → MPLS su FC + FTTC Internet

Monitoring

Tutta l'infrastruttura, nel suo complesso, viene costantemente monitorata utilizzando il sistema di monitoraggio *Zabbix®*, di cui ADS-gruppo Finmatica è il principale partner certificato italiano e tra i maggiori europei.

In questo modo i tecnici di ADS avranno sempre a disposizione lo stato reale di utilizzo dell'infrastruttura complessiva e di quella dedicata ad ogni singolo cliente, potendo così garantire il massimo livello di servizio possibile.

Il cliente a sua volta, avrà la possibilità, tramite portale, di verificare in tempo reale lo stato di utilizzo della propria infrastruttura informatica, ricavandone anche tutti i parametri di utilizzo per poter costantemente fare raffronti di mercato o organizzare gare di appalto successive.

Ad intervalli regolari, verrà comunque comunicato al cliente, tramite l'invio di un report, il livello di utilizzo della propria infrastruttura cloud in modo da permettere un continuo equilibrio delle risorse richieste.

Backup/DR Policies
Backup Policies

Per il Backup/DR degli ambienti cloud dei clienti ospitate presso il proprio cloud pubblico, ADS si affida alle consolidate tecnologie proprietarie di Oracle, RMAN, Export e Standby Database, in combinazione con la piattaforma software, attualmente leader di mercato per la "Data Availability" degli ambienti virtuali, Veeam Backup & Replication.
Le policies standard applicate prevedono un backup giornaliero, on site, di tutti gli ambienti su di un supporto disco ("disk-to-disk") dedicato e non condiviso, per garantire la riservatezza del dato anche all'interno del supporto di backup.
Nello specifico, le componenti DBMS, le più critiche dell'intera soluzione software, verranno sottoposte a due tipologie diverse di backup, di tipo "Logico" e "Fisico", mentre le due componenti, Application e Reverse Proxy server, non contenendo al loro interno nessun dato critico, beneficeranno di un'unica tipologia di backup, quella "Full VM", che prevede comunque il salvataggio, Full ed incrementale, dell'intera virtual machine.
Ai file di backup dei DBMS Oracle e delle altre VMs viene applicata un'ulteriore policy di sicurezza che prevede un'archiviazione di lungo periodo "off site": tale policy prevede una replica di questi file su di un supporto disco criptato ospitato presso la sede di Gruppo Finmatica a Bologna (BO), sito alternativo a quello di backup primario.
L'algoritmo utilizzato su tale supporto è di tipo "*Advanced Encryption Standard*", AES-256, con "chiave" di criptazione residente in locale e sottoposta anch'essa a policy di backup e sicurezza.
La connessione tra i due siti avviene mediante una connessione VPN dedicata di tipo "Site-to-Site", con protocollo IPSEC ed in nessun caso, durante le due fasi di backup e archiviazione, neanche in maniera temporanea, i dati dei clienti vengono posizionati geograficamente al di fuori del territorio italiano. Tutte e due le dislocazioni dei dati, sito primario e sito di archiviazione, sono accessibili e visitabili, previa richiesta scritta ed organizzazione preventiva per motivi di sicurezza.

DBMS Oracle (Backup Logico) - Export DB

Con schedulazione giornaliera, in orario notturno, viene eseguito un "Database Dump" logico del database contenente tutte le informazioni necessarie al ripristino della struttura dati, nonché dei dati in essa contenuta dell'intero DBMS. Questa tipologia di backup permette un ripristino logico del dato, dalla tabella fino all'intero database, con una granularità a livello di singolo utente Oracle e può essere effettuato direttamente sul database di produzione, piuttosto che su di un database di appoggio/test, prelevando dal database dump solamente i record necessari all'operazione.
L'export dei dati viene eseguito tramite script batch schedulati sul sistema operativo della macchina DBMS e la dislocazione, per motivi di sicurezza, risulta esterna allo storage di produzione in modo da garantire sempre la presenza del dump e la sua disponibilità in caso di necessità di ripristino.
La retention applicata è di una settimana, in modo da garantire la presenza contemporanea di tutti gli ultimi 7 dump eseguiti.
Vengono inoltre archiviati "off site" gli export (dump) relativi alle ultime 4 settimane (settimanali), così come gli ultimi 12 mensili per rendere possibile un ripristino di dati con profondità annuale.
L'integrità degli export viene verificata tramite script di "Import Show" ad ogni esecuzione del job.

RPO (Recovery Point Objective) Massimo: 24 Ore

RTO (Recovery Time Objective) Medio: 30 Minuti

DBMS Oracle (Backup Fisico) - RMAN

Tramite l'utility Oracle Recovery Manager – RMAN – viene impostato un backup fisico del DBMS.
Tali backup set vengono anch'essi storicizzati su storage differente da quello di produzione, permettendo in qualsiasi momento, oltre alle normali operazioni di restore, anche eventuali funzionalità di replica e/o duplicazione del database su di un ambiente differente da quello di produzione.
La schedulazione standard dei job di RMAN, prevede dei backup full settimanali (sabato pomeriggio, ore 14) con incrementali ogni 2 ore, dalle 7 alle 19, dal lunedì al venerdì, e dalle 7 alle 13 del sabato.
L'integrità dei backup RMAN viene verificata tramite il comando di "Verificate Backup" ad ogni esecuzione del job.
RPO (Recovery Point Objective) Massimo: 120 Minuti

RTO (Recovery Time Objective) Medio: 120 Minuti

Application/Proxy Server – Veeam B&R

Tramite il sistema di backup Veeam Backup & Replication vengono eseguiti i job di backup degli Application e dei Proxy Server virtuali. La schedulazione dei backup job prevede un backup Full mensile con incrementali settimanali (domenica) ed una retention di 4 settimane; vengono inoltre conservati "off site" gli ultimi 12 backup mensili.
L'integrità dei backup viene verificata dagli strumenti proprietari di Veeam B&R (Backup Maintenance) con frequenza settimanale.
RPO (Recovery Point Objective) Massimo: 7 Giorni

RTO (Recovery Time Objective) Medio: 5-10 Minuti

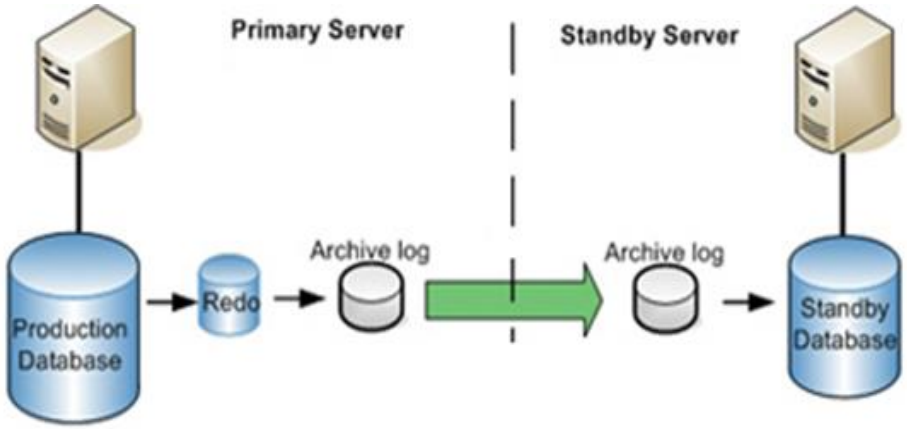
Anche l'esecuzione dei job di backup, sia Oracle che Veeam B&R, è sottoposto interamente al sistema di monitoraggio interno per il controllo dell'esecuzione dei job schedulati, con l'invio di report periodici al cliente sullo stato delle policies applicate.

Replication Policies

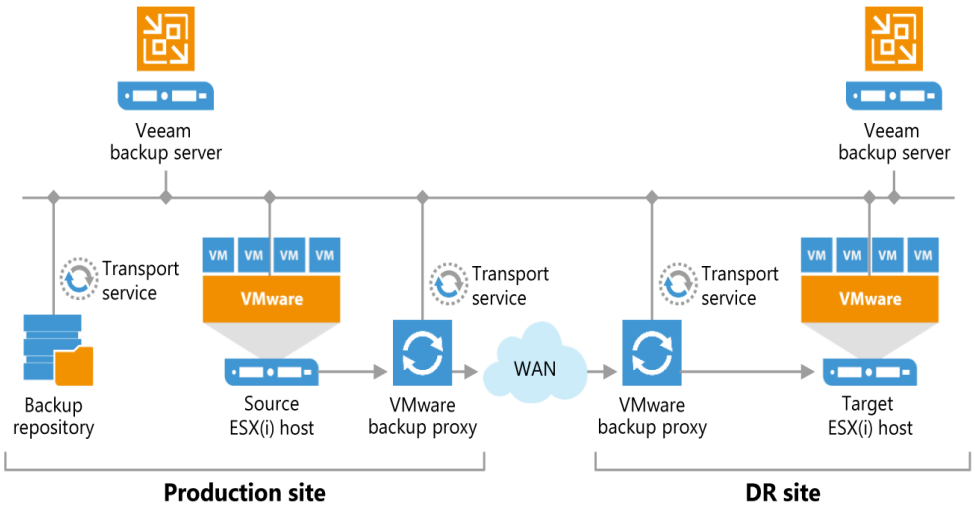
Per la replica dei dati e delle macchine virtuali dal sito primario sul sito secondario si utilizza una combinazione delle tecnologie proprietarie di Oracle, lo "*Standby Database*", e la funzionalità di replica di Veeam Backup & Replication, l'attuale piattaforma di riferimento per il backup e il disaster recovery del mondo virtuale.
L'allineamento delle due piattaforme Oracle Database viene eseguito ogni ora, garantendo quindi un RPO minimo di 60 Minuti, mentre, per ciò che riguarda le repliche delle componenti Application Server, esse vengono eseguite ogni 12 ore garantendo quindi un RPO ufficiale di pari entità ma, non interessando nello specifico nessuna base di dati,

Area	Tecnologia	Recovery Point Objective (RPO)	Connessione Primary→DR	Encryption	Recovery Time Object (RTO) - Massimo
DB Server Oracle	Standby Database	60 Minuti	VPN "Site-to site"	AES – 128 bit	12 Ore
Application Servers	Veeam B&R Replication Job	12 Ore	VPN "Site-to site"	AES – 128 bit	12 Ore

Il collegamento tra il sito primario e il sito secondario è di tipo simmetrico su FTTH dedicata ad 1 Gbps e linea dedicata di tipo "Layer 2".



Oracle Standby Database



Veeam B&R Replication Job

Servizi di Cloud Computing - Allegato IaaS (Infrastructure as a Service)

Il servizio di IaaS (Infrastructure as a Service) prevede l'utilizzo da parte del Cliente, tramite la rete Internet, dell'infrastruttura di server e apparati virtuali creata su hardware dislocato nella server farm della Società. La Server Farm della Società è situata all'interno di Datacenter dislocati in territorio Italiano e conformi agli standard ISO 27001.

Il Servizio IaaS comprende:

- la creazione iniziale dei server/apparati virtuali
- l'utilizzo delle risorse (server / apparati) messe a disposizione dalla Società presso la propria server farm;
- il supporto sistemistico sull'infrastruttura di virtualizzazione

Il servizio , non comprende:

- la fornitura e installazione di hardware e software di base presso la sede del Cliente;
- le licenze d'uso del software di base, di sistemi operativi, di software applicativo , loro aggiornamenti e servizi relativi;
- gli oneri relativi alla connettività dalle postazioni utente del Cliente alla server farm della Società.

Prerequisiti

Il servizio potrà essere attivato a condizione che il Cliente disponga di un collegamento Internet a Banda Larga.

Struttura generale del Data Center

Il Data Center proposto per i servizi Cloud ha ottenuto il riconoscimento della conformità agli standard ISO 27001, che costituisce, a tutt'oggi, il principale standard internazionale che certifica la capacità di garantire la sicurezza del proprio patrimonio informativo (dei sistemi e delle reti) o di quello che altre aziende o organizzazioni le hanno affidato in gestione.

Il Data Center è situato a Bologna ed è una struttura altamente industrializzata, dotata dei più moderni sistemi, impianti e risorse professionali; esso è predisposto per una connessione ad Internet attraverso linee multiple per una capacità complessiva di oltre 10 Gbit/s ed è dotato di sistemi di condizionamento, gruppi di continuità, generatori elettrici, sistemi antincendio e monitoraggio attivo 24x7. Il Data Center è attrezzato con sistemi e procedure sottoindicate:

Rilevazione fumi e spegnimento incendi

Tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso FM-200. Gli impianti garantiscono la sola disattivazione della zona oggetto dell'intervento di manutenzione. In particolare l'impianto di spegnimento è stato progettato nel pieno rispetto della normativa UNI 9795 che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente o calamità naturale ed il continuo funzionamento del resto dell'impianto.

Anti allagamento

Sono previste delle sonde di rivelazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua. Eventuali fuori uscite di acqua saranno opportunamente allontanate mediante convogliamento e scarico verso l'esterno.

Anti intrusione

E' previsto un sistema di anti intrusione integrato con l'impianto di rivelazione fumi e spegnimento incendi, con il sistema di TVCC, con il sistema di controllo accessi e con gli allarmi tecnologici.

I sensori del sistema allocati all'interno dell'edificio saranno attivati e disattivati da segnali provenienti dal sistema di controllo accessi.

Telecamere a circuito chiuso

Le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche. Il sistema TVCC sarà soggetto ad attivazione tramite "motion detection".

Condizionamento

Nell'area I/T sono mantenute, sia in estate sia in inverno, le seguenti condizioni ambientali:

- Temperatura 18-24° ±1 °C

- Umidità relativa: controllata (30 – 70 %)

- Ricambi d'aria pari a 0.5 volumi/ora.

Continuità ed Emergenza

Sono previsti dei gruppi di continuità (UPS) aventi batterie con autonomia di 15-20 minuti a pieno carico; tale intervallo di tempo consente l'attivazione del sistema di emergenza (costituito da 3 gruppi elettrogeni) che a sua volta garantisce un'autonomia di almeno 36 ore e capacità di asservire tutto il complesso. Gli UPS assicurano la continuità a tutti i dispositivi informatici.

Controllo degli accessi fisici all'IDC

Con sorveglianza armata 24 ore su 24, procedure di registrazione degli accessi e identificazione del personale che accede in nome e per conto dei Clienti, accesso alle sale sistemi controllato elettronicamente tramite badge e sistemi di rilevamento di impronte digitali, controllo del perimetro con impianti a raggi infrarossi, test periodici di evacuazione, procedure di sicurezza con identificazione ed assegnazione di responsabilità.

Le tecnologie

H.P. La parte computazionale e di storage del Data Center, così come le interconnessioni di rete, sono realizzate utilizzando materiale del brand HP leader di mercato per queste soluzioni.

I Server sono strutturati su tecnologia Blade in modo da permettere un ulteriore ottimizzazione delle economie di scala, mentre gli storage permettono la differenziazione in livelli di servizio grazie alla possibilità di utilizzare tecnologie SAS o SATA a seconda delle necessità.

Tutti i sistemi sono ridondati in modo da garantire un alta affidabilità di servizio costante, con servizi di assistenza effettuati e garantiti dal brand produttore stesso.

VMware vSphere 6

L'ottimizzazione dei sistemi è assicurata da layer di virtualizzazione leader di mercato, VMware vSphere in versione 6.x, in grado di garantire l'affidabilità e la massima compatibilità necessaria a servizi Cloud.

Tutti i partner tecnologici che offrono da tempo consulenza e realizzazioni in ambito di efficientamento delle infrastrutture informatiche e migrazione al Cloud, devono avere approfondita conoscenza di questo prodotto ormai divenuto fondamentale per disaccoppiare l'hardware dalle applicazioni, permettendo il raggruppamento e l'ottimizzazione delle risorse IT in pool logici di server, storage e di rete.

L'implementazione di infrastrutture virtuali VMware vSphere 6.x, su un qualsiasi numero di nodi, ha l'obiettivo di consolidare su un'unica piattaforma tutto il sistema informativo del cliente, attivando contestualmente servizi di Disaster Recovery in Cloud sia di Backup che di Replica, in modo da garantire sempre la Continuità Operativa richiesta dal C.A.D.

Al suo interno il Gruppo Finmatica racchiude tecnici certificati di livello VCP6 per la realizzazione di infrastrutture virtuali e tecnici VSP6 e VTSP6 specializzati nel disegno e nella progettazione delle infrastrutture stesse.

Veeam Backup & Replication in versione Enterprise

La soluzione Veeam garantisce elevate prestazioni e funzionalità relativamente alla gestione dei backup di infrastrutture virtuali.

Veeam è uno strumento che garantisce:

Software di backup progettato appositamente per ambienti virtuali in grado di effettuare il backup delle macchine virtuali senza bloccarne il funzionamento

Protezione priva di agenti, quindi con minor impatto configurativo

Garanzia di approccio multilivello per la protezione del dato

Riduzione dei tempi di backup tramite deduplica

Il software Veeam è principalmente composto dalla tecnologia vPower, che consente di eseguire una macchina virtuale (VM) direttamente da un file di backup compresso e deduplicato su un comune storage di backup.

Fortigate

La gestione di tutta la sicurezza perimetrale viene demandata ad apparati FortiGate in grado di attivare funzionalità di IDS (Intrusion Detection System), IPS (Intrusion Prevention System), Antivirus in configurazione di alta affidabilità.

Ogni singolo cliente verrà dedicato ad un corrispondente Virtual DOMain (VDOM) dell'infrastruttura FortiGate, in modo da garantire il massimo livello di isolamento e protezione del dato, mantenendo sempre alto il livello di sicurezza informatica fornita.

Zabbix

Tutta l'infrastruttura, nel suo complesso, viene costantemente monitorata utilizzando il sistema di monitoraggio Zabbix. In questo modo i tecnici del Gruppo Finmatica avranno sempre a disposizione lo stato reale di utilizzo dell'infrastruttura complessiva e di quella dedicata ad ogni singolo cliente, potendo così garantire il massimo livello di servizio possibile.

Il cliente a sua volta, avrà la possibilità, tramite portale, di verificare in tempo reale lo stato di utilizzo della propria infrastruttura informatica, ricavandone anche tutti i parametri di utilizzo per poter costantemente fare raffronti di mercato o organizzare gare di appalto successive.

Ad intervalli regolari, verrà comunque comunicato al cliente, tramite l'invio di un report, il livello di utilizzo della propria infrastruttura cloud in modo da permettere un continuo ricalibramento delle risorse richieste.

Citrix

Citrix con XenAPP è la piattaforma di riferimento per la remotizzazione delle applicazioni. Tramite questi strumenti è possibile, ottimizzando anche la banda, remotizzare qualsiasi applicazione – anche client/server – permettendo così di migrare in cloud qualsiasi applicazione di qualsiasi fornitore software.

Configurazione a disposizione del Cliente

Viene di seguito riportata la configurazione resa disponibile al Cliente:

SERVER	VCPU	GB Ram	GB spazio disco	GB spazio disco alte performance
DB SERVER	4	8	60+120	0
APPLICATION SERVER (Tomcat)	2	4	50 GB	0
APPLICATION SERVER (Tomcat)	2	4	50 GB	0
APPLICATION SERVER (Tomcat)	2	4	50 GB	0
APPLICATION SERVER (Tomcat)	2	4	250 GB	0
APPLICATION SERVER (Forms11)	2	4	60 GB	0

SPAZIO DISCO PER I BACKUP	GB
Spazio disco destinazione Spazio disco destinazione per archiviazione backup	1110

Nel periodo di copertura contrattuale, nel caso il Cliente avesse esigenze aggiuntive, sarà possibile rimodulare tale configurazione. Le eventuali implementazioni saranno oggetto di valutazione tecnica ed economica successiva.

SLA sulla disponibilità dei servizi di infrastruttura

Il servizio standard è erogato secondo uno SLA per l'uptime annuale (1) dal valore minimo del 99%.

I tempi di indisponibilità del servizio sono considerati come downtime e sono calcolati a partire dalla segnalazione da parte del cliente fino alla nuova disponibilità:

- Uptime del Data Center del 99,99% (presidio degli impianti con copertura h24 365 giorni annui)
- Uptime dei Server del 99% (sistema di controllo con reperibilità con copertura h24 365 giorni annui)

E' possibile aumentare il valore dello SLA con servizi supplementari

Non rientrano nei conteggi dello SLA i seguenti casi:

- Manutenzione preavvisata del datacenter o dei Server.
- Tempi di inattività causata da catastrofi
- Tempi di inattività causata da attacchi DDoS

(1) Tabella di Uptime Annuale: 99.99% sono 53 minuti; 99.9% sono 9 ore; 99.5% sono 2 giorni; 99% sono 4 giorni

Durata e rinnovo

Il servizio di IaaS ha la durata indicata in tabella e non sarà rinnovato tacitamente. **Tre mesi** prima della scadenza contrattuale la Società provvederà a proporre al Cliente una offerta di rinnovo. È espressamente stabilito che, in mancanza di tempestiva accettazione, verrà disattivata la disponibilità del Servizio IaaS alle ore 24.00 dell'ultimo giorno di durata contrattuale. Resta inteso che nessun intervento o prestazione, di nessuna natura, sarà dovuto dopo la data di scadenza.

Restituzione dei dati

Immediatamente prima di disattivare il servizio e sempre che il Cliente lo abbia richiesto con **trenta giorni** di anticipo sulla data di scadenza, originaria o prorogata, del contratto, l'Azienda provvederà a rendere disponibili al Cliente, per un tempo non superiore a trenta giorni dalla scadenza dello stesso, i dati immessi nel sistema durante il periodo di durata contrattuale.

In caso di mancata tempestiva comunicazione in forma scritta di questa richiesta, il Servizio IaaS verrà disabilitato senza necessità di alcuna ulteriore comunicazione e senza alcun salvataggio dei dati su supporto ottico.

Pubblicazione dati su WEB

Laddove il Cliente richiedesse alla Società la pubblicazione di dati sul WEB, attivando un link dal proprio sito istituzionale ad un sito presente nella server farm della Società, esso sarà responsabile della predisposizione e dell'aggiornamento dei propri dati ed informazioni che verranno pubblicati sul server Web della Società .

La Società non è responsabile:

- dell'eventuale uso illecito che il Cliente potrà fare sia del servizio sia delle informazioni reperite o fornite attraverso il servizio stesso;
- dei danni eventuali che il Cliente potrebbe causare a terzi con l'uso anche lecito del servizio;
- dei danni provocati dall'errato o mancato funzionamento del servizio né delle rivendicazioni di terze parti nei riguardi del Cliente.

Il Cliente inoltre dichiara:

- che nessun dato inserito conterrà informazioni diffamatorie, riservate, esclusive, trafugate o false di qualsiasi tipo;
- di accettare che nessun dato o informazione inserita sia considerato un segreto industriale;
- di avere sui dati inseriti tutti i titoli per disporne la diffusione e ogni altro utilizzo;
- che nessun dato conterrà sistemi di protezione, virus et simili
- che possano alterare il regolare funzionamento del sistema Web dell'Azienda.

Responsabilità

La Società non sarà in ogni caso responsabile per ritardi, malfunzionamenti e/o interruzioni nell'erogazione del Servizio causati da:

(a) forza maggiore (eventi catastrofici, attacchi DDoS contro la rete, etc.),

(b) malfunzionamento hardware o software dei terminali utilizzati dal Cliente,

(c) interruzione totale (dorsali di collegamento) o parziale del servizio di accesso locale o di terminazione fornito dall'operatore di telecomunicazioni.

Servizi di Cloud Computing - Allegato PaaS) Utilizzo del Cloud come Platform as a Service

Oggetto del servizio è l'utilizzo da parte del Cliente, tramite la rete Internet, dell'infrastruttura di server ed apparati virtuali, l'utilizzo delle componenti software di base e servizi di monitoraggio del sistema creato su hardware dislocato nella server farm della Società La Server Farm è situata all'interno di Datacenter dislocati in territorio Italiano e conformi agli standard ISO 27001.

In particolare il canone comprende:

- Servizio IaaS) Utilizzo del Cloud come Infrastructure as a Service, la cui descrizione è indicata nell'allegato IAAS, parte integrante del servizio PaaS, il canone del servizio è compreso nel servizio PaaS
- il diritto all'utilizzo delle componenti software di base necessarie e loro aggiornamenti;
- Il servizio "SY – RBK Backup degli archivi e dell'infrastruttura virtuale in conformità con il Recovery Point Objective (RPO);
- I seguenti servizi sistemistici la cui descrizione dettagliata e modalità di erogazione sono indicati nell'Allegato SS:
  - ✓ SY_ GDB Supporto Specialistico sui Database . Servizio di supporto Database Administrator
  - ✓ NETPRACK - Servizio di Proactive Monitoring dell'infrastruttura
  - ✓ NETBUPC0 Servizio di Back Up Log Control - Controllo giornaliero dei log;
  - ✓ NETACCO – Access Control Controllo dei tentativi di intrusione e raccolta accessi come amministratore di sistema.
  - ✓ SY_PLS Assistenza sistemistica avanzata alle Infrastrutture. Servizio di supporto all'infrastruttura virtuale implementata

Il canone, non comprende:

- la fornitura di software applicativo,
- i servizi di assistenza, aggiornamento, manutenzione e formazione agli applicativi;
- il servizio di supporto sistemistico agli applicativi
- gli oneri relativi ai collegamenti delle postazioni utente del Cliente alla server farm della Società;
- la eventuale fornitura e installazione di hardware e software di base presso la sede del Cliente.

Licenza d'uso temporanea Software di base.

Il software di base, che viene utilizzato dal Cliente a fronte del canone di servizio, si intende messo a disposizione a titolo di licenza d'uso temporanea. Il periodo di validità della licenza si intende coincidente con il periodo di validità del canone: al termine del periodo di validità del canone, il Cliente non vanterà alcun diritto sull'utilizzo successivo dell'applicativo.

- Limitazioni d'uso.

È fatto divieto al Cliente di cedere a sua volta in licenza d'uso, dare in affitto, vendere , trasferire, distribuire o rendere in qualsiasi altra forma disponibile ad altri il software oggetto del contratto sia a titolo gratuito che oneroso.

E' fatto divieto al cliente di copiare in tutto o in parte le procedure ed i programmi oggetto del presente contratto sia in forma stampata che in forma leggibile dall'elaboratore fatta eccezione del diritto di effettuare copie di back-up o archivio riproducendo su di esse tutti i contrassegni e gli avvisi presenti sugli originali.

È fatto divieto al cliente di tradurre, modificare, incorporare in tutto o in parte in altre procedure o programmi, disassemblare, alterare o creare utility basate sul software o su qualsiasi parte in esso contenuta. Il Cliente non potrà modificare la struttura del software né chiedere a terzi di effettuare la modificazione predetta così da mutare le funzionalità del software.

Nel caso di mancata osservanza di questi termini, l'accordo cesserà automaticamente senza alcun preavviso.

- Proprietà Intellettuale ed Industriale.

La Società garantisce di avere la facoltà di cedere al cliente le licenze d'uso oggetto del presente contratto e garantisce altresì di avere il diritto di disporre di programmi, dispositivi e di soluzioni tecniche che possano essere utilizzati nella esecuzione del contratto.

Tutti i diritti di proprietà anche intellettuale, di autore, di brevetto e di invenzione industriale sui Prodotti oggetto del presente contratto non sono in alcun modo modificabili o cancellabili dal cliente.

I programmi rimangono di proprietà esclusiva della Società.

Durata e rinnovo

Il servizio PaaS ha la durata indicata in tabella e non sarà rinnovato tacitamente.

Tre mesi prima della scadenza contrattuale la Società provvederà a proporre al Cliente una offerta di rinnovo.

È espressamente stabilito che, in mancanza di tempestiva accettazione, verrà disattivata la disponibilità del Servizio PaaS alle ore 24.00 dell'ultimo giorno di durata contrattuale. Resta inteso che nessun intervento o prestazione, di nessuna natura, sarà dovuto dopo la data di scadenza.

Restituzione dei dati

Immediatamente prima di disattivare il servizio e sempre che il Cliente lo abbia richiesto con trenta giorni di anticipo sulla data di scadenza, originaria o prorogata, del contratto, la Società provvederà a rendere disponibili al Cliente, per un tempo non superiore a trenta giorni dalla scadenza dello stesso, i dati immessi nel sistema durante il periodo di durata contrattuale.

In caso di mancata tempestiva comunicazione in forma scritta di questa richiesta, il Servizio PaaS verrà disabilitato senza necessità di alcuna ulteriore comunicazione e senza alcun salvataggio dei dati su supporto ottico.

Responsabilità

La Società non sarà in ogni caso responsabile per ritardi, malfunzionamenti e/o interruzioni nell'erogazione del Servizio causati da:

(a) forza maggiore (eventi catastrofici, attacchi DDoS contro la rete, etc.),

(b) malfunzionamento hardware o software dei terminali utilizzati dal Cliente,

(c) interruzione totale (dorsale di collegamento) o parziale del servizio di accesso locale o di terminazione fornito dall'operatore di telecomunicazioni.

Rinvii

Per tutto quanto non previsto e non in opposizione valgono le Norme e Condizioni Generali allegate:

Servizio IaaS) Infrastructure as a Service

Servizio SS) Supporto Sistemistico

Prezzo del servizio

Per usufruire del servizio il Cliente dovrà corrispondere alla Società un canone, il cui importo viene di seguito riportato.

Cordice	Descrizione	Peiodo	Prezzo	Prezzo a Voi riservato
SY_PAAS	Servizio di Platform as a Service (con DR su infrastruttura Gruppo Finmatica)	01/07/2018- 30/06/2019	~~14.108~~	**11.768***

*Il prezzo per il servizio PaaS viene fissato in un canone annuale pari a € 14.108 **ma in virtù del fatto che nel contratto GOLD in essere sono già compresi alcuni servizi sistemisti necessari al servizio PAAS, al valore del canone annuale (sopra indicato) va decurtato l'importo di € 2.340**.

Condizioni di fornitura

Tempi di consegna e validità dell'offerta

La presente offerta ha una validità di 30 giorni.

Per l'accettazione dell'offerta è condizione necessaria che la presente ritorni all'Azienda debitamente sottoscritta in tutte le sue parti ed allegati entro il periodo di validità. In mancanza, qualora dovesse pervenire l'accettazione della presente con diverse modalità, le clausole della presente offerta e di tutti i contratti allegati si intenderanno tutte, nessuna esclusa, concordate ed accettate dal Cliente.

Tempi di consegna

I tempi di consegna per la realizzazione di quanto offerto verranno con Voi in seguito concordati; si ipotizza comunque la consegna entro 90 giorni dall'ordine.

Pagamenti e Fatturazione

Il pagamento dovrà essere effettuato entro "30 giorni data fattura" dalle singole fatture, che verranno emesse alla data di consegna delle singole personalizzazioni. In caso di ritardati pagamenti verranno applicate le disposizioni di cui al D.Lgs. 231/2002 e successive modificazioni.

Responsabilità

L'Azienda non assume alcuna obbligazione oltre a quelle previste dal presente contratto e, salvo il caso di dolo o colpa grave, non assume alcuna responsabilità per i danni di qualsiasi natura comunque sofferti dal Cliente in relazione all'oggetto del presente contratto o alle prestazioni previste nello stesso. La Responsabilità dell'Azienda non può essere superiore al valore della fase cui si riferisce.

Disposizioni generali

Contestazioni. Qualunque contestazione sulle prestazioni effettuate dall'Azienda deve, a pena di nullità, essere effettuata in forma scritta entro dieci giorni dalla consegna del prodotto o dalla erogazione del servizio.
Estensioni. Tutto quanto qui convenuto si applica, in quanto compatibile, anche alle prestazioni extracontrattuali.
Adempimenti in tema di tracciabilità finanziaria - Legge 136/2010. L'Azienda si obbliga ad osservare le disposizioni contenute nell'art. 3 della legge n. 136/2010 e successive modifiche o integrazioni in materia di tracciabilità dei flussi finanziari. L'Azienda si obbliga altresì ad inserire nei contratti sottoscritti con i sub appaltatori e i sub contraenti apposita clausola con la quale ciascuna delle parti si assume gli obblighi previsti dall'art. 3 della Legge n. 136/2010 e successive modifiche e integrazioni. L'Azienda si impegna a dare immediata comunicazione al Cliente della notizia dell'inadempimento della propria controparte (sub appaltatore - sub contraente) agli obblighi di tracciabilità finanziaria. Ai sensi dell'art. 3 comma 9 bis della Legge n. 136/2010, il presente contratto si risolve automaticamente di diritto nel caso di violazione degli obblighi in materia di tracciabilità.
Costi della sicurezza. Il prezzo della fornitura è comprensivo dei costi della sicurezza afferenti all'esercizio dell'attività svolta dall'impresa. I costi che l'Azienda sostiene per gli adempimenti di cui al DLgs. .81/2008 e succ. modificazioni corrispondono allo 0,5% del valore del corrispettivo.

Privacy e Consenso al Trattamento dei Dati

Le parti potranno, nel corso dello svolgimento del contratto, avere accesso a dati e ad informazioni ad esso connessi e si impegna ad utilizzarli esclusivamente ai fini del raggiungimento degli obiettivi dell'incarico, nonché a mantenere riservate le informazioni di cui potranno venire a conoscenza nel rispetto della vigente normativa sulla privacy (D.Lgs. 196/03).

Il Cliente presta il consenso al trattamento dei dati da parte dell'Azienda, ai sensi delle vigenti disposizioni in materia di trattamento dei dati personali, per le finalità connesse all'esecuzione del presente contratto.

Subappalto

L'Azienda, nell'ambito dell'intera fornitura, può eventualmente subappaltare a terzi o ad aziende del Gruppo Finmatica, i servizi indicati in offerta, nel rispetto dell'art. 118 del D.lgs. 163/2006 e s.m.i.

Rimane comunque invariata la responsabilità del fornitore contraente, il quale continuerà a rispondere di tutti gli obblighi contrattuali.

Competenza

In caso di controversia sarà competente esclusivamente il Foro di Bologna.

Rinvii

Per tutto quanto non previsto e non in opposizione si rimanda quale parte integrante all'offerta, alle norme e condizioni generali del Contratto di Licenza d'uso del software applicativo allegato .

Firma del Cliente

_____

Firma dell'Azienda

_____

CLAUSOLE DI SPECIFICA APPROVAZIONE

Agli effetti degli articoli 1341 e 1342 Codice Civile sono specificatamente approvate le clausole di cui agli articoli: Modalità di Accettazione della fornitura – Responsabilità – Contestazioni – Foro Competente Data Privacy e Subappalto.

Bologna, lì .....

Firma del Cliente per accettazione

_____