

InfoCamere-**ALL ECON OFFERTA** 20160413

Servizio IC4Cloud- Virtual Data Center  
Allegato Tecnico Contrattuale

|                   |                 |                |            |
|-------------------|-----------------|----------------|------------|
| Versione:         | 1.0             | Data Versione: | 20/05/2019 |
| Descr. modifiche: | Prima emissione |                |            |
| Motivazioni :     | non applicabile |                |            |
| Collaborazioni :  |                 |                |            |

## Indice

|  |           |
|--|-----------|
| <b>1 Introduzione al documento</b>                                 | <b>4</b>  |
| Scopo e campo di applicazione del documento                        | 4         |
| Livello di riservatezza  | 4         |
| Precedenti emissioni   | 4         |
| <b>2. Descrizione del servizio</b>                                 | <b>5</b>  |
| <b>2.1 Componenti base del servizio</b>                            | <b>5</b>  |
| 2.1.1 Risorse computazionali e spazio disco                        | 5         |
| 2.1.2 Macchine virtuali  | 6         |
| 2.1.3 Rete e firewall  | 6         |
| 2.1.4 Sistemi di sicurezza   | 7         |
| 2.1.5 Backup centralizzato   | 8         |
| 2.1.6 Accesso utente   | 8         |
| <b>2.2 Componenti opzionali del servizio</b>                       | <b>9</b>  |
| 2.2.1 Gestione sistemi virtuali                                    | 9         |
| 2.2.2 Gestione sistema operativo                                   | 9         |
| 2.2.3 Firewall as a service  | 9         |
| 2.2.4 Backup as a service  | 9         |
| 2.2.5 Load balancer  | 10        |
| 2.2.7 Servizio di VA/PT  | 10        |
| 2.2.8 DNS e DHCP   | 10        |
| 2.2.9 Connettività geografica                                      | 10        |
| 2.2.10 Accessi VPN SSL   | 10        |
| 2.2.11 Time Server   | 11        |
| 2.2.13 Antivirus   | 11        |
| 2.2.14 Disaster Recovery as a service                              | 11        |
| <b>3 Supporto tecnologico</b>                                      | <b>12</b> |
| 3.1 Supporto tecnologico: Contact Center e Service Desk            | 12        |
| 3.2 Supporto tecnologico: Event management e Monitoraggio eventi   | 12        |
| 3.2.1 Metriche monitorate  | 13        |
| 3.3 Supporto tecnologico: Service Management                       | 13        |
| 3.4 Supporto tecnologico: Incident Management e Problem Management | 13        |
| 3.4.1 Definizione del processo                                     | 14        |
| 3.4.2 Gestione dell'incidente                                      | 14        |
| 3.4.3 Incidenti di sicurezza                                       | 14        |
| 3.5 Sla Management   | 14        |
| 3.5.1 Gestione dei Report  | 15        |

|                                      |    |
|--------------------------------------|----|
| <b>4 Datacenter InfoCamere</b>       | 15 |
| 4.1 Protezione fisica e logica       | 15 |
| 4.2 Sostenibilità                    | 16 |
| 4.3 Elenco degli standard utilizzati | 16 |

## **1 Introduzione al documento**

### **1.1 Scopo e campo di applicazione del documento**

Il documento illustra le funzionalità e condizioni contrattuali del servizio IC for Cloud Virtual data center offerto da InfoCamere .

### **1.2 Livello di riservatezza**

|   | Livello     | Ambito di diffusione consentito  |
|---|-------------|--|
|   | Pubblico    | Il documento può essere diffuso <b>all'esterno</b> dell'azienda.   |
| X | Uso interno | Il documento può essere diffuso solo <b>all'interno</b> dell'azienda.<br>E' consentito darne comunicazione a terzi con clausola di non diffusione.   |
|   | Riservato   | Il documento <b>non può essere diffuso</b> all'interno dell'azienda.<br>La sua visibilità è limitata ad un gruppo ristretto di persone.<br>L'indicazione "Riservato" DEVE essere riportata anche nel Piè-di-pagina del documento . |

### **1.3 Precedenti emissioni**

|                   |                 |                |            |
|-------------------|-----------------|----------------|------------|
| Versione:         | 1.0             | Data Versione: | 20/05/2019 |
| Descr. modifiche: | Nessuna         |                |            |
| Motivazioni :     | Non Applicabile |                |            |

## **2. Descrizione del servizio**

IC for Cloud Virtual Data Center è un servizio di tipo IaaS offerto da InfoCamere che consente al cliente di creare e gestire in autonomia un proprio Virtual Data Center tramite l'acquisto di una quantità personalizzabile di risorse computazionali (vCPU, RAM), di rete (es. VLAN, IP pubblici, virtual firewall), spazio disco e servizi a corredo (es. backup, antivirus, DNS).

Al cliente viene garantito un insieme di utenze opportunamente profilate con le quali ha la possibilità di amministrare in modo del tutto autonomo le risorse attraverso GUI ed API, creando virtual machine a partire da template base predisposti da InfoCamere, configurando opportune policy firewall per la comunicazione sicura tra i propri server e gestendo tutto il ciclo di vita delle proprie virtual machine (es. power on, power off, snapshot).

L'infrastruttura con cui viene erogato il servizio è basata, dal punto di vista computing, su tecnologia VMware sia per quanto riguarda la piattaforma di virtualizzazione, realizzata con le ultime versioni di VMware vSphere; il portale di accesso utente è invece basato su VMware vRealize Automation. Dal punto di vista rete, invece, la tecnologia di riferimento è Cisco ACI, soluzione all'avanguardia nell'ambito della Software Defined Network; grazie a questa infrastruttura l'utente finale ha la possibilità di accedere ad un portale self-service da cui creare e gestire le proprie macchine virtuali/risorse.

Il servizio porta all'utente finale una serie di funzionalità e benefici:

- **Autonomia:** possibilità, nell'ambito delle risorse assegnate, di creare e gestire in autonomia le proprie VM ed i servizi ad esse correlati tramite GUI ed API.
- **Prestazioni:** server di virtualizzazione con processori di ultime generazioni, interconnessioni di rete a 10Gbps o superiore, apparati storage di livello enterprise.
- **Affidabilità:** infrastruttura di virtualizzazione tollerante ai guasti grazie a cluster in alta affidabilità, connessioni di rete e apparati storage ridondati.
- **Flessibilità:** possibilità di creare infrastrutture virtuali adeguate e dimensionate per ogni necessità, dalle più semplici alle più complesse per le aziende clienti più esigenti.
- **Scalabilità:** capacità di incrementare o diminuire le risorse assegnate in base alle proprie esigenze e volumi di business, senza dover affrontare investimenti in hardware e datacenter.
- **Sicurezza:** protezione del dato mediante backup centralizzato automatico delle VM.
- **Licenze:** possibilità di acquisire ed utilizzare licenze di sistema operativo Microsoft Windows Server o Red Hat Enterprise Linux.
- **Servizi aggiuntivi opzionali:** disaster recovery su sito remoto, continuità operativa mediante replica su sito secondario, monitoraggio infrastrutturale, antivirus, backup e restore in autonomia, connettività geografica, gestione sistemi operativi standard, DNS.
- **Certificazioni:** compliance normativa grazie alle certificazioni ISO 27001, ISO 27017, ISO 27018, ISO 9001, ISO 20000-1, ISO 22301, ISO 14001.

Nel complesso sono previste una serie di componenti base del servizio che vengono offerte al cliente più eventuali add-on che devono essere esplicitamente richiesti.

### **2.1 Componenti base del servizio**

Si descrivono di seguito le componenti base comprese nel servizio di Virtual Data Center offerto da InfoCamere.

#### **2.1.1 Risorse computazionali e spazio disco**

Al cliente viene assegnata una quantità personalizzabile di risorse computazionali e spazio disco sulla base di quanto contrattualizzato, in termini di:

- numero di vCPU
- GB di RAM
- GB di spazio disco

Le risorse computazionali (vCPU e RAM) vengono messe a disposizione tramite una piattaforma di virtualizzazione VMware vSphere che, grazie all'adozione di cluster con host VMware ESXi, garantisce:

- **Prestazioni:** utilizzo di server di ultima generazione con le più recenti versioni di processori e RAM;
- **High Availability (HA):** riaccensione automatica delle macchine virtuali in caso di guasto ad un host;
- **Distributed Resource Scheduling (DRS):** distribuzione automatica dei carichi di lavoro al fine di ottimizzare le performance;

Lo spazio disco viene erogato mediante apparati storage ridondati di livello enterprise, basati su piattaforma EMC e Netapp, con tipologia di disco ad alte prestazioni.

## 2.1.2 Macchine virtuali

Nell'ambito delle risorse assegnate descritte al punto precedente, il cliente ha la possibilità di creare e gestire in autonomia le macchine virtuali che compongono il suo Virtual Data Center.

Il cliente metterà a disposizione dei template, con sistemi operativi proprietari (analizzati e concordati con InfoCamere), supportati ed eventualmente corredati di opportuna licenza a proprio carico, template che InfoCamere provvederà ad importare e rendere disponibili all'interno del Virtual Data Center.

Opzionalmente, InfoCamere può mettere a disposizione a catalogo due tipologie di template generici con le seguenti versioni di sistema operativo:

- Microsoft Windows Server 2016 Datacenter Edition
- Red Hat Enterprise Linux 7.6

La tipologia e la numerosità dei template da prevedere a catalogo deve essere pattuita in sede contrattuale e, naturalmente, in seguito può essere variata rivolgendosi alla struttura commerciale di InfoCamere.

A partire da tali template il cliente può creare in autonomia le proprie macchine virtuali rispettando delle taglie predefinite e riportate nelle tabelle che seguono. L'aumento o la diminuzione delle risorse assegnate alle singole macchine virtuali deve adeguarsi a queste taglie.

| Tipologia di macchina | S.O.  | GB RAM | vCP<br>U | GB Spazio Disco    |
|-----------------------|-------|--------|----------|--------------------|
| Taglia S              | RHEL* | 2      | 1        | > 30 (a richiesta) |
| Taglia M              | RHEL* | 4      | 1        | > 30 (a richiesta) |
| Taglia L              | RHEL* | 8      | 2        | > 30 (a richiesta) |
| Taglia XL             | RHEL* | 16     | 4        | > 30 (a richiesta) |
| Taglia XXL            | RHEL* | 32     | 4        | > 30 (a richiesta) |

\* Red Hat Enterprise Linux 7.X nel caso di licenze fornite da IC, oppure altre distribuzioni supportate e fornite dal cliente

| Tipologia di macchina | S.O.        | GB<br>RAM | vCP<br>U | GB Spazio Disco    |
|-----------------------|-------------|-----------|----------|--------------------|
| Taglia S              | MS Windows* | 4         | 1        | > 60 (a richiesta) |
| Taglia M              | MS Windows* | 8         | 2        | > 60 (a richiesta) |
| Taglia L              | MS Windows* | 16        | 4        | > 60 (a richiesta) |
| Taglia XL             | MS Windows* | 24        | 4        | > 60 (a richiesta) |
| Taglia XXL            | MS Windows* | 32        | 8        | > 60 (a richiesta) |

\*Microsoft Windows Server 2016 nel caso di licenze fornite da IC, oppure altre versioni supportate e fornite dal cliente

La quantità di risorse contrattualizzata può essere amministrata in autonomia dal cliente al fine di creare, cancellare, ridimensionare le proprie macchine virtuali secondo le logiche suddette. Non è prevista una scalabilità automatica, ma il cliente può decidere in autonomia come e quando utilizzare le risorse assegnate. Nel caso sia necessario variare il pool di risorse assegnate, il cliente può rivolgersi alla struttura commerciale di InfoCamere.

## 2.1.3 Rete e firewall

Per quanto riguarda l'ambito rete, la soluzione Virtual Data Center di InfoCamere è basata su un'infrastruttura realizzata con Cisco ACI e prevede l'assegnazione ad ogni cliente di un ambiente completamente isolato dal punto di vista network (in seguito identificato come "tenant") tramite l'utilizzo di

opportuni apparati di sicurezza. All'interno di un tenant, la soluzione di base, prevede due VLAN (Virtual Local Area Network):

- Intranet: rete con piano di indirizzamento privato che contiene i servizi interni non esposti in internet;
- DMZ: rete con piano di indirizzamento pubblico o privato che contiene i servizi da rendere accessibili dalla rete internet;

Il livello di sicurezza tra le suddette network è demandata ad un firewall virtuale installato e gestito completamente dal cliente (con relativa licenza) oppure opzionalmente da InfoCamere.

L'architettura di rete all'interno del Virtual Data Center, nel caso in cui la gestione sia delegata ad InfoCamere, deve essere definita e concordata in fase contrattuale.

Per esporre i servizi in internet ogni cliente avrà a disposizione 8 indirizzi IPv4 pubblici che InfoCamere, in quanto LIR (Local Internet Registry) registrato presso il RIPE, assegnerà in modo esclusivo al cliente. Gli indirizzi IP pubblici saranno selezionati dall'attuale spazio di indirizzamento pubblico IPv4 di InfoCamere (80.82.0.0/20).

Il cliente potrà avere a disposizione un banda internet minima garantita e traffico illimitato. Le possibili soluzioni sono esposte nelle tabella sottostante:

| Tipologia Banda | di | Velocità Garantita U.L. | Velocità Garantita D.L. |
|-----------------|----|-------------------------|-------------------------|
| Taglia S        |    | 1                       | 1                       |
| Taglia M        |    | 5                       | 5                       |
| Taglia L        |    | 10                      | 10                      |
| Taglia XL       |    | 50                      | 50                      |
| Taglia XXL      |    | 100                     | 100                     |

#### 2.1.4 Sistemi di sicurezza

InfoCamere adotta, per l'infrastruttura di erogazione del servizio e per quella attinente al proprio ambiente di gestione, tutte le soluzioni tecniche di protezione dei dati, comprese le soluzioni che fanno uso di sistemi crittografici per proteggere i dati in transito. Tali infrastrutture sono progettate, realizzate ed erogate in accordo con le policy interne di sicurezza, derivate dai controlli ISO27002, ISO 27017 ed ISO 27018. E' posta particolare attenzione alla verifica della conformità di tali strumenti con le prescrizioni della normativa in materia di protezione dei dati personali (GDPR e legislazione nazionale).

##### Anti DDOS.

InfoCamere ha realizzato un sistema di difesa da attacchi informatici di tipo DDoS (Distributed Denial of Service) in grado di individuare e bloccare il traffico anomalo prima che questo arrivi alla connessione Internet.

Per traffico anomalo si intende, in questo contesto, un flusso massiccio di richieste dolose provenienti da sorgenti distribuite e dirette verso uno dei servizi erogati, in grado di saturare la banda trasmissiva o la capacità elaborativa dei dispositivi di rete. Una protezione efficace da attacchi di tipo DDoS richiede meccanismi di intercettazione del traffico doloso distribuiti nell'infrastruttura di rete del Fornitore di connettività (operatore TLC), in modo da poter intervenire il più "a monte" possibile nei flussi che vanno dalle sorgenti degli attacchi ai loro obiettivi (che nel nostro caso sono posti all'interno dei datacenter InfoCamere).

##### Penetration Test e Vulnerability Assessment

InfoCamere verifica la sicurezza delle proprie infrastrutture secondo due modalità:

- Tramite propri strumenti e personale interno, viene eseguito un test di Vulnerability Assessment sull'intera infrastruttura; la cadenza è tipicamente mensile, salvo maggiore frequenza dettata da alert su minacce particolarmente gravi;
- Indicativamente due volte l'anno, viene svolta attività di vulnerability assessment e penetration test effettuate da fornitori esterni specializzati, selezionati appositamente.

In base alle risultanze dei test, le attività di remediation che si rendono necessarie sono priorizzate in funzione del relativo rischio.

### 2.1.5 Backup centralizzato

Le macchine virtuali create dal cliente che compongono il suo Virtual Data Center sono sottoposte a backup automatico e centralizzato. L'infrastruttura di backup è realizzata con il prodotto Veeam Backup & Replication che consente di eseguire il backup delle macchine virtuali interagendo direttamente con la piattaforma di virtualizzazione senza la necessità di installare agenti all'interno delle macchine virtuali. InfoCamere, come servizio base, assicura il backup e l'eventuale restore dell'intera macchina virtuale prevedendo:

- Un backup full settimanale
- Un backup incrementale giornaliero
- Retention dei dati di 42 giorni (6 settimane).

In fase contrattuale è possibile per il cliente stabilire la fascia oraria durante la quale verrà eseguito il backup.

Il servizio base di backup prevede che le attività di backup e restore siano in completa gestione da parte di InfoCamere e, basandosi su snapshot delle macchine virtuali, non tiene conto e non assicura la consistenza in presenza di particolari applicativi installati all'interno delle macchine (SQL Server, Oracle, Exchange, Active Directory, ...). Nel caso in cui il cliente abbia particolari esigenze per quanto riguarda il backup del suo Virtual Data Center, queste devono essere discusse e gestite in sede contrattuale eventualmente attingendo a componenti opzionali del servizio di backup.

### 2.1.6 Accesso utente

Il cliente può accedere al proprio Virtual Data Center tramite un portale self-service raggiungibile da rete internet mediante i seguenti browser:

- Internet Explorer (versione 11)
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Il portale è stato realizzato da InfoCamere avvalendosi di VMware vRealize Automation e l'accesso può essere effettuato tramite il seguente link:

<https://icssp.clic.infocamere.it/vcac/org/<tenant del cliente>>

dove <tenant del cliente> è il nome specifico assegnato al suo Virtual Data Center.

Al cliente vengono assegnate le utenze concordate in fase contrattuale, opportunamente profilate per l'accesso al portale. Una volta eseguita l'autenticazione al portale il cliente è in grado di amministrare in completa autonomia le risorse assegnate, potendo creare/cancellare macchine virtuali a partire dai template presenti a catalogo e gestendo l'intero ciclo di vita (power on, power off, snapshot, connect to console, ...).

In alternativa all'accesso tramite GUI, il cliente può interagire con il proprio Virtual Data Center anche mediante le API che il portale mette a disposizione e raggiungibili per l'autenticazione al seguente link:

<https://icssp.clic.infocamere.it/identity/api/tokens>

A titolo esemplificativo tramite API il cliente può:

- Visionare la lista dei servizi disponibili a catalogo
- Richiedere la creazione di una virtual machine
- Visionare le risorse correntemente allocate
- Spegnere una virtual machine
- Modificare la data di scadenza di una virtual machine
- Eseguire lo snapshot di una virtual machine
- Eseguire il revert dello snapshot di una virtual machine

Per maggiori dettagli sull'uso delle API e sulle operazioni che il cliente è in grado di innescare tramite il loro utilizzo, si rimanda alla documentazione ufficiale VMware disponibile al link:

<https://code.vmware.com/apis/568/vra-catalog?p=vrealize-automation>



Nel caso di particolari esigenze da parte del cliente o a causa di temporanea indisponibilità del portale self-service, è possibile prevedere un accesso di emergenza tramite il quale il cliente accede direttamente alla piattaforma di virtualizzazione che ospita il suo Virtual Data Center mediante VMware vCenter.

## **2.2 Componenti opzionali del servizio**

Si descrivono di seguito le componenti che opzionalmente il cliente può richiedere a supporto del proprio Virtual Data Center.

### **2.2.1 Gestione sistemi virtuali**

Nel caso in cui il cliente non voglia affrontare in autonomia la creazione e gestione del proprio Virtual Data Center, ad esempio perché non è dotato di un reparto con specifiche competenze IT, InfoCamere può opzionalmente occuparsi di tutta la fase di creazione delle macchine virtuali del cliente e gestirne il ciclo di vita lato piattaforma di virtualizzazione.

Viene demandata al cliente la gestione di tutto quello che riguarda il sistema operativo e il software installato all'interno delle macchine virtuali.

### **2.2.2 Gestione sistema operativo**

Questa componente opzionale richiede come prerequisito quella descritta al punto 2.2.1, ovvero la gestione da parte di InfoCamere delle macchine virtuali del cliente lato piattaforma di virtualizzazione. Il cliente ha opzionalmente la possibilità di demandare ad InfoCamere anche la gestione del sistema operativo, purché rientri in quelli considerati standard da InfoCamere ovvero Microsoft Windows Server oppure Red Hat Enterprise Linux.

L'erogazione di questo servizio opzionale prevede attività specialistiche nei seguenti ambiti:

- Manutenzione correttiva ed evolutiva del sistema operativo (ad esempio installazione patch, anche in collaborazione con il cliente per la verifica di eventuali conflitti con i sistemi in uso)
- Amministrazione delle aree dati, quali la gestione dei file system
- Gestione degli utenti secondo le politiche definite con il cliente
- Supporto nella risoluzione di problemi o bug legati al sistema operativo.

Questo servizio può essere esteso anche al di fuori dei sistemi operativi standard prima indicati. In questo caso però InfoCamere può offrire un supporto di tipo "best effort". Altrimenti, nel caso di esigenze specifiche da parte del cliente, è possibile pattuire livelli di servizio diversi in sede contrattuale.

### **2.2.3 Firewall as a service**

Come descritto al punto 2.1.3, all'interno di ogni tenant è previsto un firewall al fine di gestire e applicare le opportune policy di sicurezza per i servizi che il cliente espone in internet, ma anche per le network presenti nel Virtual Data Center. Opzionalmente il cliente può scegliere le seguenti soluzioni:

- InfoCamere fornisce le licenze e il software necessario per poter installare un firewall virtuale (tecnologia di riferimento Fortinet). La configurazione del firewall e la definizione/applicazione delle policy di sicurezza è a carico del cliente.
- InfoCamere fornisce e gestisce il firewall.

### **2.2.4 Backup as a service**

InfoCamere può opzionalmente offrire un servizio di BaaS (Backup as a Service) addizionale rispetto al backup automatico standard delle macchine virtuali del proprio Virtual Data Center.

Il servizio permette al cliente di effettuare in autonomia backup basati su immagini remotizzate delle proprie macchine virtuali e i relativi restore, lavorando a stretto contatto con la piattaforma di virtualizzazione VMware, evitando di dover installare agenti all'interno delle macchine virtuali da proteggere.

La tecnologia utilizzata, non avvalendosi della capacità di rete e delle risorse computazionali delle macchine virtuali per il trasferimento dei dati, garantisce il minimo overhead possibile e la massima trasparenza di esecuzione. La macchina virtuale sottoposta a protezione viene interamente salvaguardata, indipendentemente dal sistema operativo installato.

Il servizio è basato su piattaforma Veeam Backup & Replication, leader di mercato nel backup basato su immagine.

### **2.2.5 Load balancer**

InfoCamere può, opzionalmente, fornire un sistema di load balancer per i servizi del cliente attivi all'interno del proprio Virtual Data Center. La soluzione permette di bilanciare il traffico tra più server garantendo così una distribuzione del carico, ridondanza delle risorse e un aumento dell'affidabilità dei servizi del cliente.

Le alternative proposte sono le seguenti:

- InfoCamere fornisce le licenze e il software necessario per poter installare un virtual load balancer (tecnologia di riferimento F5). La configurazione e gestione è a carico del cliente;
- InfoCamere fornisce e gestisce una soluzione di virtual load balancer;

### **2.2.7 Servizio di VA/PT**

Opzionalmente è possibile eseguire dei test di sicurezza delle infrastrutture di proprietà del cliente, ottenendo informazioni sulle vulnerabilità tecniche in modo tempestivo e per l'intero perimetro aziendale. InfoCamere può offrire le proprie competenze nella selezione di un partner esterno qualificato, affiancando poi il Cliente nella fase di conduzione del test e dell'analisi dei risultati.

### **2.2.8 DNS e DHCP**

Qualora il cliente non avesse un servizio DNS/DHCP all'interno del proprio Virtual Data Center può, opzionalmente, richiedere ad InfoCamere la fornitura del suddetto servizio per la risoluzione dei nomi interni/esterni e per l'assegnazione dinamica degli indirizzi IPv4. Il cliente, inoltre, può demandare ad IC anche la registrazione e gestione dei domini pubblici.

L'erogazione di questo servizio opzionale richiede un'analisi di fattibilità da completare durante la fase contrattuale.

### **2.2.9 Connettività geografica**

I clienti che necessitano di collegare il proprio Virtual Data Center con sedi distribuite sul territorio nazionale possono, opzionalmente, chiedere ad InfoCamere un servizio di connettività geografica che consiste in una rete intranet realizzata con tecnologia MPLS.

InfoCamere, con la collaborazione dei principali provider presenti sul mercato può installare, gestire e monitorare una rete intranet che connette le sedi remote del cliente con il Virtual Data Center. La soluzione prevede, per ogni filiale, l'installazione di un circuito geografico in alta affidabilità attestato in una coppia di router (requisiti necessari per evitare single point of failure) nei quali è attivo un protocollo di routing dinamico, sono configurate le ACL (Access Control List) per la gestione del traffico e sono impostate politiche di QoS (Quality of Service). L'adozione del servizio richiede un'adeguata analisi in fase contrattuale perché, ad esempio, è necessario concordare il dimensionamento dei link da attivare nelle filiali, il piano di indirizzamento, le politiche di gestione del traffico (QoS), ecc.

### **2.2.10 Accessi VPN SSL**

Per eventuali accessi amministrativi ad di fuori degli strumenti convenzionali, opzionalmente è possibile utilizzare la connettività VPN SSL.

Un VPN SSL funziona con quasi tutti i browser Web standard. A differenza di Internet Protocol Security (IPSEC) VPN, SSL VPN non necessita di software specializzato sul computer dell'utente finale. Questo aumenta notevolmente la flessibilità di SSL VPN Wireless gli utenti possono inoltre connettersi alla rete tramite SSL VPN, fornendo una maggiore protezione, come pure meno complessa amministrazione del sistema.

### 2.2.11 Time Server

Infocamere può fornire un servizio di sincronizzazione temporale dei sistemi avviati all'interno del Virtual Data Center del cliente. Il servizio viene erogato da tre time server in alta affidabilità sincronizzati con la costellazione di satelliti GPS e Galileo, tramite il protocollo NTP (Network Time Protocol).

### 2.2.13 Antivirus

InfoCamere protegge la propria rete e i propri sistemi con un sistema antivirus e antimalware basato su tecnologia Trend Micro, adottando per la protezione delle macchine virtuali la soluzione Trend Micro Deep Security.

Tale soluzione può essere opzionalmente messa a disposizione anche per le macchine virtuali che compongono il Virtual Data Center del cliente, che vengono così monitorate ed aggiornate da un sistema di Control Manager messo a disposizione da Trend Micro.

Inoltre esiste la possibilità di fornire al cliente un report sullo stato delle macchine virtuali (infezioni e rimozioni, quarantena dei file, ...).

### 2.2.14 Disaster Recovery as a service

Il servizio di **Disaster Recovery as a Service** (DRaaS), proposto come opzione e da concordare con il cliente, permette di proteggere la propria infrastruttura da eventi disastrosi.

Il servizio prevede, qualora InfoCamere dichiari lo stato di disastro (Piano di disaster recovery e continuità operativa), di attivare l'infrastruttura IAAS nel sito alternativo, mediante strumenti che garantiscono la replica delle macchine virtuali basate su immagini.

Durante la definizione di una soluzione di Disaster Recovery, fondamentale importanza rivestono due parametri di misurazione: RPO e RTO.

- **RPO** (*Recovery Point Objective*) rappresenta il disallineamento massimo che si è disposti a tollerare tra ambiente di produzione (Sito primario) e ambiente replicato (Sito secondario). Descrive quindi a tutti gli effetti la quantità di dati rimasti non sincronizzati in caso di disastro.
- **RTO** (*Recovery Time Objective*) rappresenta il tempo necessario al ripristino operativo dei servizi sul Sito secondario, a seguito di disastro. Descrive quindi il tempo necessario per completare operativamente la procedura di disaster recovery necessaria a rendere i propri servizi nuovamente attivi.

Sono previsti dei test di DR che dovranno essere concordati e pianificati tra InfoCamere/Cliente.

### **3 Supporto tecnologico**

Di seguito vengono riportate le descrizioni dei supporti tecnologici previsti nel servizio IC for Cloud Virtual data Center, riferiti esclusivamente a quanto di competenza InfoCamere, ovvero per la componente infrastrutturale (hardware e software) e per la continuità elettrica a supporto delle macchine virtuali messe a disposizione del cliente, con i livelli di servizio successivamente descritti.

#### **3.1 Supporto tecnologico: Contact Center e Service Desk**

Il supporto tecnologico viene garantito da InfoCamere 24x7 attraverso il Contact Center ed il Service Desk. I canali di comunicazione utilizzati sono il telefono e la email.

##### **Contact Center**

Gli operatori del Contact Center supportano i clienti a fronte di qualsiasi segnalazione, che viene tracciata all'interno dello strumento aziendale di Ticketing.

Il contatto via email, sempre utilizzabile, garantisce l'invio della risposta iniziale alla segnalazione del Cliente entro il Maximum First Support Response Time definito.

Viene reso disponibile uno specifico numero telefonico di supporto tecnico per la segnalazione di disservizi importanti che necessitino di un intervento immediato, in quanto inficiano la capacità del Cliente di offrire i servizi per i quali viene utilizzata l'infrastruttura gestita da InfoCamere.

Tale canale prevede la presa in carico immediata con conseguente gestione della problematica esposta.

Ogni cambiamento di stato del ticket (Apertura, In lavorazione e Chiusura) viene segnalato al cliente con una notifica email. Nel caso di evidente disservizio, il Ticket viene gestito all'interno del normale flusso di Incident Management aziendale. (vedi par.3.4)

Il servizio telefonico di Contact Center è attivo dal lunedì al venerdì dalle 08.30 alle 18.30. Nelle altre fasce le segnalazioni sono inoltrate automaticamente al Service Desk.

##### **Service Desk**

Gli operatori del Service Desk gestiscono il primo contatto telefonico col cliente nelle fasce orarie non presidiate dal personale del Contact Center.

Il personale del Service Desk attraverso le competenze tecniche ed il diretto presidio sui servizi, consente un rapido intervento per la risoluzione della malfunzione, garantendo l'ingaggio di ulteriori figure specialistiche.

A seguire la tabella con indicati orari e modalità per il supporto InfoCamere.

| <b>Servizio Virtual Data Center</b> |   |
|-------------------------------------|---|
| <b>Disponibilità del servizio</b>   | 24x7  |
| <b>Contatti</b>                     | Ad ogni Cliente verrà assegnato uno specifico numero di telefono ed una casella e-mail dedicata |
| <b>Identificativo Servizio</b>      | Come da standard Infocamere verrà assegnato uno specifico identificativo del servizio           |

#### **3.2 Supporto tecnologico: Event management e Monitoraggio eventi**

Il processo di Event Management gestisce il controllo ed il monitoraggio unificato dell'infrastruttura tecnologica, attraverso le seguenti principali attività:

- Controllo continuo ed automatizzato di sistemi e risorse, mediante specifico Agente installato nelle macchine, con la rilevazione e notifica degli eventi;
- Azioni di ripristino automatiche a fronte di specifici eventi;
- Monitoraggio continuativo dei servizi web, attraverso "Sonde" automatiche che simulano la fruizione del servizio;

E' prevista la predisposizione di un cruscotto grafico in cui vengono esposti gli indicatori che in tempo reale offrono una visione dello stato delle componenti infrastrutturali, ovvero che riguarda la disponibilità delle risorse.

Le informazioni vengono ricavate attraverso lo strumento usato in azienda per il monitoraggio.

Tale strumento consente anche di creare delle viste ad hoc ritagliate sulle esigenze del cliente.

Opzionalmente, se richiesto dal cliente, potrà essere predisposto anche un servizio di monitoraggio sulle risorse in uso da quest'ultimo.

### **3.2.1 Metriche monitorate**

Metriche di base applicate ad ogni Sistema:

- Disponibilità di CPU
- Disponibilità ed Occupazione spazio disco
- Consumo di memoria
- Raggiungibilità dell'infrastruttura

Metriche opzionali su eventuale richiesta del Cliente:

- Controllo componente
- Controllo processi
- Controllo Applicazioni web

### **3.3 Supporto tecnologico: Service Management**

InfoCamere garantisce al cliente un'accurata gestione del servizio principalmente attraverso l'azione dedicata di figure professionali quali il Technical Account Manager, che con la collaborazione dell'Incident Manager, Problem Manager e Service Level Manager, assicura che l'infrastruttura ed i servizi erogati siano organizzati, strutturati ed eseguiti al fine di:

- allineare i servizi ai bisogni correnti e futuri del cliente;
- migliorare in modo continuo la qualità dei Servizi IT erogati;
- collaborare con i partner tecnologici del cliente per sviluppare ed integrare Servizi IT.

Inoltre le principali attività del Team dei Technical Account Manager sono le seguenti:

- avviare, pianificare e coordinare le attività previste dalla fornitura;
- costituire il punto di primo contatto per il supporto proattivo;
- interfacciarsi con il management ed il Team tecnico del Cliente;
- coordinare le attività a richiesta descritte di seguito.

### **3.4 Supporto tecnologico: Incident Management e Problem Management**

### 3.4.1 Definizione del processo

Per “**Incident**” si intende un’interruzione non pianificata o la riduzione di qualità di un servizio IT;

Per “**Problem**” si intende la causa primaria che ha provocato l’insorgere di uno o più “Incident”.

Il principale obiettivo del processo di “**Incident Management**” è di ristabilire il regolare stato delle attività il **prima possibile e minimizzare l’impatto** sul Servizio erogato).

Il principale obiettivo del processo di “**Problem Management**” è l’identificazione delle cause primarie dell’Incident e conseguente adozione di misure atte ad impedire il ripresentarsi della malfunzione.

I processi di Incident e Problem Management sono formalmente definiti ed adottati da tutte le forze aziendali che concorrono alla continuità di erogazione del servizio. L’adozione di Best Practices ITIL e di strumenti automatici per l’escalation funzionale e gerarchica, garantiscono un immediato innesco dei processi.

### 3.4.2 Gestione dell’incidente

L’incidente una volta registrato, viene assegnato ad un gruppo di competenza che lo valuta e lo qualifica definendone o confermandone la Severity.

Le severity possibili sono:

- **FT – Fermo Totale (High)**: il servizio è inaccessibile a tutti gli utenti;
- **FP – Fermo Parziale (Medium)**: il servizio è accessibile agli utenti (anche a parte di essi), ma con limitazioni di servizio;
- **RA – Rallentamento (Low)**: il servizio è accessibile agli utenti e pur non presentando limitazioni significative necessita di un intervento manutentivo.

La “Presenza in Carico” dell’Incidente da parte dei Team preposti avviene nel più breve tempo possibile.

L’incidente viene “Chiuso” solo con il servizio ripristinato e la conferma della funzionalità da parte del cliente

### 3.4.3 Incidenti di sicurezza

InfoCamere dispone un team interno (Security Operation Center interno), specializzato per la gestione degli incidenti di sicurezza (operando quindi come CSIRT: Computer Security Response Team). Il team interno opera in comunicazione con altri enti di riferimento (come CERT-PA e CERT-IT) e con un servizio di CSIRT/SOC esterno che opera in sinergia con il personale InfoCamere, ampliandone le capacità di monitoraggio e di individuazione delle minacce cyber.

Quando il SOC interno oppure quello esterno, attraverso i propri strumenti di SIEM (Security Information and Event Management), individua una situazione di anomalia, si attiva un processo di analisi e gestione dell’incidente. Nel caso la tipologia di incidente richieda l’attivazione del Cliente (come nell’eventualità di “data-breach”, normata dal GDPR) il SOC InfoCamere attiverà il canale di comunicazione instaurato, attraverso il Technical Account Manager, per le altre tipologie di incidente.

Allo stesso modo, quando è il Cliente a voler segnalare un evento di possibile incidente di sicurezza informatica, avrà a disposizione i canali già previsti per le altre tipologie di incidente: il processo InfoCamere di gestione dell’incidente prevede poi l’attivazione di flussi specializzati nei casi di incidente di sicurezza.

## **3.5 Sla Management**

Per il servizio proposto viene garantito uno SLA del **99,9%** su base annuale.

La mancata disponibilità e la responsabilità dell’evento verranno valutate tramite il processo di Incident

Management.

Quando l'indisponibilità risulterà attribuita al Fornitore, questa entrerà nel computo dello SLA.

Da tale computo vanno esclusi eventuali fermi pianificati e concordati con il cliente.

### 3.5.1 Gestione dei Report

A seconda delle richieste del cliente, possono essere generati e forniti dei report indicanti i livelli di servizio di quanto a carico di InfoCamere.

## **4 Datacenter InfoCamere**

Tutti i servizi del CED di Padova sono erogati in **architettura logica e fisica di alta affidabilità** e continuità operativa. Il Data Center è protetto con architetture di Continuous Availability e Disaster Recovery. Circa **100.000 controlli al giorno** in un ambiente a forte automazione garantiscono **100 Milioni di operazioni** e ad ogni sito sono dedicate linee in fibra ottica Gigabit Ethernet ad alta affidabilità con doppio operatore.

La **sicurezza fisica e logica** dei siti è garantita da un presidio 24 ore su 24 con controlli perimetrali TVCC. Gli accessi sono controllati con lettori badge e dispositivi biometrici. Oltre 5.000 sensori per il controllo dei parametri fisici: temperatura, umidità, anti-intrusione, anti-incendio, stato alimentazione-condizionamento.

I Sistemi di protezione e conservazione dei dati sono **conformi ai requisiti della Certificazione ISO/IEC 27001**.

Il Data Center Infocamere è stato progettato tenendo presenti i requisiti richiesti dal livello 3 (Tier 3) dello standard ANSI/TIA942

### **4.1 Protezione fisica e logica**

Gli approcci usati per la protezione dei dati sono studiati ed implementati tenendo conto della tipologia dei dati che devono essere trattati, delle normative vigenti e dell'analisi dei rischi. In generale possiamo dire che viene garantito un livello di protezione "base" al quale vengono aggiunti ulteriori livelli a seconda delle necessità. In tutti i casi si deve distinguere tra sicurezza intesa in senso fisico, ovvero la protezione dell'integrità del dato stesso sia in termini di controllo degli accessi ai locali dove si trovano i dispositivi di memorizzazione delle informazioni, ma anche di predisposizione di politiche e misure atte a proteggere l'integrità del dato attraverso meccanismi di backup, ridondanza, replicazione sia da problemi legati al malfunzionamento degli apparati sia da eventi potenzialmente disastrosi come alluvioni, terremoti, incendi o quant'altro e sicurezza in senso "logico" che riguarda la regolamentazione dell'accesso all'informazione attraverso la definizione di ruoli e responsabilità, tracciatura degli accessi.. Per quanto riguarda il data center di InfoCamere nella procedura di Controllo Accessi sono ben definite tutte le aree della sede e indicate le regole per le abilitazioni di accesso. Le aree sono segregate con porte di sicurezza controllate con lettori di badge. Per alcuni locali sensibili vi sono lettori con obbligo di codice PIN, a sbarramento singolo o a controllo biometrico.

Il sito principale di PD inoltre è monitorato h24 e 365 giorni l'anno da un impianto di videosorveglianza a circuito chiuso (TVCC) esteso al perimetro esterno e a tutte le aree sensibili. Lo stesso è presidiato dal servizio di portineria. Anche il data center di MI, utilizzato come sito per la Disaster Recovery, è dotato di un sistema di controllo accessi basato su badge differenziati (per personale interno, per fornitori o per visitatori), è dotato di allarme volumetrico, sensori anti-intrusione e sistema di controllo varchi con TVCC.

Tutti i dati sono memorizzati su dispositivi con intrinseche capacità di alta affidabilità e controllo di integrità oltre ad essere sottoposti a backup incrementali e/o completi in dipendenza dalle necessità e dalle tecnologie disponibili, tali backup vengono effettuati in duplice copia e conservati in due siti distinti. Alcuni dati, oltre essere sottoposti regolarmente a backup vengono replicati in modo continuo sui dispositivi che si trovano nel CED di Milano, la replica avviene attraverso diverse tecnologie a seconda del supporto di memorizzazione dei dati e dello strumento di gestione, ad esempio viene utilizzato Oracle Data Guard per i

principali database Oracle, VMware Site Recovery Manager, Hyper-V replica e replica storage per gli ambienti virtuali. InfoCamere è certificata ISO 27001:2017 ed effettua tutti i controlli previsti in ISO27002.

Una sintesi delle misure di sicurezza e dei controlli applicati è disponibile presso: <http://www.infocamere.it/documents/10193/27993/Sintesi+politiche+sicurezza+informazioni.pdf/>

La conformità al GDPR è garantita by design e by default in ogni processo, strumento o servizio. I controlli di sicurezza e privacy riguardano la progettazione, realizzazione, erogazione ed assistenza di tutti i servizi informatici. Tali controlli sono seguiti da strutture organizzative interne appositamente istituite, la sicurezza è inoltre coordinata a livello aziendale da figure appositamente preposte, verificata costantemente tramite audit (sia interni che esterni) e con l'ausilio del Data Protection Officer.

I Sistemi di protezione e conservazione dei dati sono conformi ai requisiti della Certificazione ISO 27001:2017, ISO 27017:2017, ISO 27018:2019

Il sistema di gestione della continuità operativa è certificato ISO 22301

Si allega il video sul Datacenter InfoCamere

<https://www.youtube.com/watch?v=P5-qLm8hCls>

## **4.2 Sostenibilità**

InfoCamere ha da tempo adottato un approccio "verde" ed energeticamente efficiente nell'evoluzione delle sue infrastrutture e dei sistemi: dalle tecniche di virtualizzazione, alle soluzioni di collaboration e communication, all'erogazione di un servizio di Cloud Computing, per arrivare all'installazione delle isole ad alta densità.

Una soluzione innovativa scelta dall'Azienda per una riduzione dei costi energetici in linea con quanto richiesto dall'Agenzia per l'Italia Digitale ai data center della Pubblica Amministrazione.

InfoCamere sta valutando l'adozione di un impianto fotovoltaico per l'utilizzo di energie rinnovabili e per ridurre ulteriormente le emissioni dannose per l'ambiente.

## **4.3 Elenco degli standard utilizzati**

Standard ITIL

ISO/IEC 20000-1:2011

UNI EN ISO 22301:2014

ISO 14001:2015

UNI CEI ISO/IEC 27001:2017

ISO/IEC 27017:2015

ISO/IEC 27018:2019

Performance Best Practices for VMware vSphere 6.7

Microsoft Best Practices for Hyper-V + RAP as a Service (Assessments da parte di Microsoft)

Red Hat Virtualization 4.2 Technical Reference

Installing and Upgrading VMware vRealize Automation

Check Point Best Practices Solutions and Documents

Cisco Application Centric Infrastructure Best Practices Guide, Release 1.3(1) and Earlier

Using VMAX and PowerMax in VMware vSphere Environments

EMC MirrorView Knowledgebook

Ontap9 FC Configuration for Windows Express Guide

VMware vSphere with ONTAP