Servizi IaaS e PaaS erogati dal TIX di Regione Toscana

REVISIONI DEL DOCUMENTO					
Revisione	**Data**	**Elenco Modifiche**	**Compilato**	**Approvato**	**Validato**
1.0	2019-06-11	Prima versione	C. Gallotti	A. Tarchi (RT)	A. Tarchi (RT)

INDICE

1 Scopo

Questo documento illustra le caratteristiche dei servizi IaaS e PaaS offerti da Regione Toscana.

I servizi rispettano la normativa vigente e in particolare:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Decreto Legislativo 196 del 2003 e successive modificazioni;
- Legge 547 del 1993 (computer crime);
- D.Lgs. 82 del 2005, "Codice dell'Amministrazione Digitale" o CAD, e successive modificazioni.

L'ente affida a Regione Toscana, in relazione ai servizi in oggetto, il trattamento di dati personali per la finalità di ricevere i servizi stessi. L'ente stabilisce quali dati trattare nell'ambito dei servizi offerti e pertanto stabilisce autonomamente le categorie di persone interessate al trattamento. A titolo esemplificativo sono:

- Dati del personale e dei collaboratori;
- Cittadini.

I tipi di dati trattati sono Personali, eventualmente anche appartenenti a particolari categorie (es. sensibili o giudiziari) e anche relativi a operazioni particolari come geolocalizzazione e profilazione.

2 Responsabilità

Regione Toscana eroga il servizio di IaaS e PaaS in qualità di:

- titolare del trattamento dei dati personali per le istanze assegnate a Regione Toscana stessa;
- responsabile del trattamento dei dati personali per le istanza assegnate ad altri enti.

Regione Toscana si avvale di fornitori per la gestione dell'infrastruttura informatica e della piattaforma applicativa ("Gestore del TIX") individuato a sua volta come:

1. Responsabile del trattamento dei dati personali per le istanze assegnate a Regione Toscana stessa;
2. Sub-responsabile del trattamento dei dati personali per le istanze assegnate ad altri enti.

Le seguenti, tra le altre, sono responsabilità di Regione Toscana (e del Gestore del TIX):

- provvedere alla gestione dell'infrastruttura fisica e alla sua dismissione sicura;
- assicurare l'accesso alle istanza PaaS ai soli amministratori di sistema;
- assicurare la configurazione sicura degli hypervisor;
- assicurare la configurazione sicura del middleware e del DBMS messo a disposizione per il servizio PaaS;
- monitorare l'utilizzo delle risorse per le piattaforme PaaS;

- configurare la difesa perimetrale, anche da malware;
- realizzare i backup dove esplicitamente indicato e mantenerli nel TIX;
- mettere a disposizione un sistema di logging;
- mettere tempestivamente a disposizione, secondo le indicazioni dei loro produttori, le patch funzionali e di sicurezza per i prodotti messi a disposizione (sistemi operativi, middleware, DBMS);
- configurare in modo sicuro e con strumenti crittografici allo stato dell'arte i canali di trasmissione e comunicazione come sopra descritto;
- gestire gli incidenti sull'infrastruttura IaaS e PaaS e fornire supporto agli enti in caso di incidenti sugli strati di software superiori;

Le seguenti, tra le altre, sono responsabilità degli enti:

- amministrare le credenziali e le autorizzazioni per l'accesso alle piattaforme acquistate;
- monitorare l'utilizzo di risorse;
- configurare il controllo di malware sulle piatteforme IaaS e PaaS;
- realizzare i backup non garantiti da Regione Toscana;
- collegare i sistemi al sistema di logging di Regione Toscana;
- installare o richiedere l'installazione delle patch;
- configurare i canali di trasmissione e comunicazione oltre a quelli messi a disposizione da Regione Toscana (p.e. https per i siti web);
- sviluppare e mantenere i sistemi su strati applicativi superiori a quelli messi a disposizione da Regione Toscana;
- gestire gli incidenti sugli strati applicativi superiori a quelli messi a disposizione da Regione Toscana.

2.1 Diritto di audit

L'ente ha facoltà di vigilare, anche tramite verifiche periodiche (previa comunicazione scritta fornita con ragionevole anticipo), sulla puntuale osservanza dei compiti e delle istruzioni qui impartite a Regione Toscana.

A sua volta, Regione Toscana assicura che svolgerà periodicamente, e almeno una volta all'anno, una verifica delle proprie misure di sicurezza adottate per controllare i rischi di accesso non autorizzato, divulgazione, mancanza di integrità e indisponibilità dei dati, sia accidentali sia illegali.

2.2 Diritti degli interessati

In qualità di responsabile del trattamento, Regione Toscana garantisce il supporto, attraverso il Service desk, agli enti per il rispetto dei diritti degli interessati.

Regione Toscana, attraverso i suoi fornitori, garantisce tempi di risposta utili affinché l'ente possa rispondere agli interessati nei tempi previsti dalla normativa vigente.

2.3 Comunicazione dei dati

Le richieste di comunicare dati devono venire direttamente dall'ente, dai referenti specificati in fase di accordo o di suoi aggiornamenti. Ogni richiesta pervenuta da altri canali sarà scartata.

Regione Toscana potrebbe ricevere richieste dalle Forze dell'ordine o dalla magistratura. In questi casi ~~ha~~ attiva una procedura per la loro gestione. Se non richiesto direttamente dalle Forze dell'ordine o dalla magistratura, Regione Toscana informa il prima possibile l'ente della richiesta.

2.4 Uso di sub-fornitori

L'ente autorizza Regione Toscana ad affidare, sotto la propria responsabilità, l'esecuzione di operazioni di trattamento a soggetti terzi (c.d. sub-fornitori), che non siano situati in Paesi Extra-UE.

Fanno eccezione i trasferimenti a sub-fornitori che abbiano adottato le seguenti misure esplicitamente previste dalla normativa applicabili:

- una dichiarazione di adeguatezza del Paese di provenienza, confermata dalla pubblicazione sul sito della Commissione europea;
- BCR (o Binding Corporate Rules o norme vincolanti d'impresa) confermate dalla pubblicazione sul sito della Commissione europea;
- contratto con il sub-fornitore basato sulle clausole tipo di protezione dei dati.

Il ricorso a sub-fornitori è condizionato alla sottoscrizione di un contratto tra Regione Toscana e il sub-fornitore che includa i medesimi (o più stringenti) requisiti del presente contratto.

L'ente si riserva il diritto di chiedere in ogni momento a Regione Toscana l'elenco dei suoi sub-fornitori che possono avere accesso (in virtù del contratto di sub-fornitura) ai dati personali dell'ente.

3 Caratteristiche di base

I servizi IaaS e PaaS sono erogato dal Data center TIX. Essi sono rivolti a tutti gli Enti aderenti (Regione Toscana, SST, comuni, ecc.).

4 Caratteristiche tecniche

Se pure nell'ambito di una infrastruttura di cloud privato, considerato che i servizi sono erogati a diversi *tenant*, quindi con ambiti di titolarità, responsabilità e governo distinti, i servizi del Data Center TIX sono erogati secondo le modalità tipiche del cloud computing: sono quindi classificati come IaaS, PaaS e SaaS, dove il cloud provider è individuato nell'infrastruttura stessa, di proprietà di Regione Toscana e gestita da un appaltatore di servizi di gestione. Il *cloud consumer* sarà una Amministrazione.

Alla infrastruttura virtualizzata (VMware) su architettura x86_64 si affianca l'infrastruttura fisica (mista X86_64 e PowerPC) essenzialmente delegata al supporto di RDBMS proprietari.

Tutti i sistemi, fisici e virtuali, sono suddivisi tra sistemi di **produzione** e **staging**.

4.1 Servizi IaaS

I servizi Infrastructure as a Service (IaaS) sono erogati dall'infrastruttura di calcolo virtualizzata come una o più Macchine Virtuali (VM) con capacità computazionale, di memorizzazione, e di rete, sulle quali l'utente può installare ed eseguire il software a lui necessario, dal sistema operativo alle applicazioni. Se necessario le macchine virtuali possono essere connesse tra di loro da una rete virtuale (VLAN). Le macchine virtuali sono raggiungibili per la loro gestione tramite VPN via accesso Internet.

Il servizio è basato sul sistema di virtualizzazione “Vmware vSphere 5” e offre potenza elaborativa x86_64 con le seguenti caratteristiche principali:

- LUN (boot + dati) per ogni VM attestate su storage di classe enterprise;
- connettività SAN realizzata con switch/director fibre channel a doppia fabric per garanzia della ridondanza dei collegamenti;
- connettività LAN completamente integrata all’interno della infrastruttura LAN del TIX utilizzando sistemi di Link Aggregation (802.3AD) e di tagging delle vlan (802.1Q);
- backup base della VM con tecnologia “ifincremental” e retention di 15 giorni e gestione dei restore.

Il modello di gestione prevede che una volta installato sulla VM il S.O. ospite, al “utente” sia comunicata la credenziale di accesso al sistema (con diritti di amministratore); tipicamente nessuna funzione del hypervisor è delegata al “utente”, così come qualsiasi attività sistemistica che richiedesse l'intervento da console. Ogni richiesta di risorse aggiuntive (disco, RAM, VCPU), viene gestita dal presidio di gestione, previa autorizzazione della Amministrazione proprietaria dei sistemi.

Il servizio di gestione dei servizi IaaS, oltre ai servizi base applicabili previsti dal Capitolato Tecnico dell'AQ al Capitolo 5, deve garantire:

1. la gestione, configurazione e tuning continuo degli host ESXi e di tutte le funzionalità del sistema di virtualizzazione necessarie
2. la gestione, configurazione e tuning continuo del sistema di Storage e SAN che espone le LUN al sistema di virtualizzazione.

4.2 Caratteristiche dei servizi di tipo PaaS

Per i servizi Platform as a Service (PaaS) si intendono quei servizi di gestione dello strato di software che si colloca sopra il S.O. (middleware) e che tipicamente consente l'esecuzione di applicazioni, o l'erogazione di un servizio infrastrutturale (http server, name server, ntp server, mail server, ...), o il data-tier di un sistema informativo, come un database management system ed il relativo set di dati. Devono essere supportate sia tecnologie open source che proprietarie.

Per i servizi Software ad a Service (SaaS) si intendono quei servizi di gestione di applicativi che già di per se sono in grado di erogare un servizio completo (come ad esempio l'erogazione di un servizio di caselle di posta elettronica evoluta multi-canale).

Il modello di gestione prevede che per questi servizi sia il presidio di gestione ad operare sui sistemi, gestendo tutte le richieste di configurazione e dispiegamento di applicazioni che arrivano dall'utente o dal fornitore delle applicazioni indicato dall'utente. In questo scenario è l'organizzazione del presidio di gestione ad assicurare il rispetto dei livelli di servizio, codificati secondo gli Indicatori di Qualità, meglio definiti nel seguito.

Fanno parte di questa categoria tutti i pacchetti di servizi infrastrutturali, middleware, application server, portal server, directory server, sistemi di gestione di database, data analytics e quanto altro citato nell'Appendice 1-A, Contesto Tecnologico.

Ove previsto dal sistema/applicazione in questione, possono essere previste due differenti tipologie di configurazione: standalone (singola istanza) o cluster (due o più istanze con la medesima configurazione). Un cluster è sempre considerato come un singolo sistema PaaS da gestire.

Si considerano **sistemi semplici** i server di servizi infrastrutturali (name server, mail server, ntp server, ldap server, web server, servlet container come Tomcat, ...). Sono considerati complessi gli altri sistemi (Jboss, i server per i servizi di Business Intelligence e Data analytics, i message broker, ecc.).

Il servizio di gestione dei servizi PaaS/SaaS, oltre ai servizi base applicabili previsti dal Capitolato Tecnico dell'AQ al Capitolo 5, deve:

(a) provvedere alla attività di supporto ed assistenza all'utenza tramite apposito service desk, accessibile tramite le modalità e con i livelli di servizio illustrati nella successiva specifica sezione di questo Capitolato tecnico;

(b) provvedere all'aggiornamento dei server virtuali, all'applicazione delle patch di sicurezza e di ogni altro aggiornamento ritenuto utile, garantendo nel contempo la funzionalità di eventuali applicativi terze parti ivi dispiegati. A tal fine dovranno essere attentamente valutati dal Fornitore i rischi e tutti i possibile effetti collaterali di eventuali aggiornamenti di middleware e sistemi operativi sugli applicativi attivi: tali valutazioni dovranno essere condivisi con le Amministrazioni titolari o loro delegati;

(c) essere garantita la collaborazione con eventuali fornitori esterni che per conto delle Amministrazioni titolari gestiranno le componenti applicative specifiche.

(d) Per i servizi di gestione dei database il Fornitore, oltre alle operazioni già previste per un servizio PaaS/SaaS, dovrà effettuare le operazioni di amministrazione di un database più comuni, tra cui a titolo esemplificativo e non esaustivo, le seguenti:

i. definizione di nuove istanze, siano esse singole, cluster e HA

ii. configurazioni particolari e modifiche di parametri di configurazione

iii. riorganizzazione/compattamento di tabelle/database

iv. tuning di parametri di memoria di istanza, database, buffer pool

v. analisi del piano di esecuzione delle query e conseguenti azioni volte a ottimizzare le performance quali ad esempio aggiunta/modifica/eliminazione di indici

vi. refresh statistiche

vii. separazione/segmentazione di istanze-db/bancadati/schema/tabella

viii. reportistica settimanale sulle prime 10 “long running query”

ix. creazione/gestione utenze e assegnazione/modifica/revoca dei relativi diritti; deve essere prevista la possibilità per alcuni utenti autorizzati di eseguire operazioni di DML (Data Manipulation Language) e DDL (Data Definition Language) in autonomia.

x. Gli spostamenti dati all'interno della stessa piattaforma (es. da db2 a db2 o da postgresql a postgresql, ecc.) sono inclusi nel servizio.

4.3 Caratteristiche crittografiche

L’accesso alle macchine ospitate nel Datacenter (Iaas e PaaS) avviene attraverso canali cifrati (VPN) Non è concesso l’accesso diretto ai server in modalità non sicura.

Le istanze PaaS espongono i servizi solamente su protocolli cifrati (es: HTTPS, SFTP, ARPA, SPID, MFA).

L’esposizione dei servizi dalle istanze IaaS è a carico dell’ente.

Per quanto riguarda le istanze PaaS non sono al momento attivi meccanismi di crittografia automatica dei dati, l’attivazione di tali sistemi è prevista su richiesta dell’ente.

Ove richiesto sono stati attivati strumenti di pseudonimizzazione del dato configurati nel rispetto delle direttive ricevute dall’ente o dal titolare del trattamento.

4.4 Gestione utenze e autorizzazioni

Per i clienti del servizio IaaS sono fornite le utenze di amministrazione (root o admin) delle macchine consegnate e quelle della VPN di accesso. È pertanto responsabilità dei clienti modificare le user-id, le password assegnate e le autorizzazioni utilizzando le funzionalità dei sistemi operativi o del middleware o anche modificare il meccanismo di connessione (ossia la VPN).

Per il servizio PaaS sono consegnate utenze:

- l'accesso standard è fornito attraverso la piattaforma ARPA (a sua volta accessibile via SPID, CNS o CIE);
- nel caso di container, l'ente chiede al TIX di installare i componenti, inclusi quelli di I&A; pertanto è sua responsabilità la scelta di usare o meno strumenti di autenticazione a più fattori;
- per le applicazioni (p.e. DBMS), l'utente accede via VPN e poi con user-id e password (quindi due fattori perché uno è VPN e poi accesso all'applicazione);
- nel caso di applicazioni, l'utente non dispone di utenze amministrative, ma può gestire autonomamente i profili applicativi e, dove previsto, definire le utenze.

Gli accessi via SPID e ARPA sono di tipo MFA (multi-factor-authentication).

4.5 Segregazione delle reti

Per le reti fisiche e le reti virtuali sono applicate le seguenti regole:

- Tutti gli ambienti IaaS, PaaS e SaaS sono segregati in termini di VLAN; in particolare gli ambienti IaaS sono attestati su VLAN dedicate ad ogni cliente;
- tutti gli ambienti sono separati da Internet da un cluster di firewall, con anche policy antiDoS (Denial of Service) e IPS.

4.6 Monitoraggio e log

Il cliente:

- può accedere al monitoraggio standard (uso CPU, occupazione memoria, eccetera) per IaaS su richiesta; monitor.tix.it con CNS;
- in caso usufruisca di servizi IaaS, può installare autonomamente strumenti ulteriori per monitoraggi specifici o fare richiesta al gestore TIX;
- può accedere al monitoraggio in tempo reale SLAM (slam.tix.it), con accesso via CNS (ARPA - SPID).

Il gestore del TIX, a sua volta, dispone di numerosi strumenti di monitoraggio. Nel caso siano attivati degli allarmi, il gestore del TIX avverte il cliente. Per esempio nei casi di:

- troppi tentativi di accesso non autorizzato;
- superamento quote;
- Virus, intrusioni rilevate via IDS.

Per quanto riguarda i log, sono raccolti con strumenti di log collecting. In questo modo, essi sono anche protetti dal controllo degli accessi impostato per questi stessi strumenti.

L'uso di strumenti di log collecting e di un SIEM assicurano il riesame costante e automatico degli eventi.

Riesami manuali sono svolti solo in caso di eventi particolari.

4.7 Clock di sistema

L'NTP è erogato da due server presso il TIX, a loro volta sincronizzati con un pool di server riconosciuto come affidabile a livello di comunità Internet. Il controllo di affidabilità è effettuato ad ogni sincronizzazione. I sistemi presso il TIX, per assicurare il livello di sicurezza, non si possono collegare autonomamente ad NTP server esterni.

4.8 Chiusura del servizio

In occasione della chiusura di una VM o un ambiente, l'intera VM è cancellata con gli strumenti messi a disposizione dall'hypervisor.

Copie dei dati sono mantenute nei backup fino alla conclusione della loro rotazione.

5 I livelli di servizio

Indicatori di qualità operativi sono i seguenti:

a. IQ10 – Disponibilità dei Servizi: il valore soglia, con cadenza trimestrale, è definito in modo distinto per i servizi di produzione e per quelli di staging:
   i. valore soglia di IQ10_SP (servizi di produzione) = 99,90%
   ii. valore soglia di IQ10_SS (servizi di staging) = 99,70%
b. IQ11 – Disponibilità dei Sistemi (con cadenza trimestrale)
c. IQ12 - Tempestività di risoluzione degli incident: le priorità (con cadenza trimestrale) sono così definite:
   i. Servizio di Produzione
      - Priorità 1: guasto bloccante 3 ore in orario di lavoro O3 (quindi equivalenti a solari)
      - Priorità 2: guasto non bloccante 8 ore in orario di lavoro O3 (quindi equivalenti a solari)
   ii. Servizio di Staging
      - Priorità 3: guasto bloccante 6 ore in O2
      - Priorità 4: guasto non bloccante 22 ore in O2
d. IQ13 - Tempestività di esecuzione (con cadenza trimestrale) dei change standard/predefiniti, le classi sono così ri-definite:
   i. classe 1 – tempo massimo di esecuzione 1 h
   ii. classe 2 – tempo massimo di esecuzione 2 h
   iii. classe 3 – tempo massimo di esecuzione 4 h
   iv. classe 4 – tempo massimo di esecuzione 8 h
   v. classe 5 – tempo massimo di esecuzione 16 h
e. IQ14 - Tempestività di esecuzione dei change non standard
f. IQ15 – Ticket oggetto di ripianificazione
g. IQ16 - Attività eseguite correttamente.

6 Help desk

È fornito dal presidio un servizio di Helpdesk, con obiettivi elencati nel paragrafo precedente.

L'Helpdesk risponde a:

- Numero verde 800.155.715;
- email operation@tix.it;
- ticket aperti dal portale www.tix.it.

L'Helpdesk riceve segnalazioni di eventi, richieste di servizio, richieste di chiarimenti.

Per ogni comunicazione è aperto un ticket gestito con uno strumento apposito e con workflow di trattamento impostato basandosi sulle pratiche ITIL.

7 Gestione degli incidenti

Sono incidenti di sicurezza informatica: uno o più eventi di sicurezza informatica, non voluti o non attesi, che hanno una probabilità significativa di compromettere le informazioni e minacciare la riservatezza, integrità e disponibilità delle informazioni sui sistemi informatici.

Esempi di incidenti relativi alla sicurezza informatica sono:

- rottura o furto o danneggiamento di componenti infrastrutturali;
- errori umani;
- non rispetto delle regole di sicurezza fisica;
- accessi fisici o informatici non autorizzati;
- eventi che portano alla indisponibilità dei sistemi informatici del TIX.

7.1 Segnalazione di incidente

Ogni evento, incidente o vulnerabilità riscontrati devono essere comunicati alle opportune strutture in modo da garantirne un rapido trattamento. I clienti devono comunicare gli incidenti all'help desk.

7.2 Trattamento degli incidenti di sicurezza informatica

Per ogni attività, il NOC del gestore segue le proprie procedure.

Se l'incidente comporta interruzioni di servizio prolungate o può portare alla diffusione o alterazione di dati critici (es. dati personali o dati economici), il Direttore di Esecuzione (o suo Assistente o delegato) del servizio pertinente lo comunicano al RUP, ai responsabili delle applicazioni e agli enti aderenti al servizio.

Ogni incidente è oggetto di approfondite analisi per verificare quali dati sono stati compromessi, in particolare i dati personali.

7.3 Rapporto sugli incidenti di sicurezza

In caso di incidenti di sicurezza, è predisposto un rapporto con indicato:

- descrizione dell'evento;
- data di occorrenza e data di segnalazione;
- le azioni eseguite;
- gli elementi che hanno consentito di considerare l'evento risolto;
- data di chiusura della segnalazione.

7.4 Comunicazioni relative a violazioni di dati personali (data breach)

In caso di incidenti con impatto sui dati personali (in particolare se l'incidente ha permesso a persone non autorizzate ad accedere ai dati personali) il Gestore del TIX li comunica al Direttore di esecuzione.

Il Gestore del TIX e il Direttore di esecuzione valuta se la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche.

Se l'incidente presenta un rischio per i diritti e le libertà delle persone fisiche, Direttore di esecuzione, in accordo con il RPU, inoltra segnalazione a:

- il Garante per la protezione dei dati personali entro 72 ore dalla rilevazione dell'incidente (se Regione Toscana è titolare del trattamento);
- gli enti titolari dei dati coinvolti dall'incidente entro 24 ore.

La segnalazione riporta:

a) l'evento;
b) la natura della violazione dei dati personali compresi le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
c) il nome e i dati di contatto di Regione Toscana;
d) le probabili conseguenze della violazione dei dati personali;
e) le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi (quest'ultimo punto può essere incluso in una versione successiva del rapporto).

Se Regione Toscana è titolare del trattamento, la medesima segnalazione è inviata agli interessati (è possibile escludere il numero e le categorie degli interessati e il numero di registrazioni). Tale comunicazione agli interessati non è necessaria se:

- i dati sono incomprensibili ad altri (per esempio sono cifrati);
- Regione Toscana ha attuato azioni per ridurre al minimo gli impatti sugli interessati.

7.5 Raccolta di prove

Nel caso sia ritenuto opportuno, potranno essere raccolte opportune prove per perseguire i responsabili dell'evento. In questo caso, è contattato l'Ufficio Legale di Regione Toscana per seguirne le istruzioni se non diversamente specificato dalle autorità competenti.

Gli enti aderenti possono sempre richiedere di raccogliere prove. In questo caso, prima di avviare le attività, dovrà essere contattato l'Ufficio Legale di Regione Toscana. I tecnici di Regione Toscana e del gestore del TIX dovranno collaborare al fine di non compromettere i servizi attivi (in caso di raccolte date "live") e i dati riservati, sia in caso di raccolte date live sia su supporti inattivi.

7.6 Caso specifico di compromissione di credenziali

In caso di compromissione di credenziali, le azioni vanno stabilite dall'ente. Il gestore del TIX, per quanto nelle sue mansioni, può fornire gli strumenti per condurre indagini e per re-inizializzare le credenziali assegnate.

8 Componenti Fisiche

Le componenti fisiche del servizio di conservazione sono localizzate in:

- sito primario, situato presso la struttura del TIX, via San Piero a Quaracchi 250, Firenze;
- sito secondario, avente almeno le stesse caratteristiche di sicurezza di quello primario ed utilizzato per erogare il servizio di Disaster Recovery (DR), presso il data centre di Cesano Maderno (MB) di Telecom Italia.