TMC REMOTE DATA PROTECTION

Backup & Disaster Recovery

1 – PREMESSA

La crescente quantità di dati presenti in azienda e la sempre più elevata importanza degli stessi, impone un'attenta definizione delle politiche di backup e disaster recovery da adottare per garantire indispensabili livelli di sicurezza. Un aspetto spesso trascurato è la disponibilità di una copia dei dati all'esterno del perimetro aziendale per tutelarsi da eventi catastrofici quali incendi, terremoti, furti e allagamenti.

Il backup deve considerare non solo il backup dei SERVER ma anche dei PC DESKTOP e PORTATILI.

Per quanto riguarda i server un'equilibrata e affidabile soluzione di BACK UP deve prevedere almeno due livelli separati e distinti:

1° LIVELLO – BACKUP LOCALE	2° LIVELLO – BACKUP REMOTO
FUNZIONALITA'	FUNZIONALITA'
Copia immagine del sistema operativo	Copia degli archivi dei dati fondamentali
Copia degli archivi dei dati	UTILITA'
Copia delle applicazioni	Disporre di una 2° copia da utilizzare nei casi di malfunzionamento del back up locale
UTILITA'	Consentire un recupero dei dati nei casi di eventi catastrofici che non rendono piu' disponibile il back up locale
Consentire un rapido restore a seguito di crash	
Consentire il restore automatico di file, applicazioni e database	

Per quanto riguarda il 1° livello di backup, quello locale, sono tante le soluzioni possibili. Di seguito invece verrà affrontata la soluzione delle problematiche relative al 2° livello di backup, il backup remoto.

2 - TMC REMOTE DATA PROTECTION - CARATTERISTICHE

A – Integrità e sicurezza dei dati

I dati dei Clienti sono ospitati all'interno di un'infrastruttura che garantisce i massimi livelli di sicurezza fisica, logica e protezione degli stessi da eventi critici. Il servizio viene erogato tramite una infrastruttura di Data Center certificati e specializzata nell'erogazione di servizi che richiedono elevati livelli di sicurezza, assistenza a ciclo continuo e capacità di connessione praticamente illimitata. E' un'infrastrutture pensata per l'erogazione di servizi di e-commerce, di e-trading e servizi applicativi critici, per garantire "no system failure" al fine di evitare ogni possibile impatto sul Servizio erogato e i dati gestiti. L'architettura tramite cui è erogato il servizio è distribuita e ridondata per garantire la massima continuità operativa a fronte di eventi critici. Le sale e l'intera infrastruttura sono progettati e realizzati per garantire i massimi livelli di continuità di Servizio e prestazionali. Tutti i parametri operativi e di sicurezza sono soggetti a monitoraggio H24 con l'attivazione di escalation in caso di allarmi.

CARATTERISTICHE DELL'INFRASTRUTTURA PER GARANTIRE LA CONTINUITA'

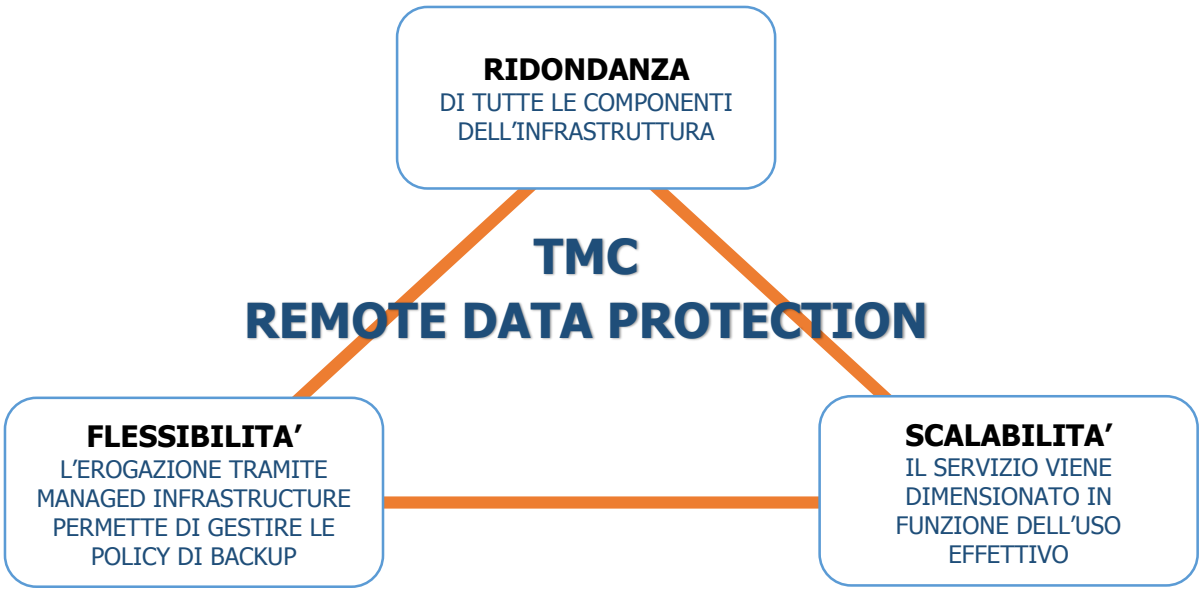
- Sistema di alimentazione elettrica completamente ridondata: linee di alimentazione con percorsi separati, ridondanza dei trasformatori principali e della distribuzione.
- Distribuzione elettrica tramite doppio circuito di blindo-sbarre che alimentano i sistemi di continuità che a loro volta, tramite due linee e quadri elettrici separati, distribuiscono energia alle sale. Rack e server installati ricevono una doppia sorgente di alimentazione che ne assicura la continuità anche durante gli interventi programmati di manutenzione generale.
- Continuità elettrica è garantita da gruppi di continuità (UPS) in configurazione parallela e ridondata e attivazione di sistemi di emergenza (gruppi elettrogeni).
- Generatori (in configurazione ridondata) che assicurano la completa autonomia per almeno 48 ore senza rifornimento di carburante. I locali dei generatori sono separati per evitare che un guasto di un gruppo elettrogeno possa compromettere l'efficienza degli altri gruppi.
- I gruppi di pompaggio del gasolio hanno una ridondanza di tipo N+1 e le cisterne sono a doppio contenimento. La garanzia di rifornimento di carburante avviene entro otto ore dalla richiesta.

B – Raggiungibilità del servizio

Il Servizio di TMC Remote Data Protection è accessibile attraverso Internet. L'accesso tramite rete Internet è incluso nel Servizio.

C – Architettura flessibile e scalabile

L'architettura completamente flessibile e scalabile permette di coniugare i vantaggi della soluzione Cloud con le esigenze di personalizzazione e flessibilità dei clienti. L'utilizzo delle più moderne tecnologie garantisce al cliente continuità di servizio e sicurezza nel tempo. La piattaforma di SINGULAR INFORMATION MANAGEMENT garantisce protezione e gestione semplificata di dati e informazioni di business, anche in cui casi di ambienti di storage complessi.



L'intera architettura è completamente modulare e composta di elementi virtualizzati con la possibilità di avere configurazioni personalizzate tipiche di una soluzione dedicata.

3 - TMC REMOTE DATA PROTECTION - DETTAGLI

Server Backup

A – Dati e sistemi supportati

SISTEMI OPERATIVI – FILE SYSTEM

SISTEMA OPERATIVO	VERSIONE
Mac OS X Server	Mac OS X v10.4.x, Mac OS X v10.5.x, Mac OS X v10.6.x
Windows server 2000, Microsoft Windows server 2003, Windows Server 2008, Microsoft Windows server 2012	32 bit, 64 bit
Novell NetWare	NetWare 6.5
Novell OES Linux	32 bit, 64 bit
Unix AIX, HP UX, Linux (Freebsd; Debian; Fedora; Gentoo; System Z; Mandriva; OpensuSE; Oracle Enterprise; Red Hat/Centos; Scientific; suSE; Ubuntu), Solaris, Tru64	32 bit, 64 bit

MIDDLEWARE – DATABASE

DATABASE	SISTEMA OPERATIVO	VERSIONE
Novell Directory Services	Novell OES2 Linux	32 bit, 64 bit
DB2	AIX, HP-UX, LINUX Red Hat Enterprise, LINUX SuSE, Linux on System z, SOLARIS, WINDOWS 2003-2008	32 bit, 64 bit
INFORMIX	AIX, HP-UX, LINUX Red Hat Enterprise, LINUX SuSE, SOLARIS	32 bit, 64 bit
MS SQL Server 2005-2008-2012	Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
MS MySQL	Unix AIX, HP UX, Linux (Debian; Gentoo; OpensuSE; Red Hat/Centos; Source Mage; Scientific; suSE; Ubuntu), Solaris, Windows (2003-2008)	32 bit, 64 bit
Oracle / Oracle Real Application Clusters (RAC)	Unix AIX, HP UX, Linux (Red Flag , Oracle Enterprise, System Z; Oracle Enterprise; Red Hat/Centos; SuSE), Solaris, Tru64	32 bit, 64 bit
PostGreSQL	Linux (Red Hat, Source Mage Linux, SuSE Linux)	64 bit

MIDDLEWARE – APPLICATION

APPLICATION	SISTEMA OPERATIVO	VERSIONE
SAP for MAXDB	AIX, HP-UX, Linux (ReD HAT, SUSE Linux), Solaris, Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
SAP for Oracle	AIX, HP-UX, Linux (ReD HAT, SUSE Linux), Solaris, Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
Active Directory	Windows Server 2003, Windows Server 2008	32-bit, 64-bit and x64 Editions with a minimum of Service Pack 1

Documentum	AIX, HP-UX, Linux (ReD HAT, SUSE Linux), Solaris, Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
Lotus Notes / Domino Server	AIX, Linux (ReD HAT, SUSE Linux), Solaris, Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
Microsoft Data Protection Manager (2006-2007-2010)	Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
Microsoft Exchange Database / Exchange Mailbox / Exchange Public Folder (2003-2007-2010)	Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
Microsoft SharePoint Server	Microsoft Window server 2003, Windows Server 2008	32 bit, 64 bit
Novell GroupWise	NetWare, Novell Open Enterprise Server (OES)	33 bit, 64 bit
Sybase	AIX, HP-UX, Linux (ReD HAT, SUSE Linux), Solaris, Microsoft Window server 2003, Windows Server 2008	33 bit, 64 bit

MIDDLEWARE – VIRTUAL ENVIRONMENT

APPLICATION	SISTEMA OPERATIVO	VERSIONE
Microsoft Hyper-V	Microsoft Windows Server 2008 Editions, Microsoft Hyper-V Server 2008 Editions	64 bit
Vmware ESX (3.4/4.0/4.1/5.0)	All Guest Operating Systems supported by vSphere vStorage API for Data Protection (VADP) and VMware Consolidated Backup (VCB)	
Citrix XenServer (5.5/5.6)	Microsoft Windows Server 2003; Microsoft Windows Server 2008	32 bit, 64 bit

HARDWARE – NETWORK ATTACHED STORAGE (NAS)

VENDOR	SUPPORTED NETWORK DATA MANAGEMENT PROTOCOL (NDMP) FILE SYSTEM
BlueArc	Up to BOS 8.0
Dell Scalable File System	1.0
EMC Celerra	DARTOS 5.5, 5.6, 6.0, 7.0
Hitachi	03-07, Data Ingestor 2.2.1
Hitachi HNAS	Up to BOS 8.0
HP X9000	5.5
Isilon	6.5
NetApp	Up to ONTAP 8.0, ONTAP 10
Pillar Data Systems	4.3
SUN 5320	4.22M1
SUN 7000	ak-2009.09.01, 2010.02.09, 2010.08.17

NOTA BENE: Le informazioni sopra riportate sono indicative e soggette a continuo aggiornamento da parte di TEAM MEMORES COMPUTER.

B – Configurazione e gestione

In caso di Managed Infrastructure, il Servizio di remote backup è configurato e gestito tramite interfaccia web di amministrazione studiata per offrire la massima facilità di utilizzo e la migliore user experience. Attraverso tale interfaccia è possibile, con poche operazioni, configurare le politiche di backup e applicarle a ciascun server o a loro gruppi. Anche le operazioni di restore sono assistite da procedure semplici per il ripristino dei dati e rispondere alle più stringenti esigenze delle aziende.

FUNZIONE	CARATTERISTICHE
Esecuzione del Backup	Monitoraggio del progresso del Job dal Job Controller e/o dall'Event Viewer
Esecuzione del Restore	Opzioni di Overwrite File e Restore to Same Folder
	Specifica del Path di destinazione tramite il tasto Browse
	Nessun file esistente viene sovrascritto

C – Protezione dati

Il software permette di crittografare i dati sia per la trasmissione su reti non sicure sia per l'archiviazione degli stessi su supporti digitali. La flessibilità di gestione delle chiavi rende possibile la cifratura dei dati in una vasta gamma di configurazioni. E' possibile cifrare i dati a livello client (sulla macchina che ospita i dati da proteggere), durante il trasferimento verso il repository centralizzato oppure al momento del salvataggio degli stessi presso il repository centrale. La crittografia a livello di client permette agli utenti di proteggere i dati prima che questi siano inviati alla piattaforma centralizzata.
È possibile scegliere tra diversi algoritmi ed estensioni delle chiavi come indicato nella tabella seguente:

DATA ENCRYPTION ALGORHITMS

CHIPHER	DETAILS	BLOCK SIZE	PERFORMANCE RATING*	KEY LENGTH OPTIONS
BLOWFISH	• Symmetric Key Block Cipher • Fast (fastest of the ciphers supported) • Secure • Finalist in the Advanced Encryption Standard Content	64 bits	10	128, 256 bits
AES (Advanced Encryption Standard) or RIJNDAEL	• Symmetric Key Block Cipher • Fast • Secure • Winner of the Advanced Encryption Standard Content • Adopted as the Government Standard (Only cipher approved by the National Security Agency to be used for top-secret information.)	128 bits	7	128, 256 bits
SERPENT	• Symmetric Key Block Cipher • Fast • Very Secure (Considered more secure than AES) • Finalist in the Advanced Encryption Standard Content	128 bits	8	128, 256 bits

TWOFISH	• Symmetric Key Block Cipher • Secure • Not standardized • Finalist in the Advanced Encryption Standard Content	128 bits	4	128, 256 bits
3-DES (Triple Data Encryption Standard)	• Symmetric Key Block Cipher • Slow • May be susceptible to certain attacks	64 bits	1.5	192 bits

* Questa valutazione a livello di prestazioni è basata su test di performance sul numero di megabytes per secondo criptati in un sistema Windows. Le valutazioni sono in un range che va da 1 a 10, dove 10 indica il risultato migliore, quindi più veloce. I risultati possono variare a seconda dell'ambiente di test.

D – Trasferimento dati

Per ridurre l'impatto sulle risorse di rete durante il backup e il restore dei dati, la soluzione TMC effettua la deduplica sia lato client sia a livello di repository centrale. La deduplica agisce a livello di singolo blocco / segmento in modo da evitare il rischio di errata associazione tra questi e il corrispondente client, desktop o sede e prevede la gestione di un unico repository logico. Inoltre, il sistema adotta tecnologie di compressione dei dati. Queste features assicurano l'utilizzo ottimale delle risorse IT ottimizzando le performance e il rapporto costi-benefici.

E – Job Monitoring: gestione Job di Backup tramite device mobili

Il Servizio permette agli amministratori di sistema di:

- ✓ Monitorare i Job di Backup (Job in esecuzione, Job in attesa, Job non andati a buon fine);
- ✓ Conoscere le motivazioni dei Job in attesa;
- ✓ Sospendere, riprendere e cancellare un Job di Backup

MOBILE JOB MONITORING è disponibile per:

- ✓ Apple iPad, Apple iPod Touch, Apple iPhone
- ✓ Android based devices
- ✓ Blackberry (OS6)
- ✓ Web browser: Mozilla Firefox, Google Chrome, Apple Safari.

FUNZIONALITA' DI MOBILE JOB MONITORING: Il servizio permette di effettuare la ricerca del Job sulla base del Job ID, della Tipologia (in attesa, in esecuzione, falliti.) o dello Status. Per ciascun Job sono disponibili informazioni generali, informazioni relative allo stato di avanzamento e informazioni sui tentavi di esecuzione del Job. È inoltre possibile gestire ciascun Job cancellandolo, sospendendolo e riattivandolo

Desktop & Laptop Backup

Il Servizio TMC REMOTE DATA PROTECTION - DESKTOP & LAPTOP è dedicato alle aziende che desiderano garantire sicurezza e continuità operativa dei Desktop & Laptop aziendali, anche in condizioni di mobility.

A – Plus del servizio

SICUREZZA	La trasmissione dati è resa sicura dall'adozione di protocolli che permettono la cifratura dei dati (SSL certificates for authentication and encryption). Questo garantisce la massima sicurezza anche durante operazioni di backup eseguite al di fuori della VPN e reti MPLS. L'accesso al Servizio è regolato mediante autenticazione e profilazione utenti per impedire, anche in caso di furto del PC, l'accesso al Servizio da parte di utenti non autorizzati.
RECOVERY	Il sistema è in grado di interrompere temporaneamente la procedura di backup in caso di mancanza di connettività e riavviarla quando la rete è disponibile, senza perdita di dati e senza dover riprendere il backup dall'inizio. Questa feature migliora la "user experience" e agevola gli Utilizzatori finali del Servizio che per motivi di lavoro sono spesso fuori sede e non connessi alla rete.
DEDUPLICA E COMPRESSIONE DATI	Per ridurre l'impatto sulle risorse di rete durante il backup e il restore dei dati, la soluzione TMCEnìa effettua la deduplica sia lato client sia a livello di repository centrale. La deduplica agisce a livello di singolo blocco / segmento in modo da evitare il rischio di errata associazione tra questi e il corrispondente client, desktop o sede e prevede la gestione di un unico repository logico. Inoltre, il sistema adotta tecnologie di compressione dei dati. Queste features assicurano l'utilizzo ottimale delle risorse IT ottimizzando le performance e il rapporto costi-benefici.
BACKUP INCREMENTALE	Oltre alla deduplica e alla compressione dei dati, il Servizio prevede modalità di backup incrementale a livello di sub-file (block)
BACKUP POLICY	Il Servizio permette la definizione di politiche di backup anche personalizzate dei dati, opzioni di conservazione di più versioni degli -stessi e la preventiva verifica della disponibilità delle risorse necessarie lato Endpoint (PC connesso ad una rete elettrica, utilizzo di CPU non superiore ad una soglia predefinita, appartenenza ad una subnet, connessione WAN sufficiente, …). Tali features, unitamente alla possibilità di disporre dei dati sia centralmente che localmente, agevola le operazioni di self-restore da parte dell'end user nel rispetto degli obiettivi di ripristino
COMPLETA AUTOMAZIONE DELLE PROCEDURE DI BACKUP	Per ridurre al minimo gli impatti sulla produttività e la continuità operativa, il Servizio è semplice da utilizzare, non richiede l'intervento dell'utente finale e neanche la sospensione dell'attività lavorativa durante l'esecuzione del backup. La schedulazione del backup può essere parametrizzata, oltre che temporalmente, in funzione di parametri quali la disponibilità di risorse di sistema (es. % di utilizzo della CPU) e del collegamento alla rete aziendale.
FACILITA' DI UTILIZZO	La gestione del Servizio lato client è semplice e intuitiva e avviene tramite una console accessibile via web. Le operazioni di restore possono essere eseguite direttamente dagli utenti finali e non richiedono l'intervento e l'assistenza di risorse IT centrali
CONTROLLO CENTRALIZZATO	Il Servizio prevede la possibilità di definire centralmente le policy di backup e l'esecuzione delle stesse per differenti tipologie di endpoint / user / gruppi, di definire le casistiche di generazione degli allarmi riducendo i rischi connessi alla sicurezza e i costi di gestione. La distribuzione degli aggiornamenti sw agli Endpoint è centralizzata, automatica e non richiede l'intervento dell'utente finale. La possibilità di controllare centralmente le operazioni di backup migliora la governance e il rispetto degli obiettivi di backup.

B – Caratteristiche Tecniche del servizio

CLIENT	• Ampio range di sistemi operativi supportati: Windows (Windows 7, Windows Vista, Windows XP), Linux, MacOSX • Scheduling ottimizzato (il backup viene eseguito quando il sistema rileva il collegamento alla rete) • Installazione policies intelligente ed automatizzata, silent push and install
PROTECTION	• Data files e Sistema (System State, Volumes, Files) • Completa cifratura di tutte le copie
DESTINATION	• Immagini di backup deduplicate • Deduplica in formato sicuro, cifrabile • La deduplica globale riduce lo spazio complessivo utilizzato
DATA TRANSFER	• HTTPs based con controllo globale dal Client al sistema di storage • Include certificati SSL per autenticazione e cifratura • Trasmissione sicura, set-up semplificato • Elimina la necessità di VPN, consente la protezione dei laptops via Internet
FAILOVER	• Completo failover e bilanciamento lato server • Oltre 300 streams concorrenti per VM
WORKLOAD	• Deduplicazione a livello Client – solo i dati modificati rispetto al database centrale sono trasferititi • Carichi di lavoro suddivisi tra i vari elementi dell'architettura in modo da ottimizzare le performance
ADMINISTRATOR INTERFACE	• In caso di Managed Infrastructure, il Servizio di remote backup é configurato e gestito tramite interfaccia web di amministrazione studiata per offrire la massima facilità di utilizzo e la migliore user experience.
USER INTERFACE	• End-user Web Desktop & Laptop Console – accessibile ovunque, consente il restore diretto o il download dei dati o modificare la schedulazione dei backup • Policy configurabili con granularità fino al singolo file • Semplice interfaccia di browsing per localizzare i dati da recuperare • Gestione avanzata dei livelli di autorizzazione (delegati, amministratori etc.)
DATA AVAILABLE	• Possiblità di accedere ai propri dati attaverso una qualsiasi postazione di lavoro compresi tablet e pda

C – Configurazione e Gestione del servizio

In caso di Managed Infrastructure, il Servizio di remote backup è configurato e gestito tramite interfaccia web di amministrazione studiata per offrire la massima facilità di utilizzo e la migliore user experience. Attraverso tale interfaccia è possibile, con poche operazioni, configurare le politiche di backup e applicarle a ciascun server o a loro gruppi. Anche le operazioni di restore sono assistite da procedure semplici per il ripristino dei dati e rispondere alle più stringenti esigenze delle aziende

FUNZIONE	CARATTERISTICHE
Esecuzione del Backup	Monitoraggio del progresso del Job dal Job Controller e/o dall'Event Viewer
Esecuzione del Restore	Opzioni di Overwrite File e Restore to Same Folder Specifica del Path di destinazione tramite il tasto Browse Nessun file esistente viene sovrascritto

D – End-User Web Desktop Console

D1 – Caratteristiche del Servizio

- Autonomia di gestione dei restore / download.
- Unica console di gestione di tutti i desktop di cui si è "owner".
- Con le le policy da Admin possono fissare i path per la protezione dei dati.
- L'utente ha la possibilità di aggiungere path supplementari per soddisfare le proprie esigenze.
- E' possibile applicare dei filtri di esclusione per ridurre la dimensione del backup su dati non criticiGestione dei diritti di ciascun utente/owner ai fini della sicurezza.
- E' possibile aggiungere l'utente specificandone il dominio (DOMAIN\user) o semplicemente l'utente – questo utente verrà automaticamente aggiunto nel profilo di sicurezza definito.
- Per grandi ambienti distribuiti questo consente un'associazione 1:1 e la possibilità di delegare laddove più utenti siano assegnati alla stessa macchina.

D2 – Funzionalità Tecniche del Servizio

- Avviare le operazione di backup o controllare le operazioni in corso (sospendi / riprendi / annulla).
- Verificare il livello di protezione (ultima esecuzione, esecuzione successiva, schedulazione).
- Possibilità di visualizzare le job history.
- L'utilizzo dell'opzione Find consente di effettuare delle semplici ricerche basate sui meta dati dei file.
- Possibilità di selezionare gli elementi di cui effettuare il Restore o il Donwload direttamente dai risultati della ricerca.
- Ottimizzazione della banda WAN (in ingresso e in uscita) in specifiche finestre di operatività.
- Opzioni Firewall/Networking che consentono di definire la banda (Kbps) sia in ingresso che in uscita dal client. Gli amministratori possono impostare specifiche policy per ridurre l'utilizzo di banda durante le operazioni di backup/restore durante le ore diurne. Questo può essere impostato sia sul singolo client sia su un gruppo di client.

4 – TMC REMOTE DATA PROTECTION – MODALITA' DI GESTIONE DEL SERVIZIO

A – Managed Infrastructure

Il Servizio prevede l'outsourcing della gestione operativa delle componenti infrastrutturali del Servizio di TMC Remote Data Protection. Di seguito le attività/responsabilità in caso di Managed Infrastructure:

N.	Attività
1	Manutenzione, Gestione e Monitoring dell'infrastruttura
2	Definizione delle politiche di Backup e Restore
3	Installazione Agent su client (Desktop / Laptop)
4	Installazione Agent su client (Server)
5	Schedulazione backups
6	Esecuzione delle procedure di Restore Desktop / Laptop
7	Esecuzione delle procedure di Restore Server
8	Creazione, modifica, cancellazione Utenti/profili e gestione accesso al Servizio di Backup
9	Gestione sicurezza (configurazione e gestione firewall e security policies piattaforma centrale)
10	Manutenzione / Aggiornamento software di backup (lato piattaforma centrale)
11	Manutenzione / Aggiornamento software di backup (lato client)

B – Integrazione Backup Locale (opzione a progetto)

TMC Remote Data Protection si integra con le soluzioni di back esistenti. L'eventuale valutazione/implementazione della soluzione locale saranno soggette a progetto separato.

4 - TMC REMOTE DATA PROTECTION – DISPONIBILITA' DEL SERVIZIO

La disponibilità del Servizio TMC Remote Data Protection è garantita al 99,90% del tempo su base annua.

5 - TMC REMOTE DATA PROTECTION – SUPPORTO TRAMITE SERVICE DESK

TMC mette a disposizione dell'Amministratore di sistema del cliente (o persona da lui nominata) un punto di contatto cui far pervenire tutte le richieste inerenti la gestione del servizio. Il Service Desk riceverà e registrerà le richieste relative a segnalazioni di Incident, Service Requests o Change Request.

6 - TMC REMOTE DATA PROTECTION – PROFESSIONAL SERVICE (A PROGETTO)

Oltre al Servizio TMC Remote Data Protection, TMC mette a disposizione del cliente servizi professionali che aiutano le organizzazioni ad avere una comprensione approfondita di specifiche tematiche ed esigenze inerenti la protezione dei dati in azienda, eseguendo analisi, studi e producendo deliverable contenenti raccomandazioni e "piani d'azione". Per ciascuna fase di un progetto di Remote Backup, TMC mette a disposizione le seguenti competenze e servizi:

A - Servizi di Assessment e Design

- Determina i requisiti necessari per l'identificazione della soluzione di TMC Remote Data Protection;
- Design della soluzione in grado di soddisfare le esigenze del cliente;
- Sviluppa e condivide i piani d'implementazione della soluzione.

B - Servizi di Implementazione

- Implementazione architettura e configurazione del Servizio nel rispetto degli obiettivi di progetto;
- Creazione di processi e documentazione, specifici per ogni cliente, che dettagliano le soluzioni e presentano i requisiti di supporto e di gestione (piano di attuazione, guida operativa, guida installazione / aggiornamento).

C - Gestione del ciclo di vita del progetto

- I Project Manager TMC lavorano in stretta collaborazione con il management del cliente per definire in modo accurato le difficoltà legate al progetto, le fasi dello stesso e le attività necessarie per lo svolgimento dei task per il raggiungimento dei target. Per tutta la durata del progetto, il PM TMC controlla e comunica costantemente l'avanzamento dello stesso e garantisce il livello di qualità e l'allineamento dei tempi, dei costi e dei deliverable con gli obiettivi del progetto.