Frosinone, 9 gennaio 2018

Spett.Le

c.a.

Ogg. Compliance servizi erogati ai sensi del Dlgs 196/2003 e successive modificazioni, integrazioni e interpretazioni

In relazione alla richiesta pervenuta dichiariamo che la nostra azienda ha provveduto alle prescrizioni di legge in tema di trattamento e tutela dei dati sensibili e personali. Ha inoltre predisposto le procedure di audit e di controllo necessarie.

In allegato un estratto del nostro DPS con particolare riferimento al servizio erogato ed alle misure adottate.

Il responsabile per il trattamento è il sig. Enrico Vona mentre il coordinatore tecnico responsabile degli amministratori di sistema è il Sig. Fabio Fedele entrambi domiciliati, per il ruolo, presso la sede di c.so Lazio, 9/a – Frosinone.

E' previsto un meccanismo di delega operativa per la gestione dei sistemi sottoposta ad opportuno censimento e tracciamento, come dettagliato del documento allegato a titolo "integrazione dlgs 196/2003 – amministratori di sistema".

Antonio Baldassarra
Amm.ne Unico

Estratto delle procedure e metodi di sicurezza attuate sui servizi di Cloud computing denominati "Cloud Server e Cloud Infrastructure" comprendenti tutte le Cloud appliance e il servizio denominato Object Storage, ai sensi del Dlgs 196/2003 e successive modificazione, integrazioni e interpretazioni

Descrizione datacenter

Possediamo i seguenti datacenter tutti in proprietà e in completa nostra gestione; tutti certificati ISO 9001, ISO 27001, ISO 14001:

Milano 1: via Caldera, 21: facility con tecnologia convenzionale (raffreddamento perimetrale under floor) ma efficienza medio alta (PUE medio stagionale c.a. 1,6); datacenter di 700mq dedicato principalmente ai servizi di colocation (shelf, rack, cage). Potenza nominale massima: 500KW. Classificazione non certificata: TIER II. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Cogent Communications, Level3, GTT, Mix (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a saturazione di Argon. Alimentazione Media Tensione da anello, gruppi elettorgeni di emergenza N+1

Milano 2: via Caldera, 21: facility con tecnologia ad alta efficienza "in rack" (raffreddamento locale dei rack ad alta densità) efficienza alta (PUE medio stagionale c.a. 1,4); datacenter di 250mq dedicato principalmente ai servizi di cloud computing. Potenza nominale massima: 300KW. Classificazione non certificata: TIER III. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Cogent Communications, Level3, GTT , Mix (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi a saturazione di Argon. Alimentazione Media Tensione da anello, gruppi elettrogeni di emergenza N+1

Sesto San Giovanni: Via Milanese, 20: facility con tecnologia convenzionale (raffreddamento perimetrale under floor) con efficienza media (PUE medio stagionale c.a. 1,8); datacenter di 200mq dedicato ai servizi di colocation (shelf, rack). Potenza nominale massima: 200KW. Classificazione non certificata: TIER II+. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Metroweb. Sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. stinzione incendi a saturazione di Argon. Alimentazione Bassa Tensione, gruppo elettrogeno di emergenza

Frosinone 1: C.so Lazio, 9/a: facility con tecnologia convenzionale (raffreddamento perimetrale under floor) con efficienza media (PUE medio stagionale c.a. 1,8); datacenter di 200mq dedicato ai servizi di cloud computing e, parzialmente, di colocation (shelf, rack). Potenza nominale massima: 200KW. Classificazione non certificata: TIER II+. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Infracom, Namex (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a CO2 e polvere. Alimentazione Bassa Tensione, gruppo elettrogeno di emergenza

Frosinone 2: Via Vona, 66 (zona industriale): facility di recentissima costruzione con tecnologie innovative (raffreddamento perimetrale under floor e combinato in rack con frecooling con acqua a temperatura moderata (15-20°) e grande portata, efficienza alta (PUE medio stagionale c.a. 1,3-1,35); datacenter di 1000mq dedicato ai servizi di cloud computing e, di colocation (shelf, rack, cage). Potenza nominale massima: 1000KW. Classificazione non certificata: TIER III+ (TIER IV a livello design). Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Infracom, Namex (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi con sistema HI-FOG® di Marioff water mist ad alta pressione twin fluid secondo quanto indicato dallo standard NFPA 750 e UNI CEN/TS 14972. Alimentazione Media Tensione, gruppi elettrogeni di emergenza N+1

Questo datacenter è realizzato in un nostro nuovo insediamento da 20000 mq del quale rappresenta il lotto iniziale, attualmente esiste una superficie coperta disponibile di 5000mq che attrezzeremo in maniera modulare in base alle esigenze di mercato ma, in via principale, per i servizi di Cloud Computing.

Per tutti i centri sono garantite le condizioni climatiche secondo raccomandazioni ASHRAE 2008.

Per tutti i datacenter sono disponibili sistemi di controllo accessi, rilevamento intrusioni, videosorveglianza conformi: CEI EN 50131 allarmi antifurto - CEI EN 50132 tvcc - CEI EN 50133 controllo accessi a doppio fattore- CEI EN 50134 allarmi sociali - CEI EN 50136 trasmissione di allarmi - EN 50137 sistemi integrati di allarme - EN50118 centrali di ricezione/telesorveglianza.

Misure Fisiche

L'accesso ai locali è regolato dalle procedure di sicurezza come da DPS predisposto ai sensi del dlgs 196/2003, separatamente riassunte e le prescrizioni ISO27001.

I locali che ospitano le apparecchiature sono dotati delle seguenti infrastrutture:

- Sorveglianza elettronica contro l'intrusione, l'incendio e anomalie ambientali critiche con segnalazione via radio e intervento in sede da parte di istituto di polizia privata autorizzato.
- Sistema ridondante di controllo del clima delle sale macchine con allarmi locali e remoti (teleallarmi su istituto di vigilanza) su valori critici
- Sistema di alimentazione ridondante su doppia rete di distribuzione a norme EIE-CE per ogni fila di armadi con prese e spine di sicurezza antistrappo e antifuoco.

- Impianto di sicurezza dell'alimentazione mediante impianto di terra certificato conforme L.626 e separazione galvanica delle sorgenti.
- Sistema di commutazione statica della sorgente duale di alimentazione per ogni armadio a servizio delle apparecchiature non dotate di alimentatori ridondanti.
- Condizionamento statico dell'alimentazione per ogni modulo tramite Gruppi di continuità statici on line
- Gruppi elettrogeni diesel ad alta autonomia con capacità adeguata, avvio automatico e cicli di diagnostica bisettimanale automatici.

Misure Logiche

1. Ogni incaricato è dotato di password e username univoci e personali costituenti le sue credenziali di autenticazione.
2. Le password sono cambiate almeno ogni tre mesi (per i dati sensibili/giudiziari e quelli ritenuti riservati dalla società, unitariamente definiti come "dati particolari") con le procedure di cui alla legge. Per i dati personali "comuni" sono cambiate almeno ogni sei mesi.
3. I codici identificativi personali sono disattivati in caso di non utilizzo per più di sei mesi.
4. Ai dati particolari hanno accesso solo ed esclusivamente gli incaricati grazie ad un sistema di verifica che gli permette di accedere alle parti degli elaboratori in cui sono conservati i dati particolari.
5. I sistemi sono dotati dei seguenti software e delle componenti hardware riportate nella tabella qui di seguito, come sistemi di protezione:
    a. Gli antivirus sono aggiornati con le nuove impronte virali ogni giorno
    b. Il firewall viene verificato periodicamente nella sua efficienza dagli amministratori di sistema che ne tengono traccia in apposito verbale.
    c. Ai sistemi vengono applicate le c.d. "patch" non appena le medesime sono disponibili e sufficientemente testate. Ai programmi acquisiti licenza le patch vengono applicate dai fornitori come da specifici contratti.
    d. Tutti i sistemi sono verificati dagli amministratori di sistema con cadenza trimestrale.
6. La logica con cui sono stati scelti i sistemi di protezione è all'insegna della indipendenza dal vendor per le operazioni di aggiornamento/manutenzione e la disponibilità, per ogni componente di aggiornamenti e patch nel minor tempo possibile.
7. L'azienda adotta le procedure di esecuzione back up specifiche per ogni famiglia di servizi; le prestazioni minime di backup sono di seguito riportate:
    a. Viene effettuato un backup giornaliero di tutti i dati presenti nei vari archivi, il backup viene effettuato a memoria 2 per gli archivi non strategici o comunque facilmente ricostruibili, a memoria 7 per gli altri. I dati di backup vengono conservati sia su un pool di dischi fissi sia su Nastri rimovibili.
    b. I dati relativi a servizio di tipo "**Cloud Server**" e "**Cloud Infrastructure**" relativamente alla parte di gestione degli account, spazio web e dati contenuti negli eventuali database a richiesta di servizio da parte del cliente, a **backup settimanale di tutti i dati presenti, il backup viene effettuato a memoria 2** salvo specifica più restrittiva concordata con il cliente
    c. La procedura di backup viene avviata automaticamente attraverso il sistema centralizzato di gestione TIVOLI TSM di IBM; lo stesso sistema centralizzato provvede all'audit sull'esecuzione e la correttezza dei cicli di backup.
8. I supporti di memorizzazione removibili contenenti dati particolari se non utilizzati sono distrutti o resi inutilizzati attraverso questi sistemi:
    a. Gli unici dispositivi di memorizzazione in uso sono i nastri del sistema di backup, la loro distruzione alla fine dell'utilizzo specifico e/o del ciclo di vita avviene tramite formattazione non invertibile.
    b. Qualora non siano recuperabili i dati, i supporti possono essere riutilizzati. I dati non sono recuperabili grazie ai seguenti sistemi: formattazione non invertibile.

Le procedure di ripristino prevedono il recupero dei dati in un'opportuna area di spool non coincidente con l'area di produzione. I dati recuperati vengono poi sottoposti a validazione tramite ispezione manuale o automatica e quindi reimmessi negli archivi di produzione.

L'eventuale interruzione di servizio non collegata con la perdita di dati ma derivante da problemi di connessione e/o da malfunzionamento dei dispositivi hardware (server, terminali, router) viene trattata in maniera autonoma dalla gestione/conservazione degli archivi.

Per le procedure di Backup, verifica, Disaster Recovery ci si avvale dello specifico software Tivoli TSM di IBM.

Il software assicura l'esecuzione dei backup in base alle politiche stabilite, verifica inoltre il contenuto delle copie di sicurezza e la loro congruità con gli archivi da proteggere.

Tivoli TSM si occupa inoltre dell'assesment delle procedure di Disaster Recovery per i dati oggetto del backup.

A livello fisico i dati sono conservati in apposite cartucce di nastro, normalmente ospitate in caricatori automatici

Analisi dei rischi

La profilazione seguente si riferisce alla prestazione di base prevista dal servizio, è possibile mitigare i rischi attraverso specifiche procedure e tecnologie negoziate in via specifica con il cliente

Tipo Danno Sistema Informatico	**Conseguenza per i dati**	**Causa Danno**	**Valutazione del rischio in base alle cause**
Distruzione o manomissione fisica o logica del sistema	Distruzione Non conformità alle caratteristiche originali Trattamento non autorizzato	Eventi non dipendenti dall'Azienda (fulmini, incendi, furti con danni) Eventi dolosi (Mano-missione interna o esterna, volontaria o non)	Rischio Basso
Intrusioni nel sistema dall'esterno dell'Azienda	Distruzione Non conformità alle caratteristiche originali Trattamento non autorizzato	Intrusione da parte di pirati informatici	Rischio Medio

In caso di perdita dei dati il tempo stimato per il loro recupero sarebbe quello certificato dalla ditta fornitrice dell'assistenza hardware e software; stimabile comunque nel limite superiore di 24 ore.

Individuazione e ruolo degli amministratori di sistema

E' stata predisposta una specifica procedura di compliance per quanto richiesto dal Dlgs 196/2003 circa l'individuazione del ruolo, delle competenze e delle responsabilità degli amministratori di sistema; tale procedura è stata integrata con le indicazioni della *determina del Garante per la protezione dei dati personali del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)* attraverso la predisposizione di opportuni accorgimenti di tracciamento delle attività svolte e l'individuazione delle opportune figure professionali abilitate all'esecuzione delle attività di amministrazione dei sistemi nel rispetto delle linee guida proposte dall'autorità Garante**.**