T.NET SPA

TIPO	DESCRIZIONE
Società:	T.net SpA
Indirizzo:	via Roberto Le Petit, 8/10
Oggetto:	Affidamento servizi Cloud
Documento:	ISO/IEC 27001_27017_27018 – Affidamento servizi Cloud
Data di consegna file:	01/04/2019
Classe:	**Pubblico**
Redattore:	Alessandro Raciti - COO
Revisione:	0

Sommario

1 PREMESSA

L'affidamento dei dati in cloud ai sensi della ISO 27017:2015 prevede la verifica di determinati requisiti sia per il Cliente che per T.net.

T.net in completa trasparenza per la gestione dei servizi offerti fornisce in seguito un riepilogo degli adempimenti riferiti al Cliente a quelli adottati da T.net come fornitore in ottemperanza alla ISO 27017: 2015.

Qualora riscontriate delle difformità rispetto a quanto sotto riportato e gli eventuali servizi offerti, vi invitiamo a segnalarcelo tramite i nostri consueti canali di comunicazione.

2 PROTOCOLLO DI AFFIDAMENTO SERVIZI CLOUD

I dati memorizzati nell'ambiente di cloud computing possono essere soggetti all'accesso e alla gestione da parte di T.net; a tutela del Cliente, T.net adotta metodi e processi certificati da terzi in ambito ISO 27001, ISO 27018 e ISO 27017;

1. T.net ha identificato nel Garante della Privacy, Agid e nella Polizia Postale le Autorità rilevanti per la protezione dei dati.

   Qualora il Cliente ritiene di modificare e/o integrare tali organismi, è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.

   Si ricorda che il Cliente è tenuto ad aggiungere ai propri programmi di formazione i seguenti elementi di sensibilizzazione, istruzione per:

   - i responsabili di funzione,
   - i referenti di funzione (sys admin, security admin etc.),
   - gli utenti del servizio cloud, inclusi i dipendenti e gli appaltatori interessati.

La consapevolezza della sicurezza delle informazioni, i programmi di istruzione e formazione sui servizi cloud dovrebbero essere formalizzati alla direzione ed ai responsabili della supervisione, compresi quelli delle unità operative.

Questi sforzi supportano un efficace coordinamento delle attività di sicurezza delle informazioni in ambiti quali:

- standard e procedure per l'utilizzo dei servizi cloud;
- rischi per la sicurezza delle informazioni relativi ai servizi cloud e come tali rischi sono gestiti;
- rischi per l'ambiente di rete e di sistema con l'uso di servizi cloud;
- considerazioni legali e normative applicabili.

2. T.net eroga i propri servizi cloud su infrastrutture residenti all'interno del territorio nazionale italiano e specificatamente presso i Data Center ubicati in Milano presso Irideos via Caldera, Palermo via Ugo La Malfa Sicily HUB e Catania viale Africa 84.

3. T.net comunicherà al Cliente con un preavviso di 15 giorni eventuali impatti e/o modifiche di change location sui servizi cloud attivati verso altri Data Center T.net ubicati all'interno della UE ed il rispetto del trattamento dei dati conforme alla direttiva europea sulla protezione dei dati (GDPR. 679/2016). T.net comunicherà sul proprio sito web eventuali espansioni infrastrutturali.

4. T.net classifica tutte le informazioni scambiate con il Cliente, l'etichettatura segue vari livelli di classificazione:

Categoria di Informazioni	**Descrizione**	**Esempi**
Pubblica o non Etichettata	L'informazione fornita non è confidenziale e quindi può essere pubblica senza che questa abbia alcuna	Brochure di Prodotti distribuite dalla forza commerciale sia direttamente

Categoria di Informazioni	Descrizione	Esempi
	implicazione negativa se la stessa viene rilevata. La mancanza di disponibilità di questa informazione in caso di down time è un rischio accettabile. L'Integrità è importante ma non fondamentale e vitale per la vita o il business del Cliente.	sia attraverso un sito pubblico o una Intranet. Il sito web pubblico del Cliente (reputation). Download di Software di prova da parte di prospect (reputation) Report finanziari richiesti per rispondere a requisiti regolamentari (reputation) Newsletter e Mailing List server
Proprietaria o Riservata (Uso Interno, non divulgabile)	L'informazione è riservata al Management e non divulgabile all'esterno. Una diffusione non autorizzata di questi dati potrebbe influenzare l'attività dell'azienda, causare perdite, provvedere un indebito vantaggio per i competitor o causare una perdita di reputazione e affidabilità nei confronti dei Clienti. In questi casi, l'Integrità dell'Informazione deve essere considerata vitale.	Password e informazioni sulle procedure di sicurezza aziendale Know-how utilizzato per elaborare le informazioni del cliente Procedure operative standard utilizzate in tutte le parti del Business della società Tutti i codici software sviluppati dall'azienda, sia usato internamente o venduto ai clienti.
Confidenziale	Sono informazioni ricevute dai clienti in qualsiasi forma per l'elaborazione in	Dispositivi e Strumenti dei Clienti

Categoria di Informazioni	Descrizione	Esempi
	produzione da parte della Società. La copia originale di tali informazioni non deve essere cambiata in qualsiasi modo senza permesso scritto da parte del cliente. Questo tipo di Informazioni rappresenta il più alto possibile livello di integrità, riservatezza assicurandosi che la diffusione di questi dati sia limitata è vitale.	Trasmissioni elettroniche da parte dei clienti (File, Posta, Dati, Archivi di Vendita, etc.) Informazioni sul prodotto generate per il cliente da attività di produzione aziendale specificate dal cliente.
Classificata	Sono informazioni trattate dei Clienti con il massimo grado di riservatezza e la cui diffusione potrebbe avere un elevato impatto sui diritti degli interessati e o rilevare informazioni di natura sensibile su infrastrutture critiche	Dati genetici, relativi a malattie o patologie Dati relativi all'accesso ad aree riservate o protette (aeroporto, strade, autostrade, porti, centrali elettriche, etc.)
Confidenziale Interna	Sono dati interni trattati dall'Organizzazione per lo svolgimento del proprio Business, come i processi di provisioning interni, la gestione dei dipendenti, lo sviluppo del software. A queste informazioni deve essere assicurato il più alto livello di integrità,	Salari e altri dati personali Dati contabili e rapporti finanziari interni Dati aziendali dei clienti riservati e contratti riservati Accordi di non divulgazione con clienti \ fornitori Piani aziendali della società (Business Plan)

Categoria di Informazioni	Descrizione	Esempi
	confidenzialità e la disponibilità di accesso deve essere limitata, gli accessi registrati e le violazioni devono essere tempestivamente segnalate. Il trattamento di questi dati è vitale per la continuità aziendale.	

5. L'inventario delle risorse che effettua periodicamente T.net tiene conto delle informazioni e delle risorse associate e archiviate nell'ambiente di cloud computing. I registri dell'inventario indicano dove vengono mantenute le risorse.

6. Ogni informazione dislocata nel cloud di T.net è identificata ed etichettata. Una apposita procedura interna ne garantisce l'applicazione.

7. T.net adotta un'adeguata allocazione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni e conferma che è nelle condizioni di adempiere ai propri ruoli e responsabilità in materia di sicurezza dei dati.

   A tal fine, sono condotte periodiche rivalutazioni dell'analisi dei rischi, vulnerability assessment e penetration test.

   Il Cliente che ritiene di modificare e/o integrare le prassi di controllo di T.net è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.

   T.net rimane a completa disposizione del Cliente sia per fornirgli il registro del trattamento dei servizi in essere sia per dargli indicazioni circa la procedura di classificazione delle informazioni attraverso il proprio sito web – https://www.tnet.it.

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."

8. Il Cliente deve richiedere informazioni a T.net sulla gestione delle vulnerabilità tecniche che possono influenzare i servizi forniti. In ogni caso, in tale ambito T.net adotta una propria politica di vulnerability assessment e di penetration test; su esplicita richiesta del Cliente, T.net è in grado di fornire documentazione a riguardo.

9. Tutti gli accessi ai sistemi di informazione di T.net devono avvenire in modo sicuro e protetto.
   T.net introduce l'autenticazione a due fattori bloccando sul nascere eventuali tentativi di accesso illecito ai servizi.

   Una autenticazione a due fattori si contrappone dunque ad una comune autenticazione basata sulla sola password.
   Adottiamo le seguenti opzioni di accesso a due fattori:

   - *random passcode by mobile (terze parti)*
   - *text message*
   - *phone call*

10. il Cliente deve sempre utilizzare tecniche di autenticazione sufficienti per autenticare i suoi utenti con profilo amministratore (ma anche user); a tale scopo, opportune policy adottate da T.net impediscono di usare credenziali deboli o inadatte allo scopo.

11. il Cliente è tenuto a verificare e garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato in conformità con la sua politica di controllo degli accessi e che tali restrizioni siano realizzate includendo:

    - la limitazione dell'accesso ai servizi cloud;
    - alle funzioni del servizio cloud;
    - ai dati dei clienti gestiti dal servizio cloud.

12. Il processo di gestione del servizio in cloud offerto al Cliente tiene conto del profilo di accesso al servizio fornito da T.net che provvede ad informare il Cliente sulle modalità di accesso standard, durante l'attivazione del servizio.

13. Per fruire del servizio cloud devono essere ben definiti gli utenti.
    A tal fine, T.net adotta due diversi profili ad uso del Cliente:

    - Customer User as Administrator - amministratori del servizio cloud che hanno accesso privilegiato.
    - Customer User - Utenti con un profilo User, che possono eseguire operazioni limitate.

14. La politica di controllo dell'accesso in cloud al servizio cha adotta T.net prevede la compartimentazione per ciascun servizio cloud.

15. il Cliente è tenuto a verificare che la procedura di gestione di T.net per l'allocazione delle informazioni di autenticazione segreta, come le password, soddisfi i propri requisiti.

16. Il Cliente deve assicurarsi che la capacità di erogazione del servizio concordata conT.net venga soddisfatta.
    Il Cliente deve monitorare l'utilizzo dei servizi e prevedere le proprie esigenze di capacità richiesta, al fine di garantire le prestazioni dei servizi cloud che gli necessitano nel tempo. T.net si rendere disponibile a mettere a disposizione adeguati strumenti per facilitare al Cliente questa attività.

17. Laddove l'utilizzo di programmi di utilità è consentito, il Cliente deve identificare i programmi di utilità da utilizzare nel proprio ambiente e assicurarsi che non interferiscano con i controlli del servizio cloud.

18. Per l'utilizzo dei servizi cloud, il Cliente, se giustificato dalla propria analisi del rischio, deve implementare controlli crittografici. I controlli devono essere sufficienti a mitigare i rischi identificati, indipendentemente dal fatto che tali controlli siano forniti daT.net.

19. T.net adotta una specifica procedura scritta per il controllo e la manutenzione dell'efficacia delle chiavi crittografiche per ciascuna fase del ciclo di vita, ossia: la generazione, la modifica o l'aggiornamento, la memorizzazione, il ritiro, il recupero, il mantenimento e la distruzione. NormalmenteT.net applica i controlli crittografici su tutte le transazioni da/per il Cliente, con standard di protezione in linea con il mercato, con valutazione periodica dello stato del certificato utilizzato.

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."
T.net è un'azienda direttamente supportata nel capitale da EIT DIGITAL, come risposta da parte dell'European Institute of Innovation and Technology e dell'Unione Europea alla pandemia dovuta al COVID-19.

E’ compito del Cliente esaminare tutte le informazioni fornite da T.net per confermare se le funzionalità di crittografia:

- soddisfano i suoi requisiti di politica;
- sono compatibili con qualsiasi altra protezione crittografica già utilizzata;
- sono applicate ai dati a riposo ed in transito e all'interno del servizio.

20. T.net ha specifiche politiche e procedure scritte per lo smaltimento sicuro o il riutilizzo delle risorse. Se richiesto,T.net fornirà tali documenti.

21. Tutti i tentativi di log-on errati, vengono registrati. Superati i cinque tentativi di accessi errati, l’account viene disabilitato. Occorre pertanto inviare richiesta di sblocco dell’account all’email noc@tnet.it fornendo:
    - il numero cliente rilasciato da T.net in fase di attivazione
    - il nominativo del richiedente con rispettivi dati anagrafici

22. Le password non sono mai registrate in chiaro occorre un’autenticazione e crittografia forte.

    Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun Cliente e quindi account ad esso correlati sono obbligati a sostituire la propria password con una nuova, univoca, che rispetti una cronologia (history) settata ad un valore pari a 14.

    La password è costituita da un minimo di 8 caratteri alfanumerici fino ad un massimo di 32 che comprendono un minino di n.1:
    - lettera minuscola
    - lettera maiuscola
    - numero
    - carattere speciale

23. Le chiavi di accesso non possono essere condivise e devono essere uniche per ciascun utente.

24. Le chiavi di accesso non devono essere tenuti su supporti scritti con indicazioni che possono facilitare l'accesso non autorizzato da parte di terzi.

25. Laddove T.net fornisca funzionalità di backup come parte del servizio cloud, il Cliente deve:
    - richiedere le specifiche della capacità di backup da T.net;
    - verificare che le specifiche di backup siano compatibili con le proprie necessità di conservazione;

    Diversamente, il Cliente è responsabile dell'implementazione delle funzionalità di backup.

    T.net utilizza come software di back-up Veeam Software, il servizio è concesso con sottoscrizione a gestione autonoma dei backup per i servizi:
    - DCaaS
    - PaaS

    Le policy di backup by default sono backup giornaliero con retention a n.14 giorni per i seguenti servizi:
    - CloudMail
    - CloudBag

    I log per l'audit sono conservati per un minimo di 6 mesi e laddove richiesto per legge fino ad un massimo di 24 mesi.

    Analogamente T.net utilizza il software Plesk Backup per la gestione dei backup degli hosting web – policy di retention personalizzabile a cura del Cliente.

    Tutti i backup vengono memorizzati su storage designati per il backup in configurazione RAID-6, la continuità dei dati è garantita fino ad un guasto contemporaneo di ben 4 dischi per shelf.

    I repository cloud sono completamente isolati gli uni dagli altri. I clienti possono inoltre crittografare i backup; ciò avviene alla fonte, prima che i dati escano dalla rete del cliente, e senza aumentare il consumo di banda.

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."
T.net è un'azienda direttamente supportata nel capitale da EIT DIGITAL, come risposta da parte dell'European Institute of Innovation and Technology e dell'Unione Europea alla pandemia dovuta al COVID-19.

26. il Cliente in autonomia può eseguire il ripristino dei backup accedendo alla propria area riservata sulle piattaforme:
    - Plesk
    - Veeam Self Portal

27. Ogni trimestre sottoponiamo a test i nostri backup verificandone il buono stato in modo da ottenere dei ripristini sicuri e non compromessi.

28. T.net implementa un set di log standard che consentono di monitorare una serie di eventi. Ciò non toglie che il Cliente è tenuto a verificare se tale set di log è sufficiente e in linea con le proprie politiche; diversamente, deve definite con T.net i requisiti per la registrazione degli eventi e verificare che il servizio cloud soddisfi tali requisiti.

29. Il file di Audit è inalterabile e non cancellabile, nemmeno accidentalmente.

30. Attraverso il SIEM generiamo periodicamente, ogni 24 ore almeno, un hash crittografico del log con il timestamp e lo memorizziamo su un supporto separato. Tale strumento ci consentirà di dimostrare ricalcolando l'hash che il log non è stato manomesso.

31. Tutte le attività rivolte alla risoluzione di problematiche di sicurezza e/o fruibilità dei servizi cloud saranno svolte da personale T.net con opportuni permessi e deleghe. Gli accessi saranno registrati con timestamp e certificati da audit esterni. Le attività saranno strettamente correlate alla risoluzione del problema nel rispetto dei criteri di integrità, riservatezza, disponibilità ed autenticità.

32. Laddove richiesto ciascun operatore che svolge attività in esterna potrà collegarsi alle Facilities tramite l'instaurazione di un collegamento virtuale VPN (Virtual Private Network) punto-punto tra l'operatore – client - ed il *site* di destinazione seguendo un percorso definito e segregato per l'accesso al target.

33. T.net adotta una policy di sincronizzazione di tutti gli orologi aziendali, e ne verifica periodicamente l'applicazione, in modo da garantire che ogni ambiente sia sincronizzato. Su richiesta, T.net può fornire informazioni al Cliente sulla policy di sincronizzazione dell'orologio utilizzata per i servizi cloud.

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."
T.net è un'azienda direttamente supportata nel capitale da EIT DIGITAL, come risposta da parte dell'European Institute of Innovation and Technology e dell'Unione Europea alla pandemia dovuta al COVID-19.

34. il Cliente deve identificare le vulnerabilità tecniche di cui sarà responsabile e dovrà definire chiaramente un processo per gestirle.

35. T.net adotta una politica di segregazione delle reti per ottenere l'isolamento nell'ambiente condiviso per il servizio cloud. Su esplicita richiesta del Cliente,T.net è in grado di fornire documentazione a riguardo.

36. Il Cliente deve determinare i requisiti di sicurezza delle informazioni e quindi valutare se i servizi offerti daT.net soddisfino tali requisiti. Per questa valutazione, il Cliente può sempre richiedere a T.net informazioni sulle funzionalità di sicurezza delle informazioni adottate.

37. T.net effettua le operazioni di sviluppo in ambiente sicuro e dedicato, con dati di prova non reali. Le operazioni di sviluppo sono governate da specifiche procedure scritte. Su esplicita richiesta del Cliente, T.net è in grado di fornire documentazione a riguardo.

38. Il Cliente deve includere T.net nella sua politica di sicurezza delle informazioni, nelle relazioni con i fornitori. Ciò contribuirà a mitigare i rischi associati all'accesso e alla gestione dei dati gestiti nei servizi offerti daT.net.

39. il Cliente deve confermare i ruoli e le responsabilità in materia di sicurezza delle informazioni relative al servizio cloud, descritti nel contratto di servizio. Questi possono includere, a seconda dei servizi offerti, i seguenti processi:

    - protezione da malware;
    - backup;
    - controlli crittografici;
    - gestione della vulnerabilità;
    - gestione degli incidenti;
    - controllo della conformità tecnica;
    - test di sicurezza;
    - auditing;
    - raccolta, manutenzione e protezione delle prove, compresi i registri e le liste di controllo;

- protezione delle informazioni al termine del contratto di servizio;
- autenticazione e controllo degli accessi;
- identità e gestione degli accessi.

40. T.net ha una specifica procedura scritta per la gestione degli incidenti di sicurezza delle informazioni.
    Questa policy, serve per assicurare un approccio coerente ed efficace per la gestione degli incidenti alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza e ai punti di debolezza.

    La politica mira a mitigare i seguenti rischi:

    - ridurre l'impatto delle violazioni della sicurezza delle informazioni garantendo che gli incidenti siano seguiti correttamente.
    - aiutare ad identificare le aree di miglioramento per ridurre il rischio e l'impatto di futuri incidenti, diminuendo la superficie di attacco e le possibilità di Data Breach.

    Gli incidenti di sicurezza delle informazioni devono essere segnalati al più presto possibile inviando un'email a privacy@tnet.it, verificata la comunicazione da parte del personale preposto si riunirà in misura straordinaria il CAB/EC che delibererà sulle opportune azioni correttive e/o blocco.

    In caso di "Data Breach", devono essere segnalati al DPO che provvede ad inoltrarli all'Autorità di Controllo dei Dati Personali, il "Garante", nei mezzi che il Garante renderà noti.

    La definizione di un "incidente di sicurezza delle informazioni" è un evento avverso che ha causato o ha il potenziale di causare danni al patrimonio, alla reputazione, ai Clienti e/o al personale della T.net, nei termini che gli attacchi o gli incidenti possono essere indirizzati o occorre anche ai Sistemi di Elaborazione che erogano i Servizi di cui usufruisce la T.net stessa.

    Un incidente di sicurezza delle informazioni include, ma non è limitato a, quanto segue:

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."

- la perdita o il furto di dati o informazioni (Data Loss).
- il trasferimento di dati o informazioni a coloro che non hanno diritto a ricevere quell'informazione (Data Leakege).
- tentativi (falliti o riusciti) di ottenere accesso non autorizzato ai dati o archivi (DataStore) delle informazioni di un sistema informatico dell'Organizzazione o dei Suoi Clienti.
- modifiche alle informazioni o ai dati o all'hardware del sistema, firmware o software senza autorizzazione e/o senza che il RSGSI o la Direzione ne siano a conoscenza e senza l'istruzione o il consenso di RSGSI e della Direzione.
- Interruzione indesiderata di un servizio erogato dai Sistemi dell'Organizzazione.
- l'uso non autorizzato di un sistema per l'elaborazione o l'archiviazione di dati da parte di qualsiasi persona interna o esterna all'organizzazione
- l'azione di un malware o un attacco DDOS

Il Cliente dovrà istruire i propri dipendenti affinché forniscano le seguenti informazioni essenziali:

- il tipo di dati, le informazioni o le attrezzature coinvolti, citando il numero di identificazione/inventario, se applicato e/o se applicabile (ad es per un Server in Hosting questo non è possibile, mentre lo è per un PC assegnato ad un Dipendente o ad un Server in Housing)
- se la perdita dei dati mette a rischio qualsiasi persona o altri dati.
- la posizione della Facility in cui si è verificato l'incidente (se desumibile o nota).
- numero di inventario di qualsiasi apparecchiatura interessata.
- data e ora in cui si è verificato l'incidente di sicurezza.
- posizione dei dati o delle apparecchiature interessate.

E' vitale quindi che il Cliente ed i collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.

Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni.

Sarà cura di T.net rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate.

La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto degli incidenti futuri.
L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze.

In prima istanza l'analisi degli incidenti spetta al SOC e in caso di particolari difficoltà al SOC Supervisor e al RSGSI.
Se l'incidente di sicurezza delle informazioni è in relazione alle informazioni personali, sia su formato cartaceo che elettronico, il responsabile della protezione dei dati (DPO), oltre alle figure sopra richiamate, deve essere informato.

Il livello di impatto di un incidente di sicurezza delle informazioni sarà determinato secondo la strategia di gestione del rischio stabilita da RSGSI, con il SOC Supervisor sentita il Data Subject ed il DPO. Di tali incontri e indirizzi strategici andrà redatto un apposito documento, che verrà aggiornato ad ogni audit.

Degli incidenti di sicurezza delle Informazioni, andrà redatto un Registro "Incident Report" e tale elenco farà parte del riesame annuale e degli Audit Infrannuali.

La gestione degli incidenti riguarda l'intrusione, il compromesso e l'abuso di informazioni e risorse informative e la continuità delle informazioni critiche relative a sistemi e processi.

Il responsabile dei servizi IT (RSGSI) manterrà una copertura del processo di gestione degli incidenti in relazione ad identificazione, valutazione, gestione e monitoraggio degli incidenti di sicurezza delle informazioni, compresa la raccolta di qualsiasi prova che potrebbe essere richiesta per l'analisi come prove forensi.

I servizi IT di T.net garantiranno che solo il personale identificato e autorizzato abbia accesso ai sistemi interessati durante l'incidente e che tutte le azioni correttive siano documentate nel modo più dettagliato possibile.

La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni, deve essere utilizzata per ridurre la verosimiglianza o l'impatto di incidenti futuri.

I Responsabili ICT esamineranno regolarmente gli incidenti di sicurezza delle informazioni effettuando ex Post una revisione dell'incidente.
I tipi ed i volumi di incidenti e costi sostenuti durante il verificarsi degli incidenti saranno analizzati per identificare eventuali modelli o tendenze (al ribasso o al rialzo).
In caso di tendenza al rialzo, le contromisure di sicurezza andranno ovviamente riviste (Riesame).

Il responsabile dei servizi IT (RSGSI) condividerà questa analisi, se del caso, con il "Reporting Point" designato (SOC Supervisor o NOC Supervisor) per aiutare il processo automatico di allerta per l'Organizzazione e stabilire dei meccanismi di Warning e Critical in linea con le esigenze riscontrate per un intervento migliore e più tempestivo.

Esempi di Incidenti:

- Va segnalato che questo elenco non è esaustivo.
- Malicius Incident and Threats (Attacchi Maligni)
- Fornire informazioni a qualcuno che non dovrebbe avere accesso ad esso - verbalmente, per iscritto o elettronicamente.
- Computer infetto da virus o altro malware (Keystroker, Brute Force, Trojan, Worm, BOT).
- Invio di un'e-mail sensibile a "tutto il personale" o a Clienti per errore.
- Ricezione di posta non richiesta di natura offensiva.
- Ricezione di posta non richiesta che richiede l'inserimento di dati personali (Phishing).
- Ricerca di dati che sono stati modificati da una persona non autorizzata.
- Ricezione e inoltro di lettere a catena - inclusi avvisi di virus, avvisi di truffa e

- altre e-mail che incoraggiano il destinatario a trasmettere agli altri (Malicius Spam).
- Persone sconosciute che chiedono informazioni che potrebbero consentire loro di accedere ai dati dell'Organizzazione (ad esempio una password o i dettagli di una terza parte) attraverso raggiri o mezzi informatici.
- Abusi
- Uso di software non approvato o senza licenza su apparecchiature dell'Organizzazione.
- Accesso a un database tramite l'autorizzazione di qualcun altro (utilizzando Nome utente e password dell'altro utente).
- Annotare la password e lasciarla in mostra in qualche modo facile da trovare.
- Stampa o copiare delle informazioni Confidenziali, Riservate o Classificate e non memorizzarle o archiviarle appropriatamente.
- Furto / perdita di un bene aziendale
- Furto / perdita di un file cartaceo.
- Furto / perdita di qualsiasi apparecchiatura informatica dell'Organizzazione
  Uso illecito della strumentazione aziendale per usi personali.

41. Tutti i dati gestiti in transito o meno sono crittografati dalla T.net. Per i dati in transito, viene utilizzata la crittografia TLS 1.2 o versione successiva. In caso contrario, viene utilizzata la crittografia AES 256 o versione successiva.

42. Il Cliente in totale autonomia può provvedere all'installazione di certificati SSL.
    Laddove si ritenesse necessario il team di T.net supporterà il Cliente alla creazione di una CSR (Certificate Signing Request) – univoca, la richiesta verrà generata sul server in cui è ospitato il servizio da proteggere.

43. il Cliente riceverà da T.net informazioni riguardo ai meccanismi per:

    - segnalare a T.net un evento di sicurezza delle informazioni che ha rilevato;
    - ricevere segnalazioni riguardanti un evento di sicurezza delle informazioni rilevato da T.net;
    - tenere traccia dello stato di un evento di sicurezza delle informazioni segnalato.

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."

44. il Cliente deve considerare che Leggi e Regolamenti pertinenti possono essere quelli delle giurisdizioni che regolano T.net, oltre a quelli che regolano lui stesso.

45. il Cliente deve richiedere evidenza della conformità di T.net con le normative e gli standard pertinenti richiesti per le sue attività. Tali prove possono essere le certificazioni prodotte dagli auditor di terze parti in ambito ISO o modelli di gestione esposte nel sito https://www.tnet.it .

46. si ricorda che l'installazione di software con licenza commerciale in un servizio cloud può causare una violazione dei termini della licenza per il software. Il Cliente deve avere una procedura per identificare i requisiti di licenza specifici per il cloud prima di consentire a T.net l'installazione di qualsiasi software con licenza. Un'attenzione particolare deve essere rivolta ai casi in cui il servizio cloud è elastico e scalabile e il software può essere eseguito su più sistemi o core del processore rispetto a quanto concordato.

47. si ricorda che il Cliente deve richiedere informazioni a T.net sulla protezione dei record raccolti e archiviati da T.net rilevanti per l'utilizzo dei servizi. T.net si impegna a fornire tali informazioni.

48. si ricorda che il Cliente deve richiedere prove documentate che l'implementazione dei controlli di sicurezza delle informazioni e linee guida per il servizio cloud sia in linea con quanto definito in sede contrattuale. Tali prove devono includere certificazioni rispetto agli standard pertinenti. A tal proposito, T.net è in possesso di varie certificazioni del proprio sistema; per maggiori dettagli, si veda il sito www.tnet.it.

49. In caso di forza grave - calamità naturali, eventi terroristici ovvero ogni fatto catastrofico, ragionevolmente imprevedibile, conseguente a eventi determinanti, e a loro volta ragionevolmente imprevedibili alle strutture deposte all'erogazione dei servizi Cloud dei clienti, se prevista sottoscrizione Disaster Recovery questi verranno migrati in altro DC specificato in fase contrattuale.

50. si ricorda che il Cliente deve definire o estendere le sue politiche e procedure esistenti in conformità con il suo uso dei servizi cloud e rendere gli utenti del servizio consapevoli dei loro ruoli e responsabilità nell'uso del servizio cloud.

51. i dati archiviati sui server della T.net saranno sempre di proprietà del Cliente.

52. T.net concede la possibilità di scaricare una copia dei dati in qualsiasi momento ed in totale autonomia e dichiarare con la massima trasparenza il luogo fisico dove risiedono i dati

53. Il cliente deve poter monitorare periodicamente la risposta del fornitore alle prestazioni e al rispetto del contratto

54. Facilitiamo la portabilità nel caso in cui il cliente decidesse di migrare applicazioni e dati da un ambiente cloud ad un altro evitando di rimanere 'bloccati' (*vendor lock-in*).

55. si ricorda che il Cliente deve richiedere a T.net una descrizione documentata del processo di cessazione del servizio che copra la rimozione delle risorse del Cliente seguita dalla cancellazione di tutte le copie di tali risorse dai sistemi di T.net . A tal fine, T.net ha una specifica procedura scritta per la dismissione del servizio, ivi inclusa la modalità di restituzione dei dati (ove necessario).

56. Si ricorda che il Cliente deve documentare le procedure per operazioni critiche in cui un errore può causare danni irreversibili alle risorse nell'ambiente di cloud computing. Esempi di operazioni critiche sono:

    - installazione, modifica e cancellazione di dispositivi virtualizzati come server, reti e storage;
    - procedure di terminazione per l'utilizzo del servizio cloud;
    - backup e ripristino.
    - il documento deve specificare che un supervisore dovrebbe monitorare queste operazioni.

57. Schema e principali allegati di un contratto di Servizi di cloud computing della T.net:

    - Premesse e Definizioni
    - Oggetto e Finalità
    - Specificazioni Tecniche del servizio affidate a uno o più allegati

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."

- Modalità di perfezionamento del contratto
- Livelli e Modalità di mantenimento del servizio e assistenza
- Corrispettivi (pay for use o canoni per servizi differenziati)
- Responsabilità fornitore e Responsabilità Cliente (eventuale possibilità di sospensione del servizio)
- Recesso e risoluzione (con clausola risolutiva espressa)
- Obblighi di riservatezza (anche successivi alla conclusione del contratto)
- Proprietà e licenze delle prestazioni oggetto del contratto (software anche di terzi, domain name, loghi etc.)
- Fase patologica (controversie, fallimento del Fornitore del servizio e del Cliente etc.)
- Passaggio di consegne (fruibilità del DB/Archivio/Soluzione dopo cessazione effetti del contratto)
- Modalità delle comunicazioni e protezione dei dati
- Modifiche del contratto e Cessione del contratto
- Durata del contratto
- Legge applicabile e Giudice Competente (o Arbitro)
- SLA [livelli di servizio su accessibilità alla piattaforma, livelli di servizio su modalità di ripristino, livelli di servizio su tempistiche di assistenza (e risoluzione) in caso di problemi di utilizzo, livelli di utilizzabilità della piattaforma e verifica di eventuali rallentamenti nella fornitura del servizio, livelli di servizio sul mantenimento dei dati (e documenti) etc.] e penali (ed eventuali delimitazioni dell'indennizzo
- ammissibilità anche in caso di colpa grave o violazione di misure di sicurezza minime, necessarie o idonee);
- Policy di utilizzo della piattaforma;
- Privacy Policy con nomina in capo al cloud provider come Responsabile del trattamento
- Data Privacy Officer – Documento reperibile all'url: https://www.tnet.it/wp-content/uploads/2018/11/20181015_DataProtectionPolicy_en-1.pdf

- definizione di misure di sicurezza a presidio della piattaforma (definizione di politiche di prevenzione da accessi abusivi con definizione di tecniche funzionali al controllo degli accessi e di verifica dell'integrità dei dati e di

monitoraggio/reporting in caso di accessi abusivi con eventuale perdita parziale del dato);

- Specificazioni Tecniche su soluzioni fornite e tecnologia utilizzata;
- Eventuali certificazioni ottenute

58. T.net si impegna affinché tutte le informazioni, concetti, idee, procedimenti, metodi e/o dati tecnici di cui il personale utilizzato dal medesimo verrà a conoscenza nello svolgimento del servizio sono considerati riservati e coperti da segreto.

    T.net infine accetta di non divulgare, comunicare o diffondere i dati dallo stesso acquisiti in ragione della attività di cui alla presente procedura, né altrimenti utilizzarli per la promozione e la commercializzazione dei propri servizi.

    T.net si obbliga ad adottare con i propri dipendenti e consulenti tutte le cautele necessarie a tutelare la riservatezza di tali informazioni e/o documentazione ed a sottoscrivere, in fase di avvio dei servizi, apposito accordo di riservatezza a norma del Capitolato tecnico.

    T.net ottempera la normativa in materia di trattamento dei dati personali nonché i diritti delle persone fisiche e degli altri soggetti secondo quanto stabilito dal Codice di protezione dei dati personali (D.lgs. 196/03 e s.m.i. e Regolamento 2016/679 e sue applicazioni).

59. Laddove il Cliente ritenesse opportuno chiedere prove documentate circa l'implementazione di specifici controlli di sicurezza da parte della T.net, se questi non comportano un rischio alla sicurezza delle informazioni della T.net stessa e dei sui rispettivi Clienti, tali documenti verranno trasmessi classificando il documento come Confidenziale.

60. La cessazione dei servizi cloud segue un flusso suddiviso in n.5 stati.

    I. Ricezione a mezzo PEC della richiesta di cessazione del/dei servizio/servizi da parte del Cliente
    II. Verifica stato del Cliente e durata contrattuale
    III. Verifiche Tecniche
    IV. Cessazione servizio/servizi
    V. Invio comunicazione a mezzo PEC al Cliente dell'avvenuta cessazione.

T.net S.p.a. | Sede Legale: Via Roberto Lepetit, 8/10 – 20124 Milano – Italy | Tel. 02 97084111 | Fax 02 97084444
Iscritta CCIAA Milano, P.IVA IT03979950874 – R.E.A. MI-2045456 | Cap. Soc. € 652.900,00 i.v. | PEC tnetitalia@cert.tnet.it
Società soggetta alla direzione ed al Coordinamento di "Antonvictor Investment s.r.l."

A seconda della specifica finalità del trattamento, i tempi di conservazione sono fissati dalla legge (24 mesi ad esempio per la conservazione dei tabulati telefonici).

T.net ottempera al diritto all'oblio di cui all'art. 17 del GDPR è il diritto alla cancellazione dei dati di una persona fisica, esteso e regolato anche con riferimento alla società digitale.

Il diritto alla cancellazione prevale quindi sull'interesse alla conservazione: nei casi previsti, se un interessato chiede la cancellazione dei propri dati T.net **procederà** senza ingiustificato ritardo, e quindi senza riservarsi di continuare a trattare il dato sino alla scadenza originariamente fissata, prossima o meno che sia.

61. T.net adotta l'hardening, cioè il rafforzamento delle piattaforme installate dal punto di vista della security.

    Fondamentalmente seguiamo due diverse tipologie di hardening:

    - One Time Hardening. Viene effettuato solo una volta e dopo il primo setup e la relativa immissione del modulo nel ciclo aziendale.

    - Multiple time hardening. Viene effettuato più volte durante la vita della piattaforma, e la sua ripetizione nel tempo dipende da due fattori fondamentali che sono il rilascio di service pack o major upgrade release o l'aggiunta di moduli complementari a quello installato di base o modifiche architetturali.

    Le nostre VM in configurazione hardening vengono rese disponibili sugli appositi Cataloghi pubblici del servizi DCaaS.

    Per i servizi PaaS il cliente attinge direttamente a template appositamente aggiornati con gli ultimi standard di sicurezza.

62. Tutte le comunicazioni erogate da T.net avvengono tramite protocollo HTTPS, SSL e TLS garantendo che i dati trasmessi raggiungano la corretta destinazione.

63. T.net registra i log di tutti i restore dei backup su appositi repository.

64. T.net assicura un uso limitato del materiale cartaceo. Il materiale a sua volta viene distrutto attraverso la triturazione degli stessi.

65. T.net assicura il mantenimento delle copie delle politiche di sicurezza e delle procedure operative per un periodo di 12 mesi.

66. T.net assicura che una volta deallocati gli spazi storage dei Clienti cessionari questi vengono formattati (zeroed) prima di essere ri-assegnati.