Carta delle Sicurezza di TI Trust Technologies

DOCUMENTO DEL SGQSI – DESCRIZIONE POLICY E MISURE PER LA SICUREZZA

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima emissione	24/09/2019

Indice degli argomenti

Premessa

Il processo di gestione della sicurezza in TI Trust Technologies costituisce un elemento critico e abilitante in ognuna delle fasi del ciclo di vita dei servizi erogati alla Clientela. La sicurezza dei servizi è intesa come una componente indispensabile per garantire e preservare la qualità del servizio offerto ed è considerata parte integrante dei processi operativi. Nel seguito sono illustrate le informazioni utili per spiegare l'approccio di TI Trust Technologies alla gestione del sistema per la sicurezza e fornire dati di riferimento sul suo funzionamento.

Elementi dell'approccio alla sicurezza di TI Trust Tecnologies	1. Politica per la gestione della sicurezza; 2. Rischi e minacce al Sistema ICT; 3. Contromisure di sicurezza; 4. Verifica dell'adeguatezza delle misure di sicurezza; 5. Obblighi, responsabilità e indennizzi; 6. Trattamento dei dati personali.

1 Politica per la gestione della sicurezza

TI Trust Technologies adotta una strategia di gestione della sicurezza integrata con il Gruppo TIM, che si caratterizza per implementazioni tecnologiche, organizzative e di processo che permettono di controllare, gestire, governare il relativo rischio e di garantire nel tempo il livello desiderato di riservatezza, integrità, disponibilità, autenticità e non ripudio delle informazioni raccolte e dei servizi erogati, in funzione l'evolversi delle problematiche di sicurezza e delle tecnologie.

Siti di erogazione dei servizi	<u>Esclusivamente</u> presso le sedi di: 7. Pomezia, dove sono collocati la Sede Legale, il Data Center e la Business Continuity Infrastructure; 8. Roma, dove è collocata l'infrastruttura di Disaster Recovery.

Cosa intendiamo per **INFORMAZIONE**	9. Dati in transito sulla rete (ad es. dati del personale, dati di posta, dati di traffico internet, log & alert dei servizi infrastrutturali, dati aziendali classificati); 10. Beni o risorse (asset) materiali o immateriali, tra i quali: ✓ organizzazione aziendale (personale, norme aziendali, processi); ✓ supporti indipendenti di memorizzazione (cartacei ed elettronici); ✓ software utilizzato per il trattamento dei dati o relativo al sistema operativo/middleware; ✓ attrezzature ICT, quali Desktop, computer portatili e sistemi mobili (laptop, palmari, smartphone, etc.), Server, Reti di comunicazione Stampanti e fax, etc.; ✓ infrastrutture fisiche (armadietti, locali riservati, cablaggi, impianti elettrici, telefonici, di condizionamento, sedi aziendali, ecc.)

Cosa intendiamo per **SICUREZZA DELLE INFORMAZIONI**	Insieme di principi e requisiti necessari a proteggere e tutelare il patrimonio informativo aziendale, ed in particolare • **Riservatezza**: necessità di non rivelare o di non divulgare ad individui, entità o processi non autorizzati, le informazioni; • **Integrità**: impedire l'alterazione, cancellazione, compromissione, accidentale o volontaria delle informazioni da parte di individui, entità e processi; • **Disponibilità**: garantire la continuità nella fruizione delle informazioni, all'interno di un intervallo temporale prestabilito e conforme agli obiettivi ed alla missione aziendale; • **Access Control**: meccanismi che, accertando preventivamente l'autenticità degli individui, forniscono l'appropriato livello di accesso a informazioni o beni aziendali; • **Non Ripudio**: l'accesso ed il trattamento delle informazioni avvengano senza la possibilità di rinnegare le operazioni effettuate in termini di ricezione, trasmissione, trasporto, consegna, creazione, modifica e cancellazione delle informazioni.

2 Rischi e minacce al Sistema ICT

Le misure di sicurezza adottate da TI Trust Technologies per il proprio Sistema ICT sono definite ed mantenute aggiornate a seguito di un processo periodico di valutazione del rischio, che prende in considerazione tutti gli asset aziendali (processi, informazioni e risorse materiali) le cui dinamiche possano comportare ragionevoli rischi di riservatezza, integrità e disponibilità del patrimonio informativo aziendale ed i cui impatti possano avere conseguenze sul complesso delle attività operative.

L'attività di valutazione del rischio viene svolta:

- con cadenza periodica, in fase di revisione e verifica del Sistema di Gestione per la Qualità e Sicurezza delle Informazioni;
- in caso di variazioni straordinarie e significative all'apparato organizzativo;
- in fase di progettazione di nuovi prodotti/servizi, quando lo richiedano la loro natura, obblighi normativi o esigenze interne.

Nell'ambito del processo di valutazione del rischio per il Sistema ICT, sono individuate le cause di rischio seguenti (rif. ISO 27002 ed ENISA):

Tipologia	Elementi di dettaglio
Danni fisici e ambientali (Natural hazards)	• Incendio; • Fenomeni climatici e sismici; • Danni generati da attività industriale; • Allagamento
Perdita di servizi essenziali (Essential services)	• Surriscaldamento dei locali; • Mancanza di Alimentazione Elettrica; • Danneggiamento delle linee di trasmissione
Problemi tecnici e tecnologici (Essential services)	• Perdita di performance di rete/sistemi/applicazioni; • Debolezze del software; • Guasto tecnico dell'hardware; • Inadeguato/mancato utilizzo di controlli crittografici; • Guasto tecnico delle componenti della rete; • Interruzione del servizio

Azioni non autorizzate (Human made threats)	• Accesso fisico non autorizzato; • Copia e uso illegale del software; • Malicious software; • Danneggiamento di apparecchiature fisiche; • Utilizzo improprio di risorse e servizi aziendali; • Errori di gestione/amministrazione sistemi/ apparati/applicazioni; Accesso non autorizzato a sistemi e applicazioni
Compromissione di informazioni (Human made threats)	• Furto ad opera di dipendenti; • Furto ad opera di esterni; • Deterioramento dei dispositivi di memorizzazione; • Intrusione nella rete aziendale; • Errato instradamento di messaggi; • Compromissione della disponibilità delle informazioni; • Recupero di informazioni da supporti riutilizzati o dismessi; • Trattamento non idoneo dei dati
Errori organizzativi/ operativi (Human made threats)	• Errata gestione delle relazioni con le terze parti; • Errata gestione dei servizi erogati dai fornitori; • Mancata/errata implementazione delle procedure di installazione e configurazione del software in esercizio; • Errata valutazione, decisione, comunicazione sugli eventi di sicurezza; • Modello organizzativo non allineato ai nuovi processi; • Ruoli, responsabilità e autorità non allineate alle necessità di processo; • Monitoraggio e miglioramento del SGSI assente/inadeguato; • Mancata/errata risoluzione di NC/azioni di miglioramento/Piani di adeguamento; • Clausole contrattuali incomplete/assenti; • Verifiche ispettive insufficienti/irregolari; • Falso documentale; • Errata gestione/manutenzione dell'asset inventory
Progettazione non sicura (Human made threats)	• Errori di progettazione iniziale/evolutiva; • Sviluppo non sicuro o non conforme a requisiti di sicurezza; • Errata/mancata esecuzione di VA/test di accettazione e sicurezza; • Project management non orientato alla sicurezza delle informazioni

3 Contromisure di sicurezza

Le misure adottate a protezione del Sistema ICT di TI Trust Technologies forniscono un livello elevato di protezione dei dati e del business dei Clienti e sono relative a:

1. Sicurezza fisica
2. Sicurezza logica
3. Sicurezza negli aspetti organizzativi
4. Gestione della continuità operativa

3.1 Sicurezza fisica

- Protezione dei perimetri esterni, mediante dispositivi tecnici locali e presidi di vigilanza e ronda armata h24 7x7;
- Controllo accessi agli edifici, agli uffici e agli archivi elettronici e cartacei;
- Infrastrutture di sicurezza e prevenzione del Data Center:
  - sistemi anti-intrusione (porte resistenti ad elevate sollecitazioni meccaniche e termiche, sensori su porte e finestre collegati ad un sistema di segnalazione degli allarmi locali/remoti, segregazione da aree di transito, registro degli accessi fisici);
  - ridondanza dei cablaggi energia e rete e continuità elettrica (segregazione delle cabine e dei cablaggi, linee multiple, sistemi di continuità statici UPS, generatore di back-up;
  - rilevazione fumi ed antincendio (rilevatori antifumo e sistemi antincendio con attivazione degli impianti di spegnimento automatico degli incendi a saturazione di ambiente);
  - antiallagamento (sonde di rivelazione presenza liquidi);
  - controllo HVAC –heating, ventilation & air conditioning (temperatura 18 - 24 gradi ± 1 °C; umidità relativa 30-70%, ricambi d'aria pari a 0,5 volumi/ora, generazione del freddo industriale attraverso 5 gruppi frigoriferi per 900.000 fr/h cadauno, distribuzione acqua refrigerata attraverso circuiti primario e secondario ad anello, 3 vasche di accumulo acqua da 10.000 litri);
  - facility monitoring (i dispositivi di alimentazione, condizionamento/raffreddamento, antiallagamento, rilevazione temperatura ed umidità e antincendio sono allarmati e supervisionati in remoto responsabile della supervisione all'interno del Centro Servizi.

3.2 Sicurezza logica

3.2.1 Modello logico

L'infrastruttura per l'erogazione di TI Trust Technologies è organizzata sulle seguenti componenti principali:

- **Front-End**: unico punto di accesso dall'esterno per l'interazione con i servizi;
- **Back-End**: componente core ad altissima sicurezza non raggiungibile da connessioni esterne all'infrastruttura TI Trust Technologies;
- **Management Network**: irraggiungibile dall'esterno di TI Trust Technologies, è utilizzata per la gestione di tutti i sistemi e gli applicativi;
- **Backup Network**: è la rete attraverso la quale passano tutti i flussi di dati necessari per il salvataggio e l'archiviazione dei dati;
- **Disaster Recovery Network**: è utilizzata per duplicare i sistemi che erogano dei servizi ed è collegata agli altri componenti dell'architettura mediante la rete privata VDCN che interconnette i Data Center TIM.

3.2.2 Misure di protezione delle componenti logiche

- Firewalling (articolato su molteplici livelli ed in alta affidabilità, filtra il traffico verso le diverse componenti ed è collegato ai sistemi di monitoraggio di TIM);
- IDS -Intrusion Detection System- ed IPS -Intrusion Prevention System- (controllano in tempo reale il traffico diretto alle piattaforme di erogazione dei servizi per intercettare attacchi ed anomalie e sono collegati ai sistemi di monitoraggio di Cyber Security di TIM);
- Antivirus;
- Verifica periodica dello stato dei sistemi e degli applicativi rispetto a vulnerabilità note;
- Ridondanza dei componenti critici delle piattaforme di erogazione e dei sistemi di protezione;

- Adozione di protocolli sicuri nelle comunicazioni (all'interno le attività operative sono svolte mediante connessione protette da sistemi firewall e proxy, con protocolli di autenticazione; le attività degli addetti IT operano in modalità SSH con accesso controllato da FIREWALL e autenticazione centralizzata LDAPed è escluso l'accesso ai sistemi via rete al di fuori della LAN locale);
- Profilazione ed amministrazione delle utenze secondo le policy del Gruppo TIM (principi di livello di criticità, separazione e necessità);

3.2.3 Backup & Restore

I dati e le informazioni contenuti nel sistema ICT di TI Trust Technologies sono soggetti a politiche di back up che si differenziano in funzione della tipologia dei dati e della loro riservatezza. Le politiche di Back Up di base sono:

- Back Up *incrementale giornaliero*
- Back Up *full settimanale*
- Retention dei dati di 1 mese

L'attività di ripristino totale o parziale prevede:

- identificazione del perimetro d'intervento, ovvero individuazione dei server sui quali deve essere eseguita l'attività di ripristino per rendere consistenti i dati;
- selezione dei dati di back-up in base all'identificativo temporale (giorno e ora);
- esecuzione del restore dei dati e verifica dell'esito positivo; nel caso in cui il restore non abbia esito positivo, viene effettuata un'operazione di roll-back.

3.2.4 Monitoraggio

I sistemi di monitoraggio adottati si avvalgono delle infrastrutture del Gruppo TIM per la visualizzazione e la notifica degli allarmi relativi a:

- corretto funzionamento dei sistemi in rete;
- raggiungibilità dei sistemi;
- stato dei sistemi (utilizzo CPU, spazio disco, schede di rete, processi, ecc.).

3.2.5 Patch Management

Tale processo limita il livello di esposizione a rischi di sicurezza del Sistema ICT derivante da attacchi che sfruttano vulnerabilità note e si articola in:

- individuazione delle vulnerabilità sia derivanti da segnalazioni specifiche, sia da fonti aperte;
- analisi degli elementi delle vulnerabilità per valutarne il livello di criticità, anche in relazione al parco di sistemi ed applicativi installato ed operante
- acquisizione e collaudo delle patch da applicare, per valutarne l'impatto e la compatibilità;
- installazione delle patch.

3.2.6 Gestione delle credenziali

3.2.6.1 Credenziali degli Utilizzatori dei servizi

Gli Utilizzatori dei servizi di TI Trust Technologies accedono attraverso Portali, mediante userid e password o attraverso dispositivi di sicurezza (smartcard, token, ecc.).

Per la formazione delle password sono implementati gli accorgimenti e le raccomandazioni provenienti dalle più autorevoli fonti di riferimento.

Le indicazioni per l'adozione di credenziali coerenti sono fornite agli utilizzatori in fase di utilizzo dei servizi (autenticazione, cambio e/o reset password).

3.2.6.2 Credenziali degli Addetti IT

La gestione delle credenziali e dei privilegi di accesso alle risorse ICT è guidata dal criterio "Need to Know" e dal principio di "Segregation of Duty". Il ciclo di vita delle credenziali di accesso degli addetti IT si compone dalle seguenti fasi:

- **creazione e provisioning**: verifica e formalizzazione dell'attribuzione di utenze privilegiate a vario titolo e vengono rilasciate le opportune credenziali e privilegi iniziali;
- **gestione**: modifica, sospensione o riattivazione delle credenziali e dei privilegi, a fronte di richieste autorizzate in accordo alle politiche di sicurezza interne;
- **cessazione**: revoca dei privilegi nei casi di naturale scadenza dell'account, problemi di sicurezza, oppure per opportuna e giustificata richiesta;
- **verifica**: monitoraggio sulla sussistenza delle esigenze che ne hanno determinato l'attivazione delle utenze.

3.3 Sicurezza negli aspetti organizzativi

3.3.1 Elementi della sicurezza relativi al personale

Rientrano in tale contesto l'insieme delle contromisure adottate per minimizzare i rischi connessi alla gestione delle informazioni e relativi al "fattore umano", con riferimento sia al personale dipendente, sia a quello non dipendente, anche presente temporaneamente:

- collocazione del personale interno in **ruoli e responsabilità** coerenti con il rispettivo livello di competenza e capacità;
- selezione del personale dipendente ed esterno sulla base dell'**esperienza**, della **competenza**, delle **capacità** e delle **attitudini** relative ai comportamenti organizzativi, con riferimento alle policy del Gruppo TIM;
- **accordi di riservatezza** contenuti nei contratti di lavoro o di prestazione per tutelare l'azienda ed i clienti da trattamenti non autorizzati delle informazioni gestite, la cui violazione comporta l'applicazione di specifici provvedimenti;
- **consapevolezza e formazione** mediante interventi mirati per la costante sensibilizzazione del personale sul tema della sicurezza delle informazioni;
- **gestione dei diritti di accesso** rispetto al ciclo di vita del rapporto di lavoro, sia per quanto concerne i locali aziendali, sia per quanto concerne le risorse informatiche;
- nomina dei dipendenti quali **incaricati del trattamento**, con la consegna di dettagliate istruzioni scritte che specificano i comportamenti da adottare per ottemperare alle disposizioni di legge, con particolare riferimento alle misure previste per garantire la protezione dei dati personali.

3.3.2 Processo di gestione degli incidenti

Gli ambiti di intervento relativi alla sicurezza sono distinto in:

- **dominio della prevenzione**: a carattere ordinario, consente di limitare gli eventi con effetti dannosi sul business aziendale;
- **dominio dell'emergenza**: a carattere straordinario, consente di reagire ad un incidente occorso e di ripristinare la normale operatività.

Cosa intendiamo per **INCIDENTE**	Qualsiasi evento negativo, di natura casuale, colposa o dolosa, che possa arrecare danni alle persone, al patrimonio (asset materiali e immateriali) e/o pregiudizio alla capacità del Gruppo TIM di rendere un servizio al livello previsto o di mantenere i livelli di ricavi attesi. È pertanto incidente ogni evento o attività non conforme alle politiche di sicurezza ed alle strategie dell'organizzazione e del Gruppo TIM. Tra gli incidenti si distinguono: • **Fatto Anomalo**: incidente che determina un danno di qualsiasi genere al Gruppo TIM, senza per questo violare norme di carattere civile o penale; • **Illecito**: incidente provocato dalla violazione di norme di carattere civile o penale che cagioni un danno al Gruppo TIM, ai suoi clienti o anche a tersi, se si configura un coinvolgimento o una responsabilità di qualsiasi tipo del Gruppo stesso

Il processo di gestione degli incidenti si articolo nelle fasi seguenti:

Fase	Attività previste
Identificazione dell'incidente	Individuazione dell'incidente e raccolta delle prime informazioni necessarie a caratterizzarne la natura e la criticità ed a segnalarlo alle strutture competenti.
Analisi e Classificazione	Raccolta ed analisi delle informazioni correlate all'incidente, per stabilirne la natura, le cause, le risposte prodotte dalle misure di protezione attive e la definitiva classificazione.
Notifica ed escalation	Comunicazione dell'incidente ai responsabili ed al personale preposto alla sua gestione.
Risposta	**Contenimento e contrasto**: trattamento temporaneo (short-term solution) dell'incidente per limitarne i danni e collezionare le evidenze/prove che lo qualificano, eventualmente da usare in un procedimento disciplinare/penale; **Recovery**: ripristino dello stato delle risorse e dei servizi impattati precedente all'incidente.
Follow-up	Review dell'incidente per la definizione la strategia o delle azioni da adottare per impedire il ripetersi dell'incidente,

3.4 Gestione della Continuità Operativa

È governata da un piano che:

- illustra l'approccio alla Continuità Operativa per la fornitura dei servizi erogati da TI Trust;
- descrive i processi per la gestione in ordinario e in emergenza della Continuità Operativa, identificando gli attori coinvolti e definendo i relativi ruoli e responsabilità;
- descrive le soluzioni di continuità per la tutela di tali processi, garantendo requisiti di ripristino adeguati alle loro caratteristiche.

In sintesi, la Continuità Operativa viene attuata avendo riguardo alle fattispecie seguenti:

- **Governo complessivo** della Continuità Operativa, con particolare riguardo all'individuazione dei processi e dei principali scenari di crisi per cui predisporre le soluzioni da adottare per garantire la continuità operativa dei processi rispetto gli scenari presi in considerazione;
- **Gestione in Ordinario** della Continuità Operativa, con particolare riguardo all'identificazione delle strutture e degli attori coinvolti nei processi per la gestione ordinaria della Continuità Operativa e le relative attività per la predisposizione delle soluzioni adottate;
- **Gestione in Emergenza** della Continuità Operativa**Errore. L'origine riferimento non è stata trovata.**, con particolare riguardo alla classificazione degli eventi e dei livelli di emergenza, all'individuazione delle modalità di attivazione delle soluzioni, di comunicazione e delle strutture da attivare in escalation;

- **Piano di Disaster Recovery**, che descrive la soluzione tecnologica individuata per implementare la funzionalità di Disaster Recovery, gli aspetti organizzativi e procedurali adottati e le operazioni necessarie per la normale amministrazione del sito di Recovery e per l'attivazione dello stesso in caso di necessità.

Gli scenari di crisi presi in considerazione nel piano di continuità operativa sono:

1. **distruzione o inaccessibilità dei locali**, comprende le possibili casistiche relative all'impossibilità di accedere ai siti necessari per l'erogazione dei servizi;
2. **indisponibilità del personale essenziale**, comprende le possibili casistiche relative all'indisponibilità del personale essenziale, intesa come assenza prolungata di un numero considerevole delle persone necessarie per l'erogazione dei servizi;
3. **interruzione del funzionamento delle infrastrutture**, prende in considerazione le possibili casistiche relative all'interruzione dell'erogazione dell'energia elettrica o del funzionamento dei servizi di fonia, ovvero del sistema informativo, fattispecie che determina l'attivazione della soluzione di Disaster Recovery.

Le tipologie di incidenti prese in considerazione per l'attivazione del Piano di Disaster Recovery sono:

- **incidenti dovuti a cause naturali**;
- **incidenti non naturali premeditati o accidentali;**
- **incidenti alle facility/infrastrutture**.

4 Verifica dell'adeguatezza delle misure di sicurezza

TI Trust Technologies verifica periodicamente l'adeguatezza ed efficacia delle misure di sicurezza adottate provvedendo ad adeguare le stesse alla particolare evoluzione tecnologica del settore, al fine di mantenere elevato il livello di protezione e ridurre, quindi, il livello di rischio.

L'attività di verifica viene attuata mediante procedure di monitoraggio e di audit:

- Il monitoraggio è effettuato dai responsabili interni che eseguono un controllo costante dell'effettivo funzionamento del Sistema ICT e delle misure di sicurezza, adottando tutte le misure necessarie ad incrementarne il livello di efficacia;
- la previsione di attività di *audit*, regolate dal Piano di Audit Interno quale controllo saltuario svolto da soggetti diversi dai responsabili interni, per un giudizio imparziale circa la qualità delle misure di sicurezza approntate ed in grado di evidenziare non conformità ed eventuali elementi per il miglioramento della loro efficacia

5 Obblighi, Responsabilità e Indennizzi

Gli obblighi e le responsabilità assunti da TI Trust Technologies per le attività svolte sono individuati nelle Condizioni generali per l'utilizzo dei servizi (valide per tutti i servizi acquistati o utilizzati) e nelle Condizioni specifiche, che variano in funzione dei servizi utilizzati. I relativi documenti sono disponibili sul sito di TI Trust Technologies.

6 Trattamento dei dati personali

Le informazioni relative al trattamento dei dati personali che TI Trust Technologies effettua in qualità di Titolare del trattamento sono contenute nei seguenti documenti pubblicati sui siti di riferimento:

- Informativa all'interessato sul trattamento dei dati personali.
- Web Privacy Policy.