	Tipo documento: **Allegato Tecnico**
Titolo documento*:* ***Allegato Tecnico di Compliance soluzione/progetto SPC Cloud Lotto 1 cliente ASUR Marche***	

ALLEGATO TECNICO DI COMPLIANCE

Di seguito sono trattati gli aspetti specifici del GDPR per i servizi IT oggetto del contratto come:

- l'elenco dei trattamenti affidati a TIM e/o suo fornitore nel ruolo di controller o processor
- la tipologia dati
- un insieme di requisiti (intesi come misure di sicurezza), definite dalla policy di Compliance TIM, da valutare prima di svolgere il trattamento in coerenza ai principi della privacy by design e by default. Ad esse si aggiungono, ove applicabile e in relazione al servizio, le misure di sicurezza specifiche per rispondere alle esigenze del cliente e previste dai contratti in corso.

Anagrafica Cliente

Cliente: Ragione Sociale	**ASUR Marche**
Referente Cliente ("Referente DPO se disponibile" o referente tecnico)	**Referente DPO**
Nome Referente	Francesco
Cognome Referente	Moroncini
email	dpo.asur@sanita.marche.it
cellulare	
telefono	071/9030585

Anagrafica TIM S.p.A.:

	TIM S.p.A.
Ragione Sociale	TIM S.p.A.
Codice Fiscale/Partita IVA	00488410010
Rappresentante per Soggetti/Fornitori extra UE	
Mail Rappresentante per Soggetti/Fornitori extra UE	

Anagrafica Fornitore Dinets S.r.l.:

Fornitore	Dinets S.r.l.
Fornitore: Ragione Sociale	Dinets S.r.l.
Codice Fiscale /Partita IVA	02030980425
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

1. Anagrafica Soluzioni/Piattaforme, Tipo dato, Trattamenti e Responsabili dei Trattamenti

Soluzioni per le quali TIM è Titolare dei Trattamenti

Soluzioni per le quali TIM o fornitori/partner sono Responsabili al Trattamento				
Nome Soluzione (Tipologia soluzione Standard, Personalizzata o Custom)	Tipologia Dati (Perimetro di Compliance)	Categorie di Trattamenti e Responsabili dei Trattamenti		Ubicazione piattaforma e dati trattati
Soluzione/Progetto SPC Cloud Lotto 1 - “Personalizzata”	Dati Personali Comuni Dati Particolari Sensibili Dati particolari relativi alla Salute Dati particolari “Fascicolo Sanitario Elettronico / Dossier Sanitario” Dati particolari biometrici o genetici	Gestione sistemistica infrastrutturale	TIM S.p.A. (CR.CD.R)	DC TIM S.p.A. (Mercato) di Rozzano (MI). Centri Servizi TIM S.p.A. di Rozzano sito in Viale Toscana 3 (MI), di Pomezia sito in Via Pontina Km. 29.1000 (RM), di Oriolo sito in Via Oriolo Romano 257 Roma e di Acilia sito in Via di Macchia Palocco 243.
		Gestione sistemistica delle VM	TIM S.p.A. (CR.CD.R)	
		Storage	TIM S.p.A. (CR.CD.R)	
		Gestione middleware	Dinets S.r.l.	
		Gestione database	Dinets S.r.l.	
		Gestione applicativa	Dinets S.r.l.	
		Backup	TIM S.p.A. (CR.CD.R)	
		Gestione sistemistica dell'apparato e raccolta, consultazione e conservazione dei security log (ad es. gestione FW, IDS, ...)	TIM S.p.A. (CR.CD.R)	

Soluzioni per le quali TIM o fornitori/partner sono Responsabili al Trattamento			
Nome Soluzione (Tipologia soluzione Standard, Personalizzata o Custom)	Tipologia Dati (Perimetro di Compliance)	Categorie di Trattamenti e Responsabili dei Trattamenti	Ubicazione piattaforma e dati trattati
			Sedi TIM S.p.A. di Bari sita in Via Dioguardi 1, di Taranto sita in Via Campania 11 e di Acilia Roma sita in Via di Macchia Palocco 243. Sede Dinets S.r.l. di Ancona Via Albertini, 36 / Blocco B4 - 60131 Ancona (AN)

Responsabile dello sviluppo software (non oggetto di questo contratto)	Nome Soluzione
Dinets S.r.l.	Nauta Salus

Stati extra UE dove trasferiti dati	Rappresentante per clienti extra UE

Presenza di servizi/trattamenti in cogestione col cliente	Nome servizio/trattamenti in cogestione col cliente
No	

2. Allegato Tecnico “Requisiti di sicurezza dei dati”

Le piattaforme sono raggruppate per tipo dati e/o in perimetri (“perimetri di compliance ICT Mercato”) sulla base della della natura dei dati trattati secondo quanto dichiarato dal Cliente (nel caso di infrastrutture IaaS o altre piattaforme infrastrutturali) o propria del servizio erogato (nel caso di SaaS/Applicazioni, Verticali e/o Soluzioni a progetto).

Attenzione, si precisa che quanto riportato nel presente documento fa riferimento solo ai servizi SPC Cloud Lotto 1 contrattualizzati dal Cliente (IaaS, Managed Services, BaaS e Cloud Enabling).

Si precisa, inoltre, che per i servizi standard IaaS, Managed Services e BaaS gli aspetti di sicurezza sono disciplinati all’interno del Documento Programmatico di Sicurezza (cod. SGSI-SPC1-0022) formalizzato con CONSIP e previsto dal Contratto Quadro SPC Cloud Lotto 1.

GLOSSARIO: Nelle misure di sicurezza sono riferiti i seguenti ruoli:

- Gestori IT: Il Gestore è il responsabile della gestione tecnica (sviluppo, esercizio, manutenzione, aggiornamento, ecc.) di un sistema ICT
- Addetti IT: I soggetti autorizzati da società del gruppo TIM al trattamento, destinatari di utenze di accesso amministrativo, preposte alla gestione sistemistica o applicativa della piattaforma. Possono essere interni (dipendenti di TIM) o esterni (dipendenti del Partner o del Fornitore)
- End-User Incaricati: Utilizzatori finali del servizio IT (ad es. dipendenti del Cliente) caratterizzati da utenze di accesso all’Applicativo, autorizzati da parte del titolare, cioè il Cliente business a compiere operazioni di trattamento sui dati gestiti dall’applicativo. Possono assumere anche il ruolo di Amministratore dell’Applicativo.
- End-User interessati: Rappresentano i soggetti cui si riferiscono i dati personali gestiti dall’applicativo e che possono eventualmente essere anche utilizzatori finali del servizio IT; in tal caso sono assegnatari di utenze di accesso all’Applicativo di tipo non amministrativo, con profili ristretti ai dati di propria competenza.

2.1. Perimetro “231/reati informatici” e/o Perimetro Dati Personali Comuni

Questo perimetro è composto da piattaforme che:

- non trattano dati personali. Il Modello Organizzativo e la relativa Policy TIM prevedono una rilevanza a medio rischio reato D.Lgs 231/01 – Reati informatici.
- trattano i Dati Personali “comuni”. Tali dati afferiscono alle informazioni relative alla persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altro dato, ivi compreso un numero di riconoscimento personale.

Laddove applicabile, all’interno del testo requisito, è indicata la corrispondente misura minima Agid soddisfatta attraverso la nomenclatura ABSC (Agid Basic Security Controls), cioè con identificatore agerarchico a tre livelli x,y.z preceduti dalla lettera M per indicare la misura come minima (**[M].x.y.z**).

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
CdC-ICT.003.1	Canali di comunicazione	Le piattaforme e gli apparati in DC TIM sono protetti da meccanismi per la rilevazione del traffico anomalo (es. sonde di sicurezza) in grado di rilevare sia attacchi provenienti dalla rete di gruppo TIM verso le piattaforme, sia attacchi uscenti dalle piattaforme (qualora gestite da personale di TIM) verso la rete pubblica.	In carico a TIM S.p.A.
CdC-ICT.006.1	Canali di comunicazione	Sulle piattaforme al momento della messa in produzione del sistema, viene svolta una attività di vulnerability assessment (ingaggiando le funzioni preposte) con una metodologia di tipo non intrusivo e/o con l'utilizzo di tool automatici. La possibilità di effettuare l'attività di VA è valutata e documentata al momento della messa in produzione della piattaforma, in funzione delle possibili criticità emerse durante la fase collaudo. Qualora sulla piattaforma non sia stato svolto un VA in fase di rilascio della stessa in ambiente di esercizio, tale intervento dovrà essere pianificato dalle funzioni preposte. In ogni caso deve essere prevista la rivalutazione del VA in caso di modifiche significative della piattaforma ingaggiando le funzioni preposte.	Effettuato da TIM anche sulle componenti SW utilizzate dall'applicativo
CdC-ICT.007.1	Canali di comunicazione	Sono previsti meccanismi di protezione perimetrale (es. Firewall) delle infrastrutture e dei sistemi. Tali meccanismi ispezionano e proteggono, laddove applicabile, almeno i 3 macro-flussi: 1. dalle reti interne TIM, cliente, fornitore verso la piattaforma; 2. dalla rete pubblica Internet verso la piattaforma; 3. dalla piattaforma verso la rete pubblica Internet.	Lato applicativo sono state adottati meccanismi di protezione (es. cifratura del canale di comunicazione, autenticazione, limitazione indirizzi IP, ecc) Sono descritti nel documento specifico
CdC-ICT.008.1	Canali di comunicazione	Sono adottate e documentate politiche di configurazione degli apparati di sicurezza (es. tipologie e direzione flussi attraverso Firewall, ecc.).	In carico a TIM S.p.A. Dinets ha fornito indicazioni per le relative policy
CdC-ICT.009.1	Canali di comunicazione	Nel caso vengano utilizzati accessi in VPN ai sistemi è identificabile in forma nominativa l'utilizzatore di un dato indirizzo IP (ad esempio mediante VPN client-to-lan o meccanismi di client-authentication delle sessioni).	Applicato Il sistema di autenticazione è fornito da TIM (RAMSES)

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
CoA-ICT.010.1	Controllo accessi	Quando il sistema utilizza la password come dispositivo di autenticazione, sono adottate misure per la protezione (ad es. cifratura) delle credenziali memorizzate a sistema (ad es. password sistemistiche ed applicative, certificati digitali). **[M] 5.11.1:** **[M] 5.11.2:**	Applicato Le misure di sicurezza sono garantite dal fornitore del sistema di autenticazione. Il sistema di autenticazione è COHESION (Regione Marche) per gli end user e RAMSES (TIM) per gli addetti IT
PdE-ICT.010.1	Protezione degli elaboratori	La piattaforma, e le sue componenti, sviluppate internamente da TIM (o da un suo fornitore) sono dotate di software sviluppato secondo metodologie di sviluppo sicuro laddove è applicabile	Applicato
AuL-ICT.008.1 AuL-ICT.008.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da: - produrre la registrazione degli accessi logici (Access Log), compresi i tentativi falliti di accesso, effettuati da parte degli Amministratori di Sistema Addetti IT interni ed esterni - conservare le registrazioni per un periodo di sei mesi.	In carico a TIM S.p.A. La piattaforma di autenticazione è RAMSES
AuL-ICT.009.1	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema Software, la piattaforma tramite cui è effettuato il trattamento di Dati Personali, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa è configurata in maniera tale da: - prevedere meccanismi di registrazione degli accessi logici (access log), compresi i tentativi falliti di accesso; - conservare le registrazioni per un periodo di sei mesi.	Non in ambito di questo contratto (non è oggetto di questo contratto, da indirizzare sul contratto di sviluppo dell'applicativo SW) Gli End User non possono effettuare questa operazione
AuL-ICT.010.1 AuL-ICT.010.2	Audit log	È garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso degli Addetti IT (ad es. tramite l'invio a sistemi di Log Collecting centralizzati).	In carico a TIM S.p.A. La piattaforma di autenticazione è RAMSES

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
AuL-ICT.011.1	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema Software (accesso a livello del Sistema Operativo, del Data Base, dei middleware, di tutte le componenti infrastrutturali comprese le piattaforme di back up e di manutenzione dell'Applicativo), è garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso all'applicativo degli stessi.	Non in ambito di questo contratto
AuL-ICT.012.1 AuL-ICT.012.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da prevedere tecnologie di sincronizzazione al fine di mantenere allineata la data e l'ora associata agli accessi registrati nei log.	Applicato
AuL-ICT.013.1 AuL-ICT.013.2	Audit log	Le registrazioni dei log relativi agli accessi (access log) alla piattaforma degli Addetti IT includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione. **[M] 5.1.2:**	Applicato
AuL-ICT.014.1 AuL-ICT.014.2	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema IT, le registrazioni dei log di accesso (access log) degli stessi all'applicativo includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione. **[M] 5.1.2:**	Non in ambito di questo contratto
Bck-ICT.002.1 Bck-ICT.002.2	Back-up	Al fine di garantire la disponibilità e l'integrità dei dati è prevista la definizione e l'esecuzione di procedure di backup con cadenza almeno settimanale per i dati di configurazione e per i dati del Cliente. **[M] 10.1.1:** **[M] 10.3.1:** **[M] 10.4.1:**	In carico a TIM S.p.A. Servizio BaaS
CdA-ICT.002.1 CdA-ICT.002.2	Credenziali di autenticazione	Tutti i profili di accesso e le politiche di gestione delle utenze degli Addetti IT (interni ed esterni) delle piattaforme sono verificati e aggiornati. Tale verifica avviene con	In carico a TIM S.p.A. L'accesso alla piattaforma

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		frequenza almeno annuale o comunque a seguito di eventi significativi (es. cambi organizzativi, evoluzioni di sistema, etc.). **[M] 5.1.1:**	avviene tramite la piattaforma RAMSES (TIM). Rimane in carico a Dinets di comunicare a TIM la variazione degli Addetti IT
CdA-ICT.003.1 CdA-ICT.003.2	Credenziali di autenticazione	Il Gestore, o un suo delegato, autorizza le utenze degli Addetti IT all'accesso ai dati nella fase di creazione, modifica o monitoraggio (gestione credenziali di accesso). **[M] 5.2.1:**	Applicato Organizzazione interna Dinets
CdA-ICT.004.1 CdA-ICT.004.2	Credenziali di autenticazione	Gli amministratori di sistema sono stati formalmente nominati. **[M] 5.2.1:**	Applicato
CdA-ICT.005.1 CdA-ICT.005.2	Credenziali di autenticazione	Per una gestione delle credenziali di autenticazione, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in modo tale da associare a ciascun utenza dedicata agli Addetti IT credenziali di autenticazione individuali (costituite da una User-ID e un dispositivo di autenticazione - ad es. password). La piattaforma, inoltre, deve prevedere all'accesso meccanismi automatici di verifica delle stesse. **[M] 5.10.2:**	Applicato
CdA-ICT.006.1 CdA-ICT.006.2	Credenziali di autenticazione	Per una gestione delle credenziali di autenticazione, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in modo tale da associare a ciascun utenza dedicata agli End User Autorizzati credenziali di autenticazione individuali (costituite da una User-ID e un dispositivo di autenticazione - ad es. password). La piattaforma, inoltre, deve prevedere all'accesso meccanismi automatici di verifica delle stesse. **[M] 5.10.2:** **[M] 5.2.1:**	L'applicativo non ha meccanismi di autenticazione, ma si appoggia a Cohesion. Il portale di front-end Nauta Salus non richiede credenziali utente ma soltanto il codice licenza rilasciato all'asur per gli operatori. Il processo viene descritto nel documento della sicurezza allegato nella precedente email.
CdA-ICT.007.1 CdA-ICT.007.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a impedire la riassegnazione di User-ID ad altri autorizzati neppure in tempi diversi. **[M] 5.10.2:**	Come sopra

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
CdA-ICT.009.1 CdA-ICT.009.2	Credenziali di autenticazione	La piattaforma è configurata in modo tale che garantisca una soluzione tecnica o procedurale che consenta, in caso di cancellazione di utenze (assegnate ad Addetti IT), di risalire in maniera certa alla persona fisica assegnataria, in un dato periodo, dell'utenza in oggetto. Tali informazioni sono conservate per almeno un periodo di 60 mesi dalla cancellazione delle utenze. **[M] 5.10.2:**	In carico a TIM S.p.A. L'autenticazione degli Addetti IT è effettuatala tramite RAMSES
CdA-ICT.011.1 CdA-ICT.011.2	Credenziali di autenticazione	La piattaforma consente di associare le utenze degli Addetti IT ai profili rispettando i principi di "need to know" e "segregation of duties" **[M] 5.1.1:** **[M] 5.1.2:** **[M] 5.2.1:**	In carico a TIM S.p.A. L'autenticazione degli Addetti IT è effettuatala tramite RAMSES
CdA-ICT.012.1	Credenziali di autenticazione	L'applicativo è sviluppato in maniera tale da consentire la definizione di insiemi di profili di accesso per gli End User Autorizzati che garantiscano i principi di "need to know".	Il profilo dell'end user è definito dall'organizzazione del cliente. Il software permette di definire chi vede cosa.
CdA-ICT.013.1 CdA-ICT.013.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa deve essere configurata in maniera tale che effettui la verifica (almeno settimanale se eseguita tramite modalità automatiche o mensile per analisi procedurali), di tutte le utenze associate ad Addetti IT che hanno lasciato l'azienda al fine di cessare tempestivamente tutte le relative abilitazioni sulla piattaforma. **[M] 5.2.1**:	In carico a TIM S.p.A. Dinets è responsabile di verificare e comunicare a TIM le variazioni. L'autenticazione avviene tramite la piattaforma RAMSES (TIM)
CdA-ICT.014.1 CdA-ICT.014.2	Credenziali di autenticazione	Tutte le utenze degli Addetti IT sono sottoposte a rivalutazioni periodiche circa la sussistenza delle esigenze che ne hanno portato all'attivazione. In particolare le revisioni delle utenze devono essere previste con periodicità almeno annuale **[M] 5.1.1:**	In carico a TIM S.p.A. Dinets è responsabile di verificare e comunicare a TIM le variazioni. L'autenticazione avviene tramite la piattaforma RAMSES (TIM)
CdA-ICT.015.1 CdA-ICT.015.2	Credenziali di autenticazione	L'applicativo è sviluppato in maniera tale da prevedere meccanismi in grado di consentire l'estrazione delle informazioni necessarie alla verifica della corretta attribuzione delle credenziali di autenticazione e dei relativi profili di autorizzazione degli End User Autorizzati.	Le credenziali di autenticazione e i profili sono definiti dal cliente.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		[M] 5.2.1:	
CdA-ICT.018.1	Credenziali di autenticazione	La piattaforma consente la sospensione delle utenze inattive degli End User Autorizzati a valle di periodi di inattività pari o maggiori a 6 mesi, salvo le utenze per le quali è stata preventivamente richiesta ed autorizzata una deroga sulla base di una necessità operativa.	Il portale di front end permette di bloccare le utenze solo nel caso la licenze rilasciata all'Asur sia scaduta o resa inattiva
CdA-ICT.019.1 CdA-ICT.019.2	Credenziali di autenticazione	Il gruppo in carico della creazione e della assegnazione delle credenziali di autenticazione agli Addetti IT richiedenti risulta essere nominato e costituito da un numero circoscritto di Addetti IT preventivamente individuati. **[M] 5.2.1:**	Applicato Dinets nominerà gli Addetti IT e lo comunicherà a TIM
CdA-ICT.020.1 CdA-ICT.020.2	Credenziali di autenticazione	E' precluso l'utilizzo di utenze di Sistema su processi automatici (ad esempio le utenze di Sistema non sono utilizzate come utenze Machine to Machine).	
CdA-ICT.021.1 CdA-ICT.021.2	Credenziali di autenticazione	E' precluso l'utilizzo di utenze di sistema e M2M da parte di persone fisiche, ad eccezione di attività saltuarie (es. gestione emergenze).	
CdA-ICT.022.1 CdA-ICT.022.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che le utenze di sistema non nominali (comprese le M2M) devono essere comunque assegnate (in termini di responsabilità) ad una persona fisica, tipicamente un Responsabile di esercizio o un suo delegato. **[M] 5.10.2:**	Applicato
CdA-ICT.023.1 CdA-ICT.023.2	Credenziali di autenticazione	Gli addetti IT a cui sono assegnate utenze deputate allo svolgimento di attività di sicurezza relative alla protezione dei sistemi (per es. configurazione regole FW o monitoraggio allarmi di sicurezza) sono distinti, a livello di singolo individuo, dagli altri addetti IT degli stessi sistemi. La separazione, a livello di singolo individuo, è applicata anche tra chi configura gli strumenti di sicurezza (es. FW o IDS) e chi svolge attività di verifica della sicurezza (es. vulnerability assessment). **[M] 5.1.1:**	In carico a TIM S.p.A. (infrastruttura SPC Cloud Lotto 1)
CdA-ICT.024.1 CdA-ICT.024.2	Credenziali di autenticazione	Gli addetti IT a cui sono assegnate utenze deputate alla gestione dei file di log sono distinti, a livello individuale, dagli altri addetti IT dello stesso sistema. Nel caso di sistema di supporto dedicato alla gestione dei file di log non sussiste vincolo di incompatibilità	In carico a TIM S.p.A. (infrastruttura SPC Cloud Lotto 1)

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		con le attività di gestione sistemistica / applicativa del sistema stesso.	
CdA-ICT.025.1 CdA-ICT.025.2	Credenziali di autenticazione	Per una gestione delle modalità di accesso dedicate a ciascun Addetto IT interno ed esterno, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che quando il sistema utilizza la password come dispositivo di autenticazione, essa effettui controlli automatici volti a garantire che la password risponda alle caratteristiche previste dalle vigenti policy aziendali. **[M] 5.11.1**: **[M] 5.7.4:**	In carico a TIM S.p.A. La piattaforma di autenticazione utilizzata da parte degli Addetti IT è RAMSES (TIM)
CdA-ICT.026.1	Credenziali di autenticazione	La piattaforma consente la sospensione delle utenze inattive degli Addetti IT a valle di periodi di inattività pari o maggiori a 6 mesi, (salvo le utenze preventivamente autorizzate per soli scopi di gestione tecnica per le quali sia stata concessa una deroga da parte del Gestore IT o suoi delegati). Nel caso di infattibilità tecnica il controllo può essere di tipo procedurale, con frequenza almeno mensile, garantendo comunque la sospensione trascorsi 6 mesi di inattività.	In carico a TIM S.p.A. La piattaforma di autenticazione utilizzata da parte degli Addetti IT è RAMSES (TIM)
CdC-ICT.002.1 CdC-ICT.002.2	Canali di comunicazione	E' prevista l'adozione di apparati hardware e software (ad es. firewall) in grado di contrastare tentativi di accesso non autorizzato da reti dati pubbliche (Internet) al fine di rispettare i livelli di isolamento e protezione dei dati trattati dalla piattaforma stessa. **[M] 8.1.2:**	Applicato
CdC-ICT.012.1 CdC-ICT.012.2	Canali di comunicazione	Per tutti i sistemi in perimetro per i quali sia consentito l'accesso al sistema da parte di entità terze/esterne all'azienda (fornitori), è garantita, salvo diversa indicazione, la sicurezza dei dati scambiati verso l'esterno (es. canali con protocolli sicuri, meccanismi di cifratura).	Applicato
CoA-ICT.004.1 CoA-ICT.004.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa prevede meccanismi automatici di verifica atti a garantire i requisiti di robustezza delle credenziali di autenticazione. A tal fine deve essere prevista l'implementazione di controlli automatici volti a garantire che le credenziali	Per gli Addetti IT in carico a TIM S.p.A. La piattaforma di autenticazione utilizzata da parte degli Addetti IT è RAMSES (TIM)

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		di autenticazione (per es. password) rispondano alle caratteristiche di sicurezza previste. In particolare la password deve prevedere: • lunghezza minima pari a 8 caratteri o al massimo permesso dal sistema; • complessità (la password deve essere costituita da caratteri diversi per tipologia quali lettere, numeri, simboli speciali) • diversità dalle precedenti 4 password (password history); In caso di soluzione/piattaforma destinata alla Pubblica Amministrazione (AgID ABSC Minimo): • se l'autenticazione a più fattori non è supportata, si utilizzano credenziali di elevata robustezza (almeno 14 caratteri) per le utenze da Addetto IT; • se per l'autenticazione si utilizzano certificati digitali viene garantito che le chiavi private siano adeguatamente protette. **[M] 5.7.1:** **[M] 5.7.4:** **[M] 5.11.1:** **[M] 5.11.2:**	Per gli End User non è in ambito di questo contratto. La piattaforma di autenticazione utilizzata da parte degli End User è infatti COHESION. Il SW si appoggia ai sistemi di identity management RAMSES e COHESION
CoA-ICT.006.1 CoA-ICT.006.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione al primo accesso delle password temporanee inizialmente assegnate a ciascun Addetto IT. **[M] 5.11.1:**	In carico a TIM S.p.A. La piattaforma di autenticazione utilizzata da parte degli Addetti IT è RAMSES (TIM)
CoA-ICT.007.1 CoA-ICT.007.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione al primo accesso delle password temporanee inizialmente assegnate a ciascun End User Autorizzato. **[M] 5.11.1:**	Non in ambito di questo contratto. La piattaforma di autenticazione utilizzata da parte degli End User è infatti COHESION
CoA-ICT.008.1 CoA-ICT.008.2	Controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun Addetto IT, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari. **[M] 5.7.3:**	In carico a TIM S.p.A. La piattaforma di autenticazione utilizzata da parte degli Addetti IT è RAMSES (TIM)

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
CoA-ICT.009.1	Controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun End User Autorizzato al Trattamento, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi nel caso di sistemi che trattano dati personali e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari.	Non in ambito di questo contratto. La piattaforma di autenticazione utilizzata da parte degli End User è infatti COHESION
CoA-ICT.014.1 CoA-ICT.014.2	Controllo accessi	Per una gestione di base delle credenziali di autenticazione, la piattaforma IT deve essere configurata in modo tale che associ a ciascun Addetto IT un "profilo di autorizzazione" adeguato a garantire l'accesso ai soli dati che sono strettamente necessari per adempiere ai compiti affidati. **[M] 5.1.1:**	In carico a TIM S.p.A. La piattaforma di autenticazione utilizzata da parte degli Addetti IT è RAMSES (TIM)
Doc-ICT.002.1	Documentazione	Viene garantita l'esistenza di un elenco aggiornato degli eventuali Partner/Fornitori che concorrono all'erogazione del servizio, nella misura in cui effettivamente intervengano nel trattamento dei dati del Cliente. Tale documentazione deve riportare le seguenti informazioni: - identificativo della società esterna; - descrizione sintetica delle responsabilità affidate; - riferimento al contratto di fornitura.	Applicato
PdE-ICT.003.1 PdE-ICT.003.2	Protezione degli elaboratori	La piattaforma prevede il corretto funzionamento e aggiornamento del software di protezione antivirus (prevenzione, rilevazione e rimozione virus e malicious code). Per le piattaforme non sincronizzate con l'infrastruttura antivirus aziendale l'aggiornamento deve avvenire con cadenza almeno mensile. **[M] 8.1.1:**	Non sono presenti antivirus
PdE-ICT.004.1 PdE-ICT.004.2	Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli aggiornamenti del software applicativo (Patch Management).	Applicato Lato SW, in caso di patch di sicurezza rilasciate dal vendor, verranno implementate.
PdE-ICT.005.1 PdE-ICT.005.2	Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli aggiornamenti del software	In carico a TIM S.p.A.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		di sistema (Patch Management).	
PdE-ICT.006.1 PdE-ICT.006.2	Protezione degli elaboratori	Sono state previste attività di configurazione che prevedano la modifica delle impostazioni predefinite del fornitore (ad esempio password, community SNMP, ecc...), l'eliminazione di account e servizi non necessari e la risoluzione delle vulnerabilità di sicurezza note. **[M] 5.3.1:**	Applicato
PdE-ICT.007.1 PdE-ICT.007.2	Protezione degli elaboratori	Le componenti della piattaforma sono dotate di software per il quale l'azienda ha i diritti di utilizzo	Applicato
PdE-ICT.008.1	Protezione degli elaboratori	Tutti i terminali utilizzati per connettersi al sistema prevedono la funzionalità di screensaver con password o in alternativa il sistema abbatte la sessione	Anche i terminali con cui l'enabler si collega soddisfa il requisito
PdE-ICT.009.1 PdE-ICT.009.2	Protezione degli elaboratori	Per i trattamenti che prevedono l'hosting fisico dei dati all'interno di siti TIM, il sistema risiede all'interno di un Data Center, di un Service Center, di una Centrale o di un sito equivalente.	In carico a TIM S.p.A.
PdE-ICT.012.1 PdE-ICT.012.2	Protezione degli elaboratori	E' prevista l'adozione di procedure documentabili e/o tecnologie che consentano la gestione sicura e protetta del codice sorgente del programma. Inoltre i codici sorgente non risiedono sui server in esercizio, se non risultano necessari alla normale operatività del sistema.	Applicato
Ris-ICT.008.1 Ris-ICT.008.2	Riservatezza	È prevista la stesura e la corretta implementazione di procedure atte a regolare il processo di cancellazione dei dati del cliente a seguito della cessazione del contratto (ad es. cessazione di qualsiasi obbligazione derivate da accordi contrattuali oppure in applicazione di specifiche normative) assicurando che tali dati vengano cancellati in maniera definitiva e irreversibile al fine di impedire trattamenti non autorizzati degli stessi da parte di Addetti IT o di eventuali altri Clienti. Le tempistiche di cancellazione sono in linea con quanto previsto a livello contrattuale.	In carico a TIM S.p.A. La cancellazione definitiva è una operazione che può svolgere il proprietario/gestore del datacenter Tra le attività dell' enabler non c'è l'export dei dati.
Ris-ICT.009.1	Riservatezza	E' garantito l'isolamento logico dei dati relativi a clienti differenti su una medesima piattaforma. In particolare, non deve essere possibile accedere/visualizzare i dati di un Cliente diverso da quello che ha acceduto alla piattaforma.	L'isolamento è confermato anche se il cliente in questo caso è unico. La piattaforma software non è utilizzata da più clienti

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
Ris-ICT.010.1	Riservatezza	E' prevista la separazione degli ambienti dedicati alle attività di sviluppo, test e collaudo dall'ambiente di esercizio della piattaforma. Per gli ambienti diversi da quello di produzione nel caso vengano utilizzati dati reali di esercizio, sono garantiti tutti i requisiti di compliance previsti.	Applicato
Ris-ICT.011.1	Riservatezza	E' prevista la redazione formale di apposite procedure di estrazione o trasmissione dei dati trattati dalla piattaforma. Tali estrazioni/trasmissioni devono consentire la portabilità dei dati tramite l'esportazione degli stessi in formati standard in relazione alla tecnologia utilizzata (ad es. sistemi di tipo UNIX) e al layer di trattamento (ad es. DB).	Applicato

2.2. Perimetro Dati particolari Sensibili

Composto dalle piattaforme che trattano Dati Personali Sensibili o Giudiziari. In particolare, di seguito si riporta la definizione di tali tipologie di dati:

- Dati Particolari Sensibili – Dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso filosofico politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale;
- Dati Giudiziari – Dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno dei Perimetri 231 e Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
Bck-ICT.001.1	Back-up	E' prevista la redazione di procedure documentate di ripristino/restore dei dati (e di configurazione se previsto dal contratto). Tali procedure di ripristino dell'accesso ai dati garantiscono tempi non superiori a sette giorni qualora tutti i dati utilizzati dal sistema andassero persi.	Applicato
CoA-ICT.008.1 CoA-ICT.008.2	Controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun Addetto IT, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari.	In carico a TIM S.p.A. La piattaforma di autenticazione utilizzata da parte degli Addetti IT è RAMSES (TIM)
PdE-ICT.001.1	Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	In carico a TIM S.p.A.
PdE-ICT.002.1	Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di DBMS e applicativo oggetto del SaaS, necessari a correggere difetti e prevenire vulnerabilità della piattaforma.	Applicato

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
Ris-ICT.002.1	Riservatezza	Sono previste soluzioni (es. cifratura o altre) che, considerato il numero e la natura dei dati trattati, rendono i dati sensibili o giudiziari temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In particolare la misura deve essere prevista qualora: - rientrino nelle responsabilità della fornitura del servizio le funzionalità applicative (es. SAAS), e le finalità del servizio prevedano (in quanto sostanziale per la finalità e non occasionale) il trattamento dei dati sensibili o giudiziari; - rientrino nelle responsabilità della fornitura del servizio infrastrutturale (IAAS) e il Cliente espliciti la necessità di trattare dati sensibili o giudiziari e richieda formalmente l'espletamento di tale misura a livello infrastrutturale.	Applicato
Sup-ICT.001.1	Supporti	E' prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi.	In carico a TIM S.p.A.

2.3. Perimetro Dati particolari relativi alla salute

Composto dalle piattaforme dedicate a clienti quali organismi sanitari o esercenti le professioni sanitarie che intendono utilizzare il servizio per trattare dati Sensibili idonei a rivelare lo stato di salute e/o la vita sessuale degli interessati.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione, minima, della stessa anche all'interno del Perimetro 231, Dati Personali e Perimetro Dati Sensibili / Giudiziari.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
Ris-ICT.001.1	Riservatezza	Nella piattaforma è prevista al fine di garantire la riservatezza dei dati sanitari conservati (data-at-rest), la cifratura degli stessi o l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In caso di trasmissione dei dati sanitari è garantita in ogni caso la cifratura dei dati.	Applicato

2.4. Perimetro dati particolari “Fascicolo Sanitario Elettronico / Dossier Sanitario”

Composto dalle piattaforme che consentono il trattamento di Dati Personali Sensibili tramite FSE / Dossier Sanitario. Tali insiemi di dati si differiscono dal semplice dato particolare riferito alla salute in termini di condivisione delle informazioni e di titolarità dei dati, come da definizioni di seguito riportate:

- Fascicolo sanitario elettronico (Fse) – insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito (cfr. Allegato C - Definizioni alle Linee guida in materia di Dossier sanitario del 4 giugno 2015). In particolare per Fse si intende il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es. azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area geografica);
- Dossier Sanitario – insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica dai professionisti sanitari che lo assistono, al fine di documentarne la storia clinica e di offrirgli un migliore processo di cura. Tale strumento è costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. ospedale o clinica privata) al cui interno operino più professionisti (cfr. Allegato C - Definizioni alle Linee guida in materia di Dossier sanitario del 4 giugno 2015). In particolare, si parla di dossier sanitario qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. ospedale o clinica privata) al cui interno operino più professionisti. I dossier sanitari possono anche costituire, ad esempio, l'insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in una iniziativa di Fse regionale.

L’appartenenza di una piattaforma a tale perimetro prevede necessariamente l’inclusione della stessa anche all’interno del Perimetro 231, Dati Personali, Perimetro Dati particolari Sensibili / Giudiziari e Perimetro particolari relativi alla salute.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
Ris-ICT.014.1	Riservatezza	L'applicativo è costruito in maniera tale da permettere l'oscuramento (revocabile nel tempo) di taluni dati o documenti sanitari a seguito di richieste dell'interessato. Le informazioni oscurate sono in ogni caso rese disponibili al professionista sanitario o alla struttura interna titolare che li ha raccolti o elaborati. L’oscuramento dell’evento clinico avviene con modalità tali da garantire che i soggetti abilitati all’accesso non possano venire automaticamente a conoscenza del fatto che l’interessato ha effettuato tale scelta.	

Ris-ICT.015.1	Riservatezza	L'applicativo deve essere costruito in maniera tale da permettere la gestione del consenso al trattamento da parte dell'interessato. L'applicativo consente di raccogliere le informazioni e renderle disponibili e visualizzabili esclusivamente a un sottoinsieme di utenze definito dal Cliente business. In caso di revoca dello stesso il Dossier/Fse non è ulteriormente implementato. Le informazioni sanitarie già presenti restano disponibili e visualizzabili esclusivamente alla funzione interna del Cliente che le ha raccolte (non sono più condivise con i professionisti di altri reparti).	n/a La piattaforma non gestisce il FSE, quindi questo onere è del Cliente visto che è lui che mette a disposizione i dati

Di seguito i requisiti aggiuntivi per adeguarsi alla normativa:

ID MISURA Circolare 263	Categoria Mimip	Testo requisito	Dinets S.r.l.
	Log	L'applicativo è costruito in maniera tale da prevedere la possibilità di implementare meccanismi di tracciamento degli accessi e delle operazioni di trattamento del Dossier/FSE effettuate da tutte le utenze autorizzate. Tali ulteriori registrazioni, in accordo con le richieste del Cliente, sono definite contrattualmente e messe a disposizione del Cliente al fine di poter rispondere ad eventuali richieste di visione da parte degli interessati. In particolare, i file di log registrano per ogni operazione di accesso ai Dossier, almeno le seguenti informazioni: l'utenza, la data e l'ora di effettuazione delle operazioni, il codice della postazione di lavoro utilizzata, l'identificativo del paziente il cui Dossier è interessato dall'operazione e la tipologia dell'operazione compiuta. La gestione di tale tracciamenti garantisce la conservazione delle registrazioni per un periodo non inferiore a 24 mesi ed avvenire in accordo alle disposizioni interne previste per tale trattamento	n/a La piattaforma non gestisce il FSE, quindi questo onere è del Cliente visto che è lui che mette a disposizione i dati
	Log	L'applicativo è costruito in maniera tale da prevedere la possibilità di implementare *alert* e meccanismi di *anomaly detection* che individuino comportamenti anomali o a rischio (che possano configurare trattamenti illeciti) relativi alle operazioni eseguite dagli incaricati del trattamento (ad es. relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi), al fine di orientare successivi ed eventuali interventi di Audit interno da parte del Cliente titolare del trattamento.	n/a La piattaforma non gestisce il FSE, quindi questo onere è del Cliente visto che è lui che mette a disposizione i dati
	Riservatezza	L'applicativo è costruito in maniera tale da consentire la gestione di un autonomo e specifico consenso dell'interessato al trattamento tramite Dossier/Fse di particolari tipologie di informazioni. Trattasi di informazioni relative a prestazioni sanitarie offerte a soggetti nei cui confronti l'ordinamento	n/a La piattaforma non gestisce il FSE, quindi

ID MISURA Circolare 263	Categoria Mimip	Testo requisito	Dinets S.r.l.
		vigente ha posto specifiche disposizioni a tutela della loro riservatezza e dignità personale (ad es. infezioni da HIV).	questo onere è del Cliente visto che è lui che mette a disposizione i dati

2.5. Perimetro Pubbliche Amministrazioni (Misure Agid)

Ad aprile 2017 AgiD ha pubblicato nella Gazzetta Ufficiale (GuRI) le Misure Minime di Sicurezza per la PA, un documento che contiene le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni le quali costituiscono parte integrante delle Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni.

Le misure minime Agid sono indicate con la nomenclatura ABSC (Agid Basic Security Controll), cioè con identificatore gerarchico a tre livelli x,y.z preceduti dalla lettera M per indicare la misura come minima (**[M].x.y.z**).

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231/01 reati informatici e del Perimetro Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
PdE-ICT.013.1 PdE-ICT.013.2	Protezione degli elaboratori	E' previsto che venga applicata una protezione crittografica sui dati rilevanti (aventi particolari requisiti di riservatezza). **Il cliente dovrà indicare quali sono i dati rilevanti.** **[M] 13.1.1:**	Applicato
Doc-ICT.012.1	Documentazione	E' prevista l'implementazione di un inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, che registra almeno l'indirizzo IP, da aggiornare quando nuovi dispositivi approvati vengono collegati in rete. **[M] 1.1.1:** **[M] 1.3.1:** **[M]1.4.1:**	N/A Siamo in ambiente cloud
PdE-ICT.014.1	Protezione degli elaboratori	E' prevista la redazione di un elenco di software autorizzati, con relative versioni, necessari per ciascun tipo di sistema, compresi server e al contempo non è consentita l'installazione di software non compreso in tale elenco. E' prevista l'esecuzione di regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. [**M] 2.1.1:** **[M] 2.3.1:**	Applicato
Bck-ICT.004.1	Back-up	Su server e per la protezione dei sistemi operativi, sono definite, impiegate e ripristinate (nel caso vengano compromessi) configurazioni standard.	In carico a TIM S.p.A.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		Le immagini d'installazione sono memorizzate offline. **[M] 3.1.1:** **[M] 3.2.1:** **[M] 3.2.2 :** **[M] 3.3.1:**	
PdE-ICT.015.1	Protezione degli elaboratori	E' assicurato che gli strumenti di scansione delle vulnerabilità (anche per i sistemi separati dalla rete) siano regolarmente aggiornati adottando misure di sicurezza adeguate al livello di criticità. Inoltre è periodicamente verificato che le vulnerabilità emerse dalle scansioni siano state risolte, documentando e accettando in caso opposto un ragionevole rischio. A ciascuna azione utile per la risoluzione delle vulnerabilità è assegnato un livello di priorità in base al rischio associato. Ad ogni modifica significativa della configurazione deve essere eseguita la ricerca delle vulnerabilità con strumenti automatici che forniscano report con indicazioni delle vulnerabilità più critiche. **[M] 4.1.1:** **[M] 4.4.1:** **[M] 4.5.2:** **[M] 4.7.1:** **[M] 4.8.2:**	L'attività di VA è effettuata da TIM anche sulla parte software
PdE-ICT.016.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma. L'installazione avviene automaticamente qualora non preveda un'interruzione o una forte limitazione dell'operatività. In particolare sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1:** **[M] 4.7.1:** **[M] 4.8.2:**	In carico a TIM S.p.A.
PdE-ICT.017.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di DBMS e applicativo oggetto del SaaS, necessari a correggere difetti e prevenire vulnerabilità della	Applicato (attività non automatica)

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		piattaforma. L'installazione avviene automaticamente qualora non preveda un'interruzione o una forte limitazione dell'operatività. In particolare sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1:** **[M] 4.7.1:** **[M] 4.8.2:**	
CoA-ICT.015.1	Controllo accessi	Vengono completamente distinte utenze privilegiate e non privilegiate degli amministratori (alle quali devono corrispondere credenziali diverse), mentre è consentito l'utilizzo delle utenze amministrative anonime (ad esempio “root” di UNIX o “Administrator” di Windows) solo per le situazioni di emergenza; queste vengono gestite in modo da garantire la disponibilità e la riservatezza e in modo da assicurare l’imputabilità di chi ne fa uso. **[M] 5.10.1:** **[M] 5.10.3:**	Applicato
PdE-ICT.018.1	Protezione degli elaboratori	Sulle piattaforme non sono consentite l’esecuzione automatica dei contenuti, dinamici e non, e l'anteprima automatica dei contenuti dei file, anche al momento della connessione dei dispositivi removibili e l'apertura automatica dei messaggi di posta elettronica. Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. **[M]8.3.1:** **[M] 8.7.1:** **[M] 8.7.2:** **[M] 8.7.3:** **[M] 8.7.4:**	Applicato
PdE-ICT.019.1	Protezione degli elaboratori	Qualsiasi supporto removibile utilizzato è automaticamente soggetto ad una scansione anti-malware, inoltre sono adottati e configurati adeguati strumenti di web filtering e nel caso di posta elettronica antispamming bloccando nella posta elettronica e nel traffico web i file potenzialmente pericolosi la cui tipologia non è strettamente necessaria per l’organizzazione. **[M] 8.8.1:**	In carico a TIM S.p.A.

ID MISURA	Categoria Mimip	Testo requisito	Dinets S.r.l.
		[M] 8.9.1: **[M] 8.9.2:** **[M] 8.9.3:**	
CdC-ICT.013.1	Canali di comunicazione	Le operazioni di amministrazione remota di server, dispositivi di rete e analoghe apparecchiature sono eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri). **[M] 3.4.1:**	In carico a TIM S.p.A.
CdC-ICT.014.1	Canali di comunicazione	E' prevista la possibilità di bloccare il traffico da e verso url presenti in una blacklist. **[M] 13.8.1:**	In carico a TIM S.p.A.
Ris-ICT.013.1	Riservatezza	Risulta garantita l'applicazione delle misure di sicurezza derivanti dalle analisi del rischio (Piano di Sicurezza) relative alla piattaforma a supporto del servizio erogato. **[M] 4.8.1:**	Applicato

2.6. Perimetro Dati particolari biometrici o genetici

Attualmente non sono definite misure di sicurezza specifiche per il perimetro dei dati particolari biometrici o genetici.

Si rimanda pertanto alle misure già riportate nei paragrafi precedenti.