Si.net / Cloud	ISO 27001 / 27017 / 27018	v3 del 14/05/2025
	Modalità di erogazione Servizi Cloud	

ATTUAZIONE CONTROLLO	SI.NET COME FORNITORE DI SERVIZI CLOUD				SI.NET COME CLIENTE DEL CSP
	SAAS Interno	Managed SAAS	Managed PAAS	Managed IAAS	
	RIFERIMENTO: PRO	RIFERIMENTO: SIS	RIFERIMENTO: CLD		
Gestione degli accessi (controllo 27017 5.1.1)	Gli applicativi sono forniti di una gestione avanzata degli accessi basata sui concetti di utenze e permessi, nella maggior parte dei casi i permessi vengono distribuiti agli utenti attraverso gruppi che raccolgono più utenze con pari autorizzazioni; Al cliente vengono fornite (una o più) utenze amministrative con le quali è possibile gestire gli utenti ed i relativi permessi. Alcuni applicativi permettono di definire policy di gestione avanzata delle credenziali (scadenza, complessità, …).	Gli applicativi sono forniti di una gestione avanzata degli accessi basata sui concetti di utenze e permessi, nella maggior parte dei casi i permessi vengono distribuiti agli utenti attraverso gruppi che raccolgono più utenze con pari autorizzazioni; Al cliente vengono fornite (una o più) utenze amministrative con le quali è possibile gestire gli utenti ed i relativi permessi. Alcuni applicativi permettono di definire policy di gestione avanzata delle credenziali (scadenza, complessità, …).	La regolamentazione degli accessi è definita nelle Politiche di sicurezza degli ambienti cloud, al cliente vengono fornite credenziali di utilizzo della piattaforma che ne permettono l'utilizzo e a seconda dei casi ammettono la possibilità di generare e gestire altre utenze. Si.net invita, in sede di formazione, il cliente a seguire la proprie politiche di sicurezza; Si.net non dispone di profili di accesso supplementari ma gestisce i servizi solamente a livello di hypervisor.	La regolamentazione degli accessi è definita nelle Politiche di sicurezza degli ambienti cloud, al cliente vengono fornite credenziali di utilizzo della piattaforma che ne permettono l'utilizzo e a seconda dei casi ammettono la possibilità di generare e gestire altre utenze. Si.net invita, in sede di formazione, il cliente a seguire la proprie politiche di sicurezza; Si.net non dispone di profili di accesso supplementari ma gestisce i servizi solamente a livello di hypervisor.	L'accesso alle risorse messe a disposizione dal CSP è regolato secondo la Politica di sicurezza per gli ambienti cloud utilizzando gli strumenti lì definiti.
Comunicazioni ai customer in caso di change (controllo 27017 5.1.1)	Le change vengono analizzate internamente da SI.net monitorando lo stato delle risorse e delle vulnerabilità applicative, la procedura di analisi è tracciata tramite ticket; In caso di necessità di change i clienti vengono avvisati tramite mail.	Le change vengono analizzate internamente da SI.net monitorando lo stato delle risorse e delle vulnerabilità applicative, la procedura di analisi è tracciata tramite ticket; In caso di necessità di change i clienti vengono avvisati tramite mail.	Le change vengono analizzate internamente da SI.net monitorando lo stato delle risorse e delle vulnerabilità applicative, la procedura di analisi è tracciata tramite ticket; In caso di necessità di change i clienti vengono avvisati tramite il canale di comunicazione dedicato agli avvisi.	Le change vengono analizzate internamente da SI.net monitorando lo stato delle risorse e delle vulnerabilità applicative, la procedura di analisi è tracciata tramite ticket; In caso di necessità di change i clienti vengono avvisati tramite il canale di comunicazione dedicato agli avvisi.	La variazione dei servizi viene comunicata attraverso vari canali (mail dedicata, newsletter, console, Partner network,…) a seconda del CSP e viene lasciato un ampio margine di tempo per l'eventuale adeguamento strutturale alle novità.
Comunicazioni con gli interessati in caso di data breach (controllo 27017 5.1.1)	SI.net effettua la gestione del data breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato, SI.net si rende poi disponibile ad affiancare lo stesso per eventuali ulteriori procedure operative.	SI.net effettua la gestione del data breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato, SI.net si rende poi disponibile ad affiancare lo stesso per eventuali ulteriori procedure operative.	SI.net effettua la gestione del data breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato, SI.net si rende poi disponibile ad affiancare lo stesso per eventuali ulteriori procedure operative.	SI.net effettua la gestione del data breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato, SI.net si rende poi disponibile ad affiancare lo stesso per eventuali ulteriori procedure operative.	I CSP, in confrmità al GDPR e alla certificazione 20018 sono tenuti a comunicare a Si.net il verificarsi di eventi di data-breach.
Ciclo di vita degli account (controllo 27017 5.1.1)	Gli account possono essere disabilitati e/o eliminati da utenti con profilo amministrativo direttamente dal cliente, i contenuti relativi a questi account potrebbero essere mantenuti collegati a account "segnalibro" per garantire il funzionamento dell'applicativo.	Gli account possono essere disabilitati e/o eliminati da utenti con profilo amministrativo direttamente dal cliente, i contenuti relativi a questi account potrebbero essere mantenuti collegati a account "segnalibro" per garantire il funzionamento dell'applicativo.	Gli account creati e gestiti da Si.net sono creati e gestiti secondo quanto indicato nelle Politiche di sicurezza, l'eliminazione (o la disabilitazione) di questi avviene su richiesta del cliente, per la violazione di una o più regole di uso lecito, per la rescissione o la naturale scadenza del contratto d'uso. Gli account gestiti dal cliente sono completamente gestiti da questo che ne regola in toto il ciclo di vita.	Gli account creati e gestiti da Si.net sono creati e gestiti secondo quanto indicato nelle Politiche di sicurezza, l'eliminazione (o la disabilitazione) di questi avviene su richiesta del cliente, per la violazione di una o più regole di uso lecito, per la rescissione o la naturale scadenza del contratto d'uso. Gli account gestiti dal cliente sono completamente gestiti da questo che ne regola in toto il ciclo di vita.	Alla chisura di un account il CSP, in conformità della ISO 27001 (ed estensioni) nonché qualificazione agid, ne elimina i dati di riferimento, le risorse potrebbero essere mantenute per un periodo di tempo, specifico per-csp, prima di essere eliminate.
Nuovi rischi considerati per erogazione servizio cloud (controllo 27018 5.1.1)	I rischi sono legati agli applicativi maggiormente esposti ad attacchi esterni essendo pubblicati sulla rete. SI.net ha deciso di mitigare questo rischio applicando nei livelli di firewall strette regole per l'utilizzo di un numero estremamente limitato di porte da/verso l'esterno abilitate laddove possibile alla comunicazione da/verso specifici indirizzi. Su alcuni progetti potrebbero essere attivi strumenti avanzati di monitoraggio intelligente della comunicazione, del comportamento delle risorse, della conformità alla politica di sicurezza o della privacy dei dati.	I rischi sono legati agli applicativi maggiormente esposti ad attacchi esterni essendo pubblicati sulla rete. SI.net ha deciso di mitigare questo rischio applicando nei livelli di firewall strette regole per l'utilizzo di un numero estremamente limitato di porte da/verso l'esterno abilitate laddove possibile alla comunicazione da/verso specifici indirizzi. Su alcuni progetti potrebbero essere attivi strumenti avanzati di monitoraggio intelligente della comunicazione, del comportamento delle risorse, della conformità alla politica di sicurezza o della privacy dei dati.	I maggiori rischi individuati sono legati agli applicativi maggiormente esposti ad attacchi esterni essendo pubblicati sulla rete. SI.net ha deciso di mitigare questo rischio applicando nei livelli di firewall strette regole per l'utilizzo di un numero estremamente limitato di porte da/verso l'esterno abilitate laddove possibile alla comunicazione da/verso specifici indirizzi. Su alcuni progetti potrebbero essere attivi strumenti avanzati di monitoraggio intelligente della comunicazione, del comportamento delle risorse, della conformità alla politica di sicurezza o della privacy dei dati.	I maggiori rischi individuati sono legati agli applicativi maggiormente esposti ad attacchi esterni essendo pubblicati sulla rete. SI.net ha deciso di mitigare questo rischio applicando nei livelli di firewall strette regole per l'utilizzo di un numero estremamente limitato di porte da/verso l'esterno abilitate laddove possibile alla comunicazione da/verso specifici indirizzi. Su alcuni progetti potrebbero essere attivi strumenti avanzati di monitoraggio intelligente della comunicazione, del comportamento delle risorse, della conformità alla politica di sicurezza o della privacy dei dati.	Le certificazioni ISO (ed eventuali altri standard internazionali) garantiscono la presa di coscienza da parte dei CSP verso tutte le problematiche, le procedure e gli interventi operativi necessari a garantire la sicurezza di dati e strutture erogate.
Ruoli e responsabilità in termini di accountability in fase contrattuale (controllo 27017 6.1.1)	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Le divisioni di responsabilità sono specificate nei termini di conformità dei CSP di riferimento che genericamente adottano le stesse regole di condivisione per-paradigmi che Si.net riflette verso i propri clienti. La responsabilità condivisa è riportata anche in diversi punti del documento di Politica di sicurezza.
A che livello si ferma la responsabilità dell'informazione da parte del provider e a che livello subentra quella del customer (controllo 27017 6.1.1)	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Si.net adotta una politica di presa di responsabilità basata sul principio della condivisione, il dettaglio sulla suddivisione dei compiti è riportata nel contratto di servizio.	Le divisioni di responsabilità sono specificate nei termini di conformità dei CSP di riferimento che genericamente adottano le stesse regole di condivisione per-paradigmi che Si.net riflette verso i propri clienti. La responsabilità condivisa è riportata anche in diversi punti del documento di Politica di sicurezza.

Modalità di accesso all'infrastruttura/piattaforma/servizio da parte di entrambe le parti, permessi e visibilità (controllo 27001 6.1.2)	Nel paradigma Saas, Si.net non accede mai ai dati presenti nei software se non in accordo con il cliente o in caso di richieste di assistenza tramite sistema di ticketing. In caso sia necessaria questa attività, Si.net utilizzerà gli account nominativi del proprio personale che verranno gestiti secondo la politica sulla sicurezza e accedendo al minor numero possibile di dati, il cliente può specificare nella sua richiesta di assistenza di voler monitorare l'attività di supporto per garantire l'operato dei tecnici Si.net. Come da specifiche dei punti precedenti ad esclusione del livello applicativo Si.net ha libero ed esclusivo accesso a tutti i livelli sottostanti per le normali operazioni di manutenzione ed evoluzione dei prodotti.	Nel paradigma Saas, Si.net non accede mai ai dati presenti nei software se non in accordo con il cliente o in caso di richieste di assistenza tramite sistema di ticketing. In caso sia necessaria questa attività, Si.net utilizzerà gli account nominativi del proprio personale che verranno gestiti secondo la politica sulla sicurezza e accedendo al minor numero possibile di dati, il cliente può specificare nella sua richiesta di assistenza di voler monitorare l'attività di supporto per garantire l'operato dei tecnici Si.net. Come da specifiche dei punti precedenti ad esclusione del livello applicativo Si.net ha libero ed esclusivo accesso a tutti i livelli sottostanti per le normali operazioni di manutenzione ed evoluzione dei prodotti.	Nel paradigma Paas, Si.net non oltrepassa mai il livello operativo della piattaforma, può accede a questo solo se in accordo con il cliente o in caso di richieste di assistenza tramite sistema di ticketing. In caso sia necessaria questa attività, Si.net utilizzerà gli account del proprio personale che verranno gestiti secondo la politica sulla sicurezza e accedendo al minor numero possibile di dati, il cliente può specificare nella sua richiesta di assistenza di voler monitorare l'attività di supporto per garantire l'operato dei tecnici Si.net. Come da specifiche dei punti precedenti, nei livelli sottostanti a quello di operatività della piattaforma Si.net ha libero ed esclusivo accesso per le normali operazioni di manutenzione ed evoluzione dei prodotti. Si.net ha accesso libero, per operazioni di manutenzione ed evoluzione, anche al livello di piattaforma, in caso di ambiente managed.	Nel paradigma Iaas, Si.net non oltrepassa mai il livello di virtualizzazione, può accede a questo solo se non in accordo con il cliente o in caso di richieste di assistenza tramite sistema di ticketing. In caso sia necessaria questa attività, Si.net utilizzerà gli account del proprio personale che verranno gestiti secondo la politica sulla sicurezza e accedendo al minor numero possibile di dati, il cliente può specificare nella sua richiesta di assistenza di voler monitorare l'attività di supporto per garantire l'operato dei tecnici Si.net. Come da specifiche dei punti precedenti, nei livelli di virtualizzazione e fisico Si.net ha libero ed esclusivo accesso per le normali operazioni di manutenzione ed evoluzione dei prodotti. Si.net ha accesso libero, per operazioni di manutenzione ed evoluzione, anche al livello di infrastruttura, in caso di ambiente managed.	L'accesso ai servizi e ai dati di Si.net è regolamentato contrattualmente verso ogni CSP che opera nei limiti del pradigma del prodotto interessato sempre secondo normative ISO certificate. (es. 3.2 Contratto AWS)
Localizzazione geografica dei dati (controllo 27017 6.1.3)	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I CSP offrono diverse location geografiche per l'utilizzo dei servizi offerti, il CSP garantisce che tutti i servizi erogati all'interno delle regioni utilizzate da Si.net e specificate all'interno della Politica di sicurezza siano conformi al GDPR e alle certificazioni ISO 27001, 27017 e 27018.
Descrizione funzionalità attraverso cui viene messa a disposizione al customer la gestione di ruoli e responsabilità di utilizzo e di sicurezza delle informazioni, attraverso documentazione tecnica e SLA (controllo 27017 CLD.6.3.1)	Il cliente gestisce in maniera indipendente e completa tutti gli aspetti di gestione di utenze, ruoli, permessi, gruppi, autenticazioni ed autorizzazioni relativi all'applicativo (questa terminologia può variare a seconda del software); Si.net mantiene solitamente uno o più account amministrativi nominali per le operazioni di supporto ed assistenza, il cliente può comunque decidere di eliminare o disabilitare questi utenti o di creane di nuovi all'occorrenza.	Il cliente gestisce in maniera indipendente e completa tutti gli aspetti di gestione di utenze, ruoli, permessi, gruppi, autenticazioni ed autorizzazioni relativi all'applicativo (questa terminologia può variare a seconda del software); Si.net mantiene solitamente uno o più account amministrativi nominali per le operazioni di supporto ed assistenza, il cliente può comunque decidere di eliminare o disabilitare questi utenti o di creane di nuovi all'occorrenza.	Il cliente gestisce in maniera indipendente e completa tutti gli aspetti di gestione di utenze, ruoli, permessi, gruppi, autenticazioni ed autorizzazioni relativi all'applicativo (questa terminologia può variare a seconda del software); Si.net mantiene solitamente uno o più account amministrativi nominali per le operazioni di supporto ed assistenza, il cliente può comunque decidere di eliminare o disabilitare questi utenti o di creane di nuovi all'occorrenza.	Il cliente gestisce in maniera indipendente e completa tutti gli aspetti di gestione di utenze, ruoli, permessi, gruppi, autenticazioni ed autorizzazioni relativi all'applicativo (questa terminologia può variare a seconda del software); Si.net mantiene solitamente uno o più account amministrativi nominali per le operazioni di supporto ed assistenza, il cliente può comunque decidere di eliminare o disabilitare questi utenti o di creane di nuovi all'occorrenza. Come descritto nelle politiche di sicurezza l'accesso root all'account non viene mai fornito al cliente (viene comunque tracciato il suo utilizzo).	I CSP mettono a disposizione di Si.net strumenti specifici per il controllo di tutto l'aspetto di sicurezza, autorizzazione ed autenticazione, verso le interfacce applicative ed i servizi offerti.
Descrizione dell'end of service (controllo 27017 CLD 8.1.5)	Su richiesta del cliente o alla risoluzione/scadenza del contratto Si.net provvederà alla cancellazione definitiva di ogni contenuto e/o struttura del cliente senza conservarne copia. Verrà consegnata al cliente la lista degli asset e account eliminati.	Su richiesta del cliente o alla risoluzione/scadenza del contratto Si.net provvederà alla cancellazione definitiva di ogni contenuto e/o struttura del cliente senza conservarne copia. Verrà consegnata al cliente la lista degli asset e account eliminati. Diversamente, se contrattualmente concordato il servizio, potrebbe essere sganciato da tutti i riferimento Si.net e consegnato al cliente per suo esclusivo utilizzo.	Su richiesta del cliente o alla risoluzione/scadenza del contratto Si.net provvederà alla cancellazione definitiva di ogni contenuto e/o struttura del cliente senza conservarne copia. Verrà consegnata al cliente la lista degli asset e account eliminati. Diversamente, se contrattualmente concordato il servizio, potrebbe essere sganciato da tutti i riferimento Si.net e consegnato al cliente per suo esclusivo utilizzo.	Su richiesta del cliente o alla risoluzione/scadenza del contratto Si.net provvederà alla cancellazione definitiva di ogni contenuto e/o struttura del cliente senza conservarne copia. Verrà consegnata al cliente la lista degli asset e account eliminati. Diversamente, se contrattualmente concordato il servizio, potrebbe essere sganciato da tutti i riferimento Si.net e consegnato al cliente per suo esclusivo utilizzo.	Nonostante la conformità alle normative ISO garantisca a Si.net piena sicurezza della validità delle procedure di end-of-service messe in opera dal CSP, Si.net si impegna ad eliminare preventivamente rispetto al termine del servizio ogni contenuto e/o struttura ospitata presso il CSP.
Modalità messe a disposizione del cliente per la classificazione delle informazioni (controllo 27017 8.2.2)	Diversi applicativi possono adottare diversi metodi di classificazione a seconda del target del software stesso; In caso venga messo a disposizione un sistema di raccolta dei dati dagli utenti finali il sistema permetterà la precisa configurazione di queste raccolte per permettere al cliente di creare input precisi e limitati, dove non specificato e/o non specificabile i dati raccolti sono sempre considerati e da considerare riservati.	Diversi applicativi possono adottare diversi metodi di classificazione a seconda del target del software stesso; In caso venga messo a disposizione un sistema di raccolta dei dati dagli utenti finali il sistema permetterà la precisa configurazione di queste raccolte per permettere al cliente di creare input precisi e limitati, dove non specificato e/o non specificabile i dati raccolti sono sempre considerati e da considerare riservati.	Diverse piattaforme possono adottare diversi strumenti di classificazione a seconda del target della piattaforma stessa; In generale dove non sono disponibili sistemi di tagging, vengono messi a disposizione del cliente vari strumenti per la messa in sicurezza che il cliente può decidere se adottare (o meno) anche in maniera cumulativa in base ad una propria classificazione; Quando questi strumenti non vengono messi a disposizione tutte le informazioni sono trattate come riservate.	Diverse infrastrutture possono adottare diversi strumenti di classificazione a seconda del target dell' infrastruttura stessa; In generale dove non sono disponibili sistemi di tagging, vengono messi a disposizione del cliente vari strumenti per la messa in sicurezza che il cliente può decidere se adottare (o meno) anche in maniera cumulativa in base ad una propria classificazione; Quando questi strumenti non vengono messi a disposizione tutte le informazioni sono trattate come riservate.	I CSP offrono all'interno del loro catalogo sistemi di tagging e/o strumenti di automazione adatti alla classificazione delle informazioni e all'applicazione di regole di conformità e sicurezza comuni. Dove questi sistemi non sono resi disponibili tutte le informazioni saranno generate e trattate come riservate.
Modalità di gestione dei diritti di accesso per i propri end-user sotto forma di documento di progetto, dettagliando le modalità di creazione utenze, come definirne ruoli e responsabilità, i protocolli per l'accesso sicuro utilizzati. (controllo 27017 9.2.1)	Al momento dell'attivazione dell'istanza al cliente viene formalmente consegnato un profilo di amministrazione con il quale è in grado di creare e gestire tutte le utenze (ed eventuali altri oggetti di autorizzazione quali ad esempio i gruppi) ed i relativi permessi, la documentazione dell'applicativo spiega poi l'utilizzo dello strumento e la sua amministrazione.	Al momento dell'attivazione dell'istanza al cliente viene formalmente consegnato un profilo di amministrazione con il quale è in grado di creare e gestire tutte le utenze (ed eventuali altri oggetti di autorizzazione quali ad esempio i gruppi) ed i relativi permessi, la documentazione dell'applicativo spiega poi l'utilizzo dello strumento e la sua amministrazione.	A seconda della piattaforma al cliente possono essere formalmente fornite una o più credenziali di autenticazione tali da permettere l'operatività e/o la gestione di ulteriori utenze. Nei casi in cui la gestione di ulteriori utenze non sia disponibile per il cliente questo può richiedere variazioni del sistema di autenticazione/autorizzazione tramite ticket di supporto.	A seconda dell'infrastruttura al cliente possono essere formalmente fornite una o più credenziali di autenticazione tali da permettere l'operatività e/o la gestione di ulteriori utenze. Nei casi in cui la gestione di ulteriori utenze non sia disponibile per il cliente questo può richiedere variazioni del sistema di autenticazione/autorizzazione tramite ticket di supporto.	I CSP dichiarano le modalità di accesso e descrivono i loro sistemi di sicurezza all'interno della documentazione specifica, tali strumenti sono quelli utilizzati da Si.net per la creazione delle proprie utenze e, nel caso, per quelle dei relativi clienti. Tali strumenti permettono una gestione completa degli accessi in conformità alle certificazioni ISO del CSP.

Il provider deve comunicare al customer fruitore del servizio gli strumenti forniti per l'amministrazione dell'autenticazione, e informarlo riguardo alla possibilità di installare tool di terze parti per la fruizione di capabilities di autenticazione (controllo 27017 9.2.3)**. Le informazioni sulle procedure di autenticazione sicura valgono non solo per IAAS/PAAS ma anche per l'application software erogato in modalità SAAS dall'Organizzazione.** (controllo 27018 9.2.4)	In fase di attivazione e/o di formazione sull'applicativo al cliente vengono spiegati tutti i sistemi e gli strumenti utili all'amministrazione delle funzionalità di autenticazione compresi sistemi di federazione (SPID, CIE, TS-CNS) e/o di integrazione (Active Directory, SSO, Entra) se disponibili per lo specifico software. Si.net non permette, se non specificato diversamente in sede contrattuale, l'installazione di strumenti terzi non validati direttamente per i meccanismi di autenticazione ed autorizzazione in ambiente cloud.	In fase di attivazione e/o di formazione sull'applicativo al cliente vengono spiegati tutti i sistemi e gli strumenti utili all'amministrazione delle funzionalità di autenticazione compresi sistemi di federazione (SPID, CIE, TS-CNS) e/o di integrazione (Active Directory, SSO, Entra) se disponibili per lo specifico software. Si.net non permette, se non specificato diversamente in sede contrattuale, l'installazione di strumenti terzi non validati direttamente per i meccanismi di autenticazione ed autorizzazione in ambiente cloud.	Laddove gestibili dal cliente, in fase di attivazione e/o di formazione sulla piattaforma, vengono spiegati al cliente tutti i sistemi e gli strumenti utili all'amministrazione delle funzionalità di autenticazione compresi sistemi di federazione (SPID, CNS, ...) e/o di integrazione (Active Directory, ...) se disponibili per la specifica soluzione. Si.net non permette, se non specificato diversamente in sede contrattuale, l'installazione di strumenti terzi non validati direttamente per i meccanismi di autenticazione ed autorizzazione in ambiente cloud.	Laddove gestibili dal cliente, in fase di attivazione e/o di formazione sull'infrastruttura, vengono spiegati al cliente tutti i sistemi e gli strumenti utili all'amministrazione delle funzionalità di autenticazione compresi sistemi di federazione (SPID, CNS, ...) e/o di integrazione (Active Directory, ...) se disponibili per la specifica soluzione. Si.net non permette, se non specificato diversamente in sede contrattuale, l'installazione di strumenti terzi non validati direttamente per i meccanismi di autenticazione ed autorizzazione in ambiente cloud.	I CSP dichiarano le modalità di accesso e descrivono i loro sistemi di sicurezza all'interno della documentazione specifica, tali strumenti sono quelli utilizzati da Si.net per la creazione delle proprie utenze e, nel caso, per quelle dei relativi clienti. Tali strumenti permettono una gestione completa degli accessi in conformità alle certificazioni ISO del CSP.
L'**erogatore di servizi IAAS/PAAS deve mettere a disposizione del customer strumenti per la gestione della regolazione degli accessi permettendone il restringimento agli autorizzati per quanto riguarda i servizi, le funzioni e i dati conservati nel servizio. Per quanto riguarda il SAAS è gestito dall'application software a fronte di requisiti concordati con il cliente**. (controllo 27017 9.4.1)	All'interno dei servizi Saas Si.net mette sempre a disposizione strumenti di gestione degli accessi e delle relative permission, tali strumenti sono introdotti e descritti al cliente tramite documentazione e/o attività di formazione.	All'interno dei servizi Saas Si.net mette sempre a disposizione strumenti di gestione degli accessi e delle relative permission, tali strumenti sono introdotti e descritti al cliente tramite documentazione e/o attività di formazione.	Nella maggior parte dei casi i servizi offerti sono dotati di sistemi autonomi di gestione delle utenze completamente amministrabili dal cliente. Dove Si.net non mette a disposizione strumenti specifici per la gestione degli accessi da parte del cliente questo può avvalersi del sistema di ticketing per qualsiasi variazione relativa ad autenticazione ed autorizzazione delle utenze. Si.net provvederà, in conformità alla politica di sicurezza, alle variazioni necessarie dando riscontro al cliente.	Nella maggior parte dei casi i servizi offerti sono dotati di sistemi autonomi di gestione delle utenze completamente amministrabili dal cliente. Dove Si.net non mette a disposizione strumenti specifici per la gestione degli accessi da parte del cliente questo può avvalersi del sistema di ticketing per qualsiasi variazione relativa ad autenticazione ed autorizzazione delle utenze. Si.net provvederà, in conformità alla politica di sicurezza, alle variazioni necessarie dando riscontro al cliente.	I CSP dichiarano le modalità di accesso e descrivono i loro sistemi di sicurezza all'interno della documentazione specifica, tali strumenti sono quelli utilizzati da Si.net per la creazione delle proprie utenze e, nel caso, per quelle dei relativi clienti. Tali strumenti permettono una gestione completa degli accessi in conformità alle certificazioni ISO del CSP.
Il provider deve concordare con il customer gli applicativi software che è possibile installare all'interno dell'ambiente fornito, comunicando quelli vietati e/o di cui l'installazione non è tecnicamente effettuabile per vincoli infrastrutturali o di piattaforma. (controllo 27018 9.4.4)	Se non specificato diversamente in fase contrattuale l'installazione di software aggiuntivo all'interno di un prodotto Saas è proibita tecnicamente o, laddove non possibile, fortemente sconsigliata. Si.net deve comunque essere posta a conoscenza della volontà di installazione di componenti software aggiuntive che devono essere approvate preventivamente.	Il cliente può installare sulla piattaforma qualsiasi software rispetti le norme di uso accettabile dei servizi e non possa inficiare/ponga pericoli per la sicurezza dei dati, della piattaforma, dei livelli operativi sottostanti, delle specifiche contrattuali o di Si.net. In caso di software particolarmente gravoso in termini di performance o potenzialmente pericoloso in termini di sicurezza il cliente è invitato ma non obbligato a richiedere l'affiancamento di un tecnico Si.net per l'ottimizzazione e la messa in sicurezza.	Il cliente può installare sulla piattaforma qualsiasi software rispetti le norme di uso accettabile dei servizi e non possa inficiare/ponga pericoli per la sicurezza dei dati, della piattaforma, dei livelli operativi sottostanti, delle specifiche contrattuali o di Si.net. In caso di software particolarmente gravoso in termini di performance o potenzialmente pericoloso in termini di sicurezza il cliente è invitato ma non obbligato a richiedere l'affiancamento di un tecnico Si.net per l'ottimizzazione e la messa in sicurezza.	Il cliente può installare sull'infrastruttura qualsiasi software rispetti le norme di uso accettabile dei servizi e non possa inficiare/ponga pericoli per la sicurezza dei dati, della piattaforma, dei livelli operativi sottostanti, delle specifiche contrattuali o di Si.net. In caso di software particolarmente gravoso in termini di performance o potenzialmente pericoloso in termini di sicurezza il cliente è invitato ma non obbligato a richiedere l'affiancamento di un tecnico Si.net per l'ottimizzazione e la messa in sicurezza.	Ogni CSP include nel contratto con Si.net una normativa di uso accettabile nella quale vengono dichiarate le attività lecite operabili sulle risorse messe a disposizione. Si.net riflette tali norme in maniera eguale o maggiormente restrittiva sui propri clienti. Laddove il CSP non alleghi una normativa di quel tipo Si.net applicherà la propria normativa a sè stessa.
Il Provider deve garantire la segregazione "logica" degli ambienti tra i diversi customer mediante soluzioni virtuali. Gli amministratori di sistema interni devono essere differenti da quelli per i singoli clienti. (controllo 27017 CLD.9.5.1)	I prodotti Saas sono sempre forniti in ambienti multi-tenant o multi-istanza costruiti appositamente per l'isolamento logico delle varie soluzioni anche dovessero corrispondere allo stesso cliente. Gli amministratori del sistema sottostante l'erogazione Saas utilizzano strumenti, profili e permessi totalmente differenti rispetto a quelli applicativi dei clienti.	I prodotti Saas sono sempre forniti in ambienti multi-tenant o multi-istanza costruiti appositamente per l'isolamento logico delle varie soluzioni anche dovessero corrispondere allo stesso cliente. Gli amministratori del sistema sottostante l'erogazione Saas utilizzano strumenti, profili e permessi totalmente differenti rispetto a quelli applicativi dei clienti.	I prodotti Paas sono sempre forniti in ambienti costruiti appositamente per l'isolamento logico delle varie soluzioni; In alcuni casi, in accordo con il cliente, due o più prodotti possono raggiungersi sul network per garantire capacità di distribuzione di ruoli, compiti e/o carichi di lavoro. Gli amministratori del sistema sottostante l'erogazione Paas utilizzano strumenti, profili e permessi totalmente differenti rispetto a quelli applicativi dei clienti.	I prodotti Iaas sono sempre forniti in ambienti costruiti appositamente per l'isolamento logico delle varie soluzioni anche dovessero corrispondere allo stesso cliente; In alcuni casi, in accordo con il cliente, due o più prodotti possono raggiungersi sul network per garantire capacità di distribuzione di ruoli, compiti e/o carichi di lavoro, per prodotti Iaas evoluti potrebbe essere messa a disposizione del cliente stesso la capacità di gestione del network sottoforma di VPC. Gli amministratori del sistema sottostante l'erogazione Iaas utilizzano strumenti, profili e permessi totalmente differenti rispetto a quelli applicativi dei clienti.	L'isolamento logico per-customer è garantito dal CSP in conformità alla relativa ISO 27017 obbligatoria per la collaborazione con Si.net.

Provider e customer devono sincerarsi che la configurazione delle macchine virtuali segua regole di sicurezza con la predisposizione di adeguate misure tecniche (anti-malware, logging..) e minimizzazione dei servizi attivi (need based) (controllo 27017 9.5.2)	La configurazione dell'infrastruttura virtuale sottostante il livello applicativo è completamente gestita da Si.net in conformità con quanto dichiarato nella politica di sicurezza e richiesto dal controllo ISO.	La configurazione dell'infrastruttura virtuale sottostante il livello applicativo è completamente gestita da Si.net in conformità con quanto dichiarato nella politica di sicurezza e richiesto dal controllo ISO.	La configurazione dell'infrastruttura virtuale sottostante il livello di piattaforma è completamente gestita da Si.net in conformità con quanto dichiarato nella politica di sicurezza e richiesto dal controllo ISO.	Si.net monitora a livello di hypervisor e API le richieste di risorse per ogni servizio in uso valutando eventuali anomalie con il cliente. Si.net può inoltre applicare alle risorse messe a disposizione del cliente strumenti automatizzati per la verifica della conformità (in tutti i suoi aspetti) alle norme previste e per l'analisi di difformità tra l'utilizzo effettivo e le regole di uso accettabile. In accordo col cliente o se specificato contrattualmente Si.net potrebbe installare sulle istanze di calcolo agenti per la rilevazione o la gestione remota di aspetti di sicurezza, performance, supporto o conformità. Per motivi di compliance Si.net, in accordo ed in affiancamento col cliente, potrebbe eseguire audit di sicurezza su una o più risorse per garantirne la corrispondenza rispetto alle modalità d'uso concordate. Il cliente può in qualunque momento verificare e comunicare tramite ticket a Si.net eventuali problematiche riscontrate. La baseline di configurazione è disponibile nell'omonimo documento.	Il fornitore mette a disposizione di Si.net tutti gli strumenti necessari all'hardening delle VM e ne consiglia i metodi di utilizzo attraverso la documentazione; Si.net sfrutta questi strumenti come da Politiche di sicurezza e secondo il principio del least privilege per garantire il massimo livello di sicurezza possibile in linea con lo scopo della VM stessa. In caso di violazione dei termini contrattuali di uso accettabile i CSP potrebbero effettuare verifiche e/o sospesioni dei servizi per preservare l'operatività dell'infrastruttura.
L'erogatore di servizi IAAS/PAAS/SAAS deve fornire al customer in fase di documentazione tecnica informazioni riguardo alle tecniche di crittografia e pseudonimizzazione utilizzate per proteggere le informazioni, in linea con le linee guida aziendali di disclosure e in accordo alla normativa vigente in materia (GDPR). Nel caso di IAAS/PAAS in fase contrattuale e di documentazione tecnica viene comunicato al customer l'insieme di strumenti messi a disposizione per la predisposizione di una propria protezione crittografica. (controllo 27017 10.1.1)	Per ogni servizio Saas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Per ogni servizio Saas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Per ogni servizio Paas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Per ogni servizio Iaas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Il fornitore descrive nella propria documentazione tecnica tutte le soluzioni e le modalità d'uso degli strumenti di crittografia e pseudonimizzazione che rende disponibili a Si.net. In base all'analisi dei possibili rischi per il servizio SaaS vengono attiviati sistemi crittografici a livello applicativo.
L'erogatore di servizi IAAS/PAAS/SAAS deve fornire al customer informazioni riguardo alle tecniche di crittografia e pseudonimizzazione utilizzate per proteggere le sue informazioni in linea con le linee guida aziendali di disclosure e in accordo alla normativa vigente in materia (GDPR). Nel caso di IAAS/PAAS in fase contrattuale e di documentazione tecnica viene comunicato al customer l'insieme di strumenti messi a disposizione per la predisposizione di una propria protezione crittografica. (controllo 27018 10.1.1)	Per ogni servizio Saas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Per ogni servizio Saas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Per ogni servizio Paas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Per ogni servizio Iaas erogato Si.net mette a disposizione, nella documentazione tecnica tutte le informazioni riguardanti componenti e funzionalità pre-attivate o attivabili nel contesto di crittografia e pseudonimizzazione.	Il fornitore descrive nella propria documentazione tecnica tutte le soluzioni e le modalità d'uso degli strumenti di crittografia e pseudonimizzazione che rende disponibili a Si.net. In base all'analisi dei possibili rischi per il servizio SaaS vengono attiviati sistemi crittografici a livello applicativo.
Il provider deve monitorare l'utilizzo delle risorse fornite al customer e intervenire in termini di sicurezza per la dismissione e il riutilizzo. Le misure che deve implementare e/o rendere fruibili all'utilizzatore all'interno dell'infrastruttura erogata sono:] **- utilizzo di sicurezza a livello di trasporto (Ipsec/TLS) per tutte le transazioni** **- registrazione sicura e autenticazione con strong password per accedere ai dati** **- in caso di multi-tenancy fornire appropriata separazione tra i differenti tenant, inaccessibili l'uno dall'altro per i rispettivi user** **- in caso di virtualizzazione garantire la disponibilità dell'informazione partendo dai requisiti dell'applicazione.** (controllo 27017 12.2.7)	Si.net eroga tutti i suoi servizi Saas in conformità a quanto richiesto, in particolare: Tutte le transazioni sono di tipo TLS con crittografia RSA (se non specificato diversamente) con chiave PKCS #1 di tipo SHA-256 a 128 bit, rilasciate dalla Certificate Authority open Let's Encrypt. La registrazione di nuovi utenti avviene con metodi che implementano un alto grado di sicurezza quali ad esempio SPID di livello 2 (nome utente e password + OTP) o CIE (dispositivo + supporto fisico + PIN). In caso di creazione manuale di utenti viene sempre indicata la robustezza della password e, a seconda del servizio, potrebbe essere reso obbligatorio l'utilizzo di password di tipo strong. La gestione della multi-tenancy avviene in maniera completamente isolata per singola istanza, non sono attualmente disponibili servizi Saas che implementano concetti di virtualizzazione.	Per l'erogazione dei servizi Saas esterni Si.net riflette la conformità a quest'obbligo dei CSP ai propri clienti sfruttando la necessità del CSP di avere certificazione ISO corrispondente per la collaborazione con Si.net. Per le configurazioni a livello di piattaforma gestite direttamente da Si.net, implementiamo le configurazioni indicate in questo documento o nella Politica di sicurezza, in maniera conforme a quanto richiesto.	Per l'erogazione dei servizi Paas Si.net riflette la conformità a quest'obbligo dei CSP ai propri clienti sfruttando la necessità del CSP di avere certificazione ISO corrispondente per la collaborazione con Si.net. Per le configurazioni a livello di piattaforma gestite direttamente da Si.net, implementiamo le configurazioni indicate in questo documento o nella Politica di sicurezza, in maniera conforme a quanto richiesto.	Per l'erogazione dei servizi Iaas Si.net riflette la conformità a quest'obbligo dei CSP ai propri clienti sfruttando la necessità del CSP di avere certificazione ISO corrispondente per la collaborazione con Si.net. Per le configurazioni a livello di infrastruttura gestite direttamente da Si.net, implementiamo le configurazioni indicate in questo documento o nella Politica di sicurezza, in maniera conforme a quanto richiesto.	Tutti i CSP che collaborano con Si.net danno evidenza della conformità a questi requisiti estremamente tecnici tramite la corrispondente certificazione ISO e/o la disponibilità di servizi ad-hoc.

Effettuare una Data Protection Impact Analysis per identificare i rischi sui dispositivi di storage contenenti dati personali e le modalità per dismetterli in modo sicuro. (controllo 27018 12.2.7)	I dispositivi di storage sono gestiti dai CSP attraverso i servizi di storage messi a disposizione, la loro gestione ricade sotto ISO 27018. Si.net riflette la conformità a questo controllo sui propri clienti.	I dispositivi di storage sono gestiti dai CSP attraverso i servizi di storage messi a disposizione, la loro gestione ricade sotto ISO 27018. Si.net riflette la conformità a questo controllo sui propri clienti.	I dispositivi di storage sono gestiti dai CSP attraverso i servizi di storage messi a disposizione, la loro gestione ricade sotto ISO 27018. Si.net riflette la conformità a questo controllo sui propri clienti.	I dispositivi di storage sono gestiti dai CSP attraverso i servizi di storage messi a disposizione, la loro gestione ricade sotto ISO 27018. Si.net riflette la conformità a questo controllo sui propri clienti.	Tutti i CSP che collaborano con Si.net danno evidenza della conformità a questo requisito tramite la corrispondente certificazione ISO e al GDPR.
Il provider deve avvisare per tempo il customer dei change che sono in procinto di essere applicati sull'infrastruttura/piattaforma/servizio, nella modalità concordata contrattualmente (ticket, mail, ecc.). Informazioni descrittive sono la categoria di change, la pianificazione (data, ora e durata), la descrizione tecnica del change, la notifica di inizio e fine dell'intervento. (controllo 27017 12.1.2)	Il processo di change dell'applicativo per aggiornamenti con cambi di funzionalità dello stesso viene valutato da SI.net, viene applicato su ambienti di sviluppo e di test e viene comunicata al cliente tramite i riferimenti indicati nei documenti di commessa prima della sua installazione.	Il processo di change della piattaforma viene valutato in primo luogo da Si.net in coordinamento col CSP, in caso di necessità di intervento, dopo valutazioni interne sulla fattibilità, economica ed infrastrutturale, della modifica, questa viene comunicata al cliente tramite ticket o canali appositi.	Il processo di change della piattaforma viene valutato in primo luogo da Si.net in coordinamento col CSP, in caso di necessità di intervento, dopo valutazioni interne sulla fattibilità, economica ed infrastrutturale, della modifica, questa viene comunicata al cliente tramite ticket o canali appositi.	Il processo di change dell'infrastruttura viene valutato in primo luogo da Si.net in coordinamento col CSP, in caso di necessità di intervento, dopo valutazioni interne sulla fattibilità, economica ed infrastrutturale, della modifica, questa viene comunicata al cliente tramite ticket o canali appositi.	I CSP comunicano per tempo eventuali change ai servizi erogati tramite diversi strumenti di comunicazione quali Mail, Newsletter, avvisi nelle console di gestione e notifiche push. L'obbligo di notifica in caso di change dei servizi è imposto dalla relativa certificazione ISO.
Fornire al customer informazioni riguardo ai vincoli di capacity, come ad esempio numero di core per applicazione, quantità di storage disponibile, ampiezza di banda di rete disponibile, sotto forma di SLA. Rendergli fruibile il monitoraggio delle risorse utilizzate tramite statistiche periodiche, come statistiche per intervalli di tempo precisi, o massimo livello di utilizzo delle risorse. (controllo 27017 CLD 12.1.5)	Si.net non permette ai clienti dei servizi Saas di accedere a strumenti di monitoraggio diretti sui livelli sottostanti quello applicativo ma, a seconda del software, il cliente può richiedere in ogni momento dati di utilizzo delle risorse tramite ticket. I limiti di capacity per istanza sono definiti contrattualmente con il cliente.	Si.net non permette ai clienti dei servizi Saas di accedere a strumenti di monitoraggio diretti sui livelli sottostanti quello applicativo ma, a seconda del software, il cliente può richiedere in ogni momento dati di utilizzo delle risorse tramite ticket. I limiti di capacity per istanza sono definiti contrattualmente con il cliente.	Si.net non permette ai clienti dei servizi Paas di accedere a strumenti di monitoraggio diretti sui livelli sottostanti quello della piattaforma ma, a seconda della piattaforma, il cliente può richiedere in ogni momento dati di utilizzo delle risorse tramite ticket. I limiti di capacity per istanza sono definiti contrattualmente con il cliente.	Il cliente può utilizzare qualsiasi strumento, nativo (dove presente) o di terze parti (se rispetta le norme di uso accettabile) per monitorare l'utilizzo di qualsiasi risorsa istanzianta all'interno del suo account. I limiti di capacity per istanza sono definiti contrattualmente con il cliente. In caso di ambiente managed al cliente vengono comunque dati accessi sufficienti all'utilizzo dei servizi di reportistica o la possibilità di richiedere questi dati tramite ticket.	All'interno della documentazione tecnica i CSP descrivono soft e hard limits per ogni servizio, mettono inoltre a disposizione strumenti di monitoraggio pianificato o continuo per permettere a Si.net di verificare l'occupazione delle risorse in uso.
In generale le responsabilità del backup vanno concordate con il customer. Generalmente il provider IAAS deve garantire che a livello infrastrutturale vengano effettuati backup con le seguenti specifiche definite: - ambito e scheduling - metodo e formato del dato, inclusa crittografia, se considerato rilevante - periodo di retention - procedure per verificare l'integrità dei dati di backup - procedure e coordinate temporali rilevanti riguardo alle modalità di restoring dei dati dal backup - location del backup oltre a fornire accesso sicuro al backup al customer. Nel caso del IAAS sono da definire le responsabilità tra customer e provider riguardo al backup, come nel caso di file eseguibili prodotti dagli strumenti di sviluppo messi a disposizione dal provider sulla piattaforma. Nel caso del SAAS sono da definire le responsabilità tra customer e provider riguardo al backup; a seconda del servizio, il provider può mettere a disposizione strumenti di backup al customer, rimettendogli la responsabilità di utilizzarli per	Si.net mette a disposizione, nei propri servizi Saas, strumenti di esportazione ed importazione dei contenuti e delle strutture così da permettere il backup in qualunque momento da parte del cliente, in fase contrattuale inoltre vengono specificati i servizi di backup attivi con le specifiche richieste. La gestione dei backup, essendo svolta a livello più basso di quello applicativo, non è gestibile dal cliente che può richiedere in ogni momento un ripristino ad un punto di disponibilità precedente tramite ticket. La quantità e la periodicità dei punti di disponibilità viene definita in fase contrattuale.	Data la natura dei servizi Saas esterni il cliente può effettuare backup personali tramite gli strumenti di utilizzo della piattaforma (es. mysqldump per Paas RDBMS MySQL) in ogni momento, in fase contrattuale inoltre vengono specificati i servizi di backup attivi con le specifiche richieste.	Data la natura dei servizi Paas il cliente può effettuare backup personali tramite gli strumenti di utilizzo della piattaforma (es. mysqldump per Paas RDBMS MySQL) in ogni momento, in fase contrattuale inoltre vengono specificati i servizi di backup attivi con le specifiche richieste. In ambienti managed la gestione dei backup, essendo svolta a livello più basso di quello di piattaforma non è gestibile dal cliente che può richiedere in ogni momento un ripristino ad un punto di disponibilità precedente tramite ticket.	Data la natura dei servizi Iaas il cliente può effettuare backup personali tramite gli strumenti di gestione dell'infrastruttura in ogni momento, in fase contrattuale inoltre vengono specificati i servizi di backup attivi con le specifiche richieste. Si.net garantisce in ambienti managed la strutturazione, il monitoraggio e la manutenzione dei servizi di backup concordati con il cliente come specificato contrattualmente. In ambiente a gestione del cliente Si.net consiglia le modalità di utilizzo durante le sessioni formative ma non entra nel merito della messa in opera delle attività.	I CSP non offrono contrattualmente piani di backup predefiniti ma offrono soluzioni sotto forma di servizi per permettere ai clienti, come Si.net, di gestire secondo le proprie esigenze qualsivoglia tipologia di attività di backup e ripristino.
Quando il provider fornisce servizi di backup e restore al customer, deve fornire chiare informazioni al customer riguardo gli strumenti del servizio cloud rispetto a backup e restore e eventuali cancellazioni dei dati del cliente contenuti (SLA). Il provider deve implementare una procedura per effettuare operazioni di backup/restore in un periodo specificato e documentato dopo un incident a livello di documentazione e linee guida tecnico-operative. (controllo 27018 12.3.1)	Tutte le politiche di backup e restore implementate da Si.net per lo specifico applicativo sono documentate a livello contrattuale e contengono esplicitamente i periodi di ritenzione e rotazione dei dati.	Tutte le politiche di backup e restore implementate da Si.net per lo specifico applicativo sono documentate a livello contrattuale e contengono esplicitamente i periodi di ritenzione e rotazione dei dati.	Tutte le politiche di backup e restore implementate da Si.net per lo specifico applicativo sono documentate a livello contrattuale e contengono esplicitamente i periodi di ritenzione e rotazione dei dati.	Tutte le politiche di backup e restore implementate da Si.net per lo specifico applicativo sono documentate a livello contrattuale e contengono esplicitamente i periodi di ritenzione e rotazione dei dati.	I CSP forniscono strumenti avanzati di backup e restore e ne documentano l'utilizzo all'interno delle loro documentazioni. Internamente i provider garantiscono a Si.net la validità dei propri piani di ripristino in caso di incident tramite le apposite certificazioni ISO.

Le responsabilità di provider e customer variano da IAAS a PAAS a SAAS, in ordine crescente per il provider e decrescente per il customer, e definiti in fase contrattuale. Il provider deve fornire al customer all'interno del servizio messo a disposizione la possibilità di raccogliere log. (controllo 27018 12.4.1)	Tutti gli applicativi Saas rilasciati da Si.net implementano capacità di logging, più o meno avanzate, a cui il cliente può avere accesso nativo o su richiesta (via ticket).	Tutti gli applicativi Saas rilasciati da Si.net implementano capacità di logging, più o meno avanzate, a cui il cliente può avere accesso nativo o su richiesta (via ticket).	Tutti i servizi Paas rilasciati da Si.net implementano capacità di logging, più o meno avanzate, a cui il cliente può avere accesso nativo o su richiesta (via ticket).	Tutti i servizi Iaas rilasciati da Si.net implementano capacità di logging, più o meno avanzate, a cui il cliente può avere accesso nativo o su richiesta (via ticket).	Tutti i CSP garantiscono capacità di logging per i servizi messi a disposizione di Si.net attraverso specifiche risorse autonomamente consultabili.
Il provider deve definire linee guida interne per tenere sotto controllo se, quando e come le informazioni di log sono rese disponibili al customer; deve altresì verificare che quando il customer ha accesso a log abbia accesso solo ai propri. Il provider deve dotarsi di un processo per revisionare a intervalli regolari gli event log per identificare irregolarità e porvi rimedio, e inoltre registrare quando questi contengono dati personali e/o sensibili. (controllo 27018 12.4.1)	L'accesso alle informazioni di log, laddove non automatizzato da servizio (che rispetta nativamente i requisiti richiesti) viene reso disponibile, successivamente ad una richiesta via ticket, attraverso un documento semplice. Dato che a seconda delle modalità di logging configurate in tutti i log potrebbero essere riportati diversi dati personali e/o sensibili tutti i documenti di log sono ritenuti strettamente riservati. Tutti i log sono isolati per Tenant.	L'accesso alle informazioni di log, laddove non automatizzato da servizio (che rispetta nativamente i requisiti richiesti) viene reso disponibile, successivamente ad una richiesta via ticket, attraverso un documento semplice. Dato che a seconda delle modalità di logging configurate in tutti i log potrebbero essere riportati diversi dati personali e/o sensibili tutti i documenti di log sono ritenuti strettamente riservati. Tutti i log sono isolati per Tenant.	L'accesso alle informazioni di log, laddove non automatizzato da servizio (che rispetta nativamente i requisiti richiesti) viene reso disponibile, successivamente ad una richiesta via ticket, attraverso un documento semplice. Dato che a seconda delle modalità di logging configurate in tutti i log potrebbero essere riportati diversi dati personali e/o sensibili tutti i documenti di log sono ritenuti strettamente riservati. Tutti i log sono isolati per Tenant.	L'accesso alle informazioni di log, laddove non automatizzato da servizio (che rispetta nativamente i requisiti richiesti) viene reso disponibile, successivamente ad una richiesta via ticket, attraverso un documento semplice. Dato che a seconda delle modalità di logging configurate in tutti i log potrebbero essere riportati diversi dati personali e/o sensibili tutti i documenti di log sono ritenuti strettamente riservati. Tutti i log sono isolati per Tenant.	Tutti i sistemi di logging messi a disposizione di Si.net da parte dei provider rispettano le richieste in quanto coperti da certificazione ISO. I servizi di logging sono isolati per account e sono effettuati a livello di infrastruttura e/o API, non contengono dunque dati personali e/o sensibili degli utenti disponibili invece solo ad alto livello.
Implementare una procedura, possibilmente automatizzata, che cancelli i log una volta passato il periodo di conservazione definito, in maniera documentata. Verificare che le procedure di controllo accessi logici assicurino che le informazioni di log siano usate solo per gli scopi prefissati. (controllo 27018 12.4.2)	I servizi adottano una di queste due procedure di rotazione dei log: - Rotazione automatica: Nella quale i documenti vengono eliminati e/o sovrascritti in maniera del tutto automatica senza intervento dello staff - Rotazione ibrida: Nella quale alcuni log implementano una rotazione automatica (spesso molto breve, per-chiamata o per-ora ad esempio) mentre altri, più generici e di sistema vengono gestiti manualmente dallo staff che ne definisce contrattualmente il limite con i clienti. E' definito contrattualmente che l'accesso alle informazioni di log è esclusivamente concesso per scopi di debug, ottimizzazione delle performance e verifiche di funzionamento dell'applicativo.	I servizi adottano una di queste due procedure di rotazione dei log: - Rotazione automatica: Nella quale i documenti vengono eliminati e/o sovrascritti in maniera del tutto automatica senza intervento dello staff - Rotazione ibrida: Nella quale alcuni log implementano una rotazione automatica (spesso molto breve, per-chiamata o per-ora ad esempio) mentre altri, più generici e di sistema vengono gestiti manualmente dallo staff che ne definisce contrattualmente il limite con i clienti. E' definito contrattualmente che l'accesso alle informazioni di log è esclusivamente concesso per scopi di debug, ottimizzazione delle performance e verifiche di funzionamento dell'applicativo.	I servizi adottano una di queste due procedure di rotazione dei log: - Rotazione automatica: Nella quale i documenti vengono eliminati e/o sovrascritti in maniera del tutto automatica senza intervento dello staff - Rotazione ibrida: Nella quale alcuni log implementano una rotazione automatica (spesso molto breve, per-chiamata o per-ora ad esempio) mentre altri, più generici e di sistema vengono gestiti manualmente dallo staff che ne definisce contrattualmente il limite con i clienti. L'accesso alle informazioni di log è esclusivamente concesso per scopi di debug, ottimizzazione delle performance e verifiche di funzionamento dell'applicativo.	I servizi adottano una di queste due procedure di rotazione dei log: - Rotazione automatica: Nella quale i documenti vengono eliminati e/o sovrascritti in maniera del tutto automatica senza intervento dello staff - Rotazione ibrida: Nella quale alcuni log implementano una rotazione automatica (spesso molto breve, per-chiamata o per-ora ad esempio) mentre altri, più generici e di sistema vengono gestiti manualmente dallo staff che ne definisce contrattualmente il limite con i clienti. L'accesso alle informazioni di log è esclusivamente concesso per scopi di debug, ottimizzazione delle performance e verifiche di funzionamento dell'applicativo.	Tutti i servizi di logging utilizzati da Si.net e messi a disposizione dei CSP implementano politiche di ritenzione limitate nel tempo ed automatiche. I sistemi di controllo degli accessi garantiscono la possibilità di limitare gli accessi alle sole figure preposte all'amministrazione del sistema e alle verifiche di operatività. L'utilizzo di servizi che estedono in maniera illimitata la conservazione di specifici log deve essere richiesta, motivata e documentata via ticket, la stessa deve poi essere approvata dall'Architect di riferimento.
Fornire al customer informazioni riguardo alla sincronizzazione data/ora dell'infrastruttura e/o del servizio proposto e se necessario indicazioni su come adattare i propri strumenti installati sull'infrastruttura/piattaforma. (controllo 27017 12.4.4)	Si.net utilizza all'interno dei suoi servizi le risorse NTP di riferimento dei CSP su cui vengono ospitati gli applicativi. I clienti possono richiedere in qualunque momento informazioni a riguardo via ticket.	Si.net utilizza all'interno dei suoi servizi le risorse NTP di riferimento dei CSP su cui vengono ospitati gli applicativi. I clienti possono richiedere in qualunque momento informazioni a riguardo via ticket.	Si.net utilizza all'interno dei suoi servizi le risorse NTP di riferimento dei CSP su cui vengono ospitati gli applicativi. I clienti possono richiedere in qualunque momento informazioni a riguardo via ticket.	Si.net utilizza all'interno dei suoi servizi le risorse NTP di riferimento dei CSP su cui vengono ospitati gli applicativi. I clienti possono richiedere in qualunque momento informazioni a riguardo via ticket.	I CSP garantiscono e forniscono servizi NTP ad hoc (o collegamenti ai servizi di riferimento) all'interno delle loro documentazioni. Si utilizza il servizio NTP di riferimento di ogni CSP per tutti i progetti ospitati sullo stesso.
Il provider deve predisporre soluzioni di monitoraggio utilizzabili dal customer per monitorare i propri servizi, segregate opportunamente tra i vari clienti. Verificare che vengano prodotte metriche conformi agli SLA. **(**controllo 27017 12.4.5)	Si.net non permette ai clienti dei servizi Saas di accedere a strumenti di monitoraggio diretti sui livelli sottostanti quello applicativo ma, a seconda del software, il cliente può richiedere in ogni momento dati di utilizzo delle risorse tramite ticket o avere a disposizione strumenti di controllo automatizzati. Le metriche prodotte, in entrambe le modalità, sono eguali o superiori a quelle di conformità SLA.	Si.net non permette ai clienti dei servizi Saas di accedere a strumenti di monitoraggio diretti sui livelli sottostanti quello applicativo ma, a seconda del software, il cliente può richiedere in ogni momento dati di utilizzo delle risorse tramite ticket o avere a disposizione strumenti di controllo automatizzati. Le metriche prodotte, in entrambe le modalità, sono eguali o superiori a quelle di conformità SLA.	Si.net non permette ai clienti dei servizi Paas di accedere a strumenti di monitoraggio diretti sui livelli sottostanti quello della piattaforma ma, a seconda della piattaforma, il cliente può richiedere in ogni momento dati di utilizzo delle risorse tramite ticket o avere a disposizione strumenti di controllo automatizzati limitati al contesto della piattaforma. Le metriche prodotte, in entrambe le modalità, sono eguali o superiori a quelle di conformità SLA.	Il cliente può utilizzare qualsiasi strumento, nativo o di terze parti (se rispetta le norme di uso accettabile), a livello di sistema operativo per monitorare l'utilizzo di qualsiasi risorsa anche in tempo reale. Il cliente può comunque richiedere in qualunque momento dati di utilizzo delle risorse tramite ticket. Le metriche prodotte, in entrambe le modalità, sono eguali o superiori a quelle di conformità SLA.	All'interno della documentazione tecnica i CSP descrivono soft e hard limits per ogni servizio, mettono inoltre a disposizione strumenti di monitoraggio pianificato o continuo per permettere a Si.net di verificare l'occupazione delle risorse in uso. Le metriche monitorabili sono eguali o superiori a quelle di conformità SLA.
Fornire in base a quanto concordato in fase contrattuale al customer informazioni riguardo alla gestione delle vulnerabilità tecniche (id, tipo di vulnerabilità, punteggio di vulnerabilità e conseguente criticità, exploit, contromisure disponibili) identificate in fase di VA/PT che devono essere schedulate periodicamente dal provider. (controllo 27018 12.6.1)	Si.net non rilascia spontamente informazioni riguardo alle attività di VA/PT effettuate periodicamente. Il cliente è informato contrattualmente della possibilità di richiedere tramite ticket rapporti generici riguardanti gli esiti delle attività di VA/PT.	Si.net non rilascia spontamente informazioni riguardo alle attività di VA/PT effettuate periodicamente. Il cliente è informato contrattualmente della possibilità di richiedere tramite ticket rapporti generici riguardanti gli esiti delle attività di VA/PT.	Si.net non rilascia spontamente informazioni riguardo alle attività di VA/PT effettuate periodicamente. Il cliente è informato contrattualmente della possibilità di richiedere tramite ticket rapporti generici riguardanti gli esiti delle attività di VA/PT.	Si.net non rilascia spontamente informazioni riguardo alle attività di VA/PT effettuate periodicamente. Il cliente è informato contrattualmente della possibilità di richiedere tramite ticket rapporti generici riguardanti gli esiti delle attività di VA/PT.	I CSP non espongono o espongono in maniera estremamente limitata informazioni riguardo le attività di VA/PT effettuate. Alcuni CSP permettono di richiedere informaizoni a riguardo attraverso appositi servizi o via supporto.

A livello IAAS/PAAS, il provider deve garantire la segregazione fra i tenant in caso di ambiente cloud con multi-tenancy. Va inoltre garantito che i dati dell'amministrazione interna del cloud provider siano segregati dai dati del customer conservati sul servizio, in maniera che non siano comunicanti. Il provider deve supportare il customer in caso questo chieda aiuto nel verificare la segregazione dei propri dati rispetto a quelli del provider o a quelli di altri customer presenti nello stesso servizio cloud. (controllo 27017 13.1.3)	Si.net garantisce, in caso di ambiente multi-tenant, la segregazione dei singoli tenant gli uni dagli altri. Si.net non ospita mai i propri dati all'interno di ambienti multi-tenant condivisi con clienti. In caso di richiesta, Si.net supporta il cliente, nelle verifiche di segregazione necessarie.	Si.net garantisce, in caso di ambiente multi-tenant, la segregazione dei singoli tenant gli uni dagli altri. Si.net non ospita mai i propri dati all'interno di ambienti multi-tenant condivisi con clienti. In caso di richiesta, Si.net supporta il cliente, nelle verifiche di segregazione necessarie.	Si.net garantisce, in caso di ambiente multi-tenant, la segregazione dei singoli tenant gli uni dagli altri. Si.net non ospita mai i propri dati all'interno di ambienti multi-tenant condivisi con clienti. In caso di richiesta, Si.net supporta il cliente, nelle verifiche di segregazione necessarie.	Si.net garantisce, in caso di ambiente multi-tenant, la segregazione dei singoli tenant gli uni dagli altri. Si.net non ospita mai i propri dati all'interno di ambienti multi-tenant condivisi con clienti. In caso di richiesta, Si.net supporta il cliente, nelle verifiche di segregazione necessarie.	I CSP offrono sistemi di segregazione basati sulla suddivisione in account, questi sono strettamente regolati da isolamenti logici a basso livello.
Nel caso di infrastruttura virtualizzata, il provider deve definire nella politica della sicurezza delle informazioni le linee guida per la configurazione del proprio virtual network e assicurarne la non conflittualità con quanto d'altro presente nella politica. (controllo 27017 CLD.13.1.4)	I servizi Saas offerti da Si.net non implementano logiche di virtualizzazione per il cliente.	Si.net descrive all'interno della documentazione tecnica e/o a livello di contratto le specifiche di sicurezza e le linee guida di messa in sicurezza dell'ambiente di virtualizzazione laddove messo a disposizione del cliente.	Si.net descrive all'interno della documentazione tecnica e/o a livello di contratto le specifiche di sicurezza e le linee guida di messa in sicurezza dell'ambiente di virtualizzazione laddove messo a disposizione del cliente.	Si.net descrive all'interno della documentazione tecnica e/o a livello di contratto le specifiche di sicurezza e le linee guida di messa in sicurezza dell'ambiente di virtualizzazione laddove messo a disposizione del cliente.	I CSP descrivono all'interno della loro documentazione tecnica e nei loro programmi di formazione e certificazione (laddove presenti) le best-practice e le linee guida consigliate per la messa in sicurezza dei network.
Il provider deve fornire al customer dettagli riguardo alle funzionalità utilizzate per rispettare i requisiti di sicurezza previsti per il servizio (o concordati ad hoc con il customer) e alle eventuali falle nella sicurezza, salvaguardandosi per mezzo di NDA dalla diffusione all'esterno delle informazioni. Quindi, a livello infrastrutturale, di firewall, di exploiting eventuale delle vulnerabilità, di networking (IAAS/PAAS), di sviluppo sicuro e vulnerabilità tecniche (SAAS). (controllo 27017 14.1.1)	Le procedure di messa in sicurezza dei servizi implementate da Si.net sono descritte nella documentazione tecnica del singolo servizio o nel documento contrattuale.	Le procedure di messa in sicurezza dei servizi implementate da Si.net sono descritte nella documentazione tecnica del singolo servizio o nel documento contrattuale.	Le procedure di messa in sicurezza dei servizi implementate da Si.net sono descritte nella documentazione tecnica del singolo servizio o nel documento contrattuale.	Le procedure di messa in sicurezza dei servizi implementate da Si.net sono descritte nella documentazione tecnica del singolo servizio o nel documento contrattuale.	I CSP descrivono all'interno della documentazione tecnica dei singolo servizi le soluzioni messe in campo per la sicurezza dei servizi e dei dati in essi contenuti o in transito.
Customer e provider devono concordare e implementare procedure per la produzione di evidenze digitali (es. log di amministrazione, timestamp di transazioni) all'interno e riguardanti l'ambiente cloud. (controllo 27017 16.1.7)	Si.net implementa e concorda con il cliente in fase contrattuale il tracciamento delle operazioni di gestione dell'ambiente cloud attraverso servizi o applicativi interni ad hoc.	Si.net implementa e concorda con il cliente in fase contrattuale il tracciamento delle operazioni di gestione dell'ambiente cloud attraverso servizi o applicativi interni ad hoc.	Si.net implementa e concorda con il cliente in fase contrattuale il tracciamento delle operazioni di gestione dell'ambiente cloud attraverso servizi o applicativi interni ad hoc.	Si.net implementa e concorda con il cliente in fase contrattuale il tracciamento delle operazioni di gestione dell'ambiente cloud attraverso servizi o applicativi interni ad hoc.	I CSP offrono servizi di tracciamento delle attività di gestione dell'ambiente cloud e le mettono a disposizione di Si.net per garantirne un monitoraggio condiviso.
Il provider deve comunicare al customer la giurisdizione da cui è governato. Il provider deve identificare i propri requisiti legali (in termini di dati personali, GDPR) comunicandoli al customer quando richiesti, e fornire se richieste evidenza della propria compliance al cogente (ad esempio Registro del Trattamenti). (controllo 27017 18.1.1)	Si.net descrive all'interno della propria politica di sicurezza le zone su cui opera, al cliente, in fase contrattuale viene specificata la regione geografica nella quale verranno ospitati i suoi servizi. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	Si.net descrive all'interno della propria politica di sicurezza le zone su cui opera, al cliente, in fase contrattuale viene specificata la regione geografica nella quale verranno ospitati i suoi servizi. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	Si.net descrive all'interno della propria politica di sicurezza le zone su cui opera, al cliente, in fase contrattuale viene specificata la regione geografica nella quale verranno ospitati i suoi servizi. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	Si.net descrive all'interno della propria politica di sicurezza le zone su cui opera, al cliente, in fase contrattuale viene specificata la regione geografica nella quale verranno ospitati i suoi servizi. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	I CSP che operano su più giurisdizioni permettono a Si.net la selezione autonoma di queste garantendo che non verrà mai effettuata migrazione di dati tra regioni se non avviata da Si.net stessa. I CSP mettono inoltre a disposizione evidenze sulla conformità ai requisiti legali vigenti.
Il provider deve stabilire un processo per rispondere a contenziosi riguardo i diritti di proprietà intellettuale. Le casistiche in cui possono verificarsi questi tipi di problemi (vedi customer) sono tipiche del provider IAAS/PAAS, ma anche in caso di servizio SAAS è bene che sia stabilito un processo di questo tipo (ad esempio sistema di ticketing). (controllo 27017 18.1.2)	Tutte le richieste, ivi comprese quelle di contenzioso riguardo ai diritti di proprietà intellettuale, sono gestiti attraverso il sistema di ticketing.	Tutte le richieste, ivi comprese quelle di contenzioso riguardo ai diritti di proprietà intellettuale, sono gestiti attraverso il sistema di ticketing.	Tutte le richieste, ivi comprese quelle di contenzioso riguardo ai diritti di proprietà intellettuale, sono gestiti attraverso il sistema di ticketing.	Tutte le richieste, ivi comprese quelle di contenzioso riguardo ai diritti di proprietà intellettuale, sono gestiti attraverso il sistema di ticketing.	Per questa tipologia di processi, Si.net colloquia con i CSP di riferimento attraverso il sistema di ticketing (o laddove non presente, mail) messo a disposizione del provider.
Il provider deve fornire al customer le modalità e la locazione dei propri dati salvati sul servizio, rilevanti per l'utilizzo del servizio cloud, in fase contrattuale. (controllo 27017 18.1.3)	Si.net descrive all'interno della propria politica di sicurezza e nel contratto di servizio le zone su cui opera al cliente. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	Si.net descrive all'interno della propria politica di sicurezza e nel contratto di servizio le zone su cui opera al cliente. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	Si.net descrive all'interno della propria politica di sicurezza e nel contratto di servizio le zone su cui opera al cliente. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	Si.net descrive all'interno della propria politica di sicurezza e nel contratto di servizio le zone su cui opera al cliente. Il cliente può richiedere a Si.net in ogni momento tramite ticket evidenze sul posizionamento dei propri dati e della conformità ai relativi regolamenti.	I CSP che operano su più giurisdizioni permettono a Si.net la selezione autonoma di queste garantendo che non verrà mai effettuata migrazione di dati tra regioni se non avviata da Si.net stessa. I CSP mettono inoltre a disposizione evidenze sulla conformità ai requisiti legali vigenti.
Il provider deve fornire evidenze a livello contrattuale che i requisiti definiti in 10.1.1 siano accettabili da un punto di vista legale e di giurisdizione (controllo 27017 18.1.5)	Si.net rende disponibile, su richiesta via ticket del cliente, le soluzioni crittografiche scelte e la motivazione per ognuna di esse.	Si.net rende disponibile, su richiesta via ticket del cliente, le soluzioni crittografiche scelte e la motivazione per ognuna di esse.	Si.net rende disponibile, su richiesta via ticket del cliente, le soluzioni crittografiche scelte e la motivazione per ognuna di esse.	Si.net rende disponibile, su richiesta via ticket del cliente, le soluzioni crittografiche scelte e la motivazione per ognuna di esse.	I CSP garantiscono la validità delle proprie scelte attraverso la confermità alla certificazione ISO 27017.

Fornire evidenze di certificazione 27000, rapporti di audit indipendenti o interni relativi all'ambito servizio cloud erogato. In presenza di impossibilità strutturali dell'effettuazione di audit, il provider deve mettere a disposizione per la durata del contratto indipendenti evidenze che è conforme alle linee guida della sicurezza delle informazioni. (controllo 27018 18.2.1)	Nei contratti di vendita dei prodotti, Si.net includerà sempre la propria certificazione ISO 27000. In mancanza di questa, Si.net metterà a disposizione per tutta la durata contrattuale evidenze di conformità alle linee guida su specifica richiesta del cliente via ticket.	Nei contratti di vendita dei prodotti, Si.net includerà sempre la propria certificazione ISO 27000. In mancanza di questa, Si.net metterà a disposizione per tutta la durata contrattuale evidenze di conformità alle linee guida su specifica richiesta del cliente via ticket.	Nei schede di vendita dei prodotti, Si.net includerà sempre la propria certificazione ISO 27000. In mancanza di questa, Si.net metterà a disposizione per tutta la durata contrattuale evidenze di conformità alle linee guida su specifica richiesta del cliente via ticket.	Nei schede di vendita dei prodotti, Si.net includerà sempre la propria certificazione ISO 27000. In mancanza di questa, Si.net metterà a disposizione per tutta la durata contrattuale evidenze di conformità alle linee guida su specifica richiesta del cliente via ticket.	Si.net collabora esclusivamente con CSP con, tra le altre, certificazione ISO 27000.
Il provider deve fornire contrattualmente al customer le relative informazioni rilevanti e/o misure tecniche quando il Titolare del trattamento dei dati dipende dal servizio cloud erogato. (controllo 27018 A.1.1)	Si.net agisce da titolare del trattamento dei dati quando raccoglie dati personali e determina le finalità e le modalità per il loro trattamento (ad esempio, quando Si.net memorizza le informazioni necessarie per la registrazione e l'amministrazione di un account, l'accesso ai servizi o le informazioni di contatto per fornire assistenza tramite il supporto clienti). In tutti gli altri casi il titolare dei dati è il cliente.	Si.net agisce da titolare del trattamento dei dati quando raccoglie dati personali e determina le finalità e le modalità per il loro trattamento (ad esempio, quando Si.net memorizza le informazioni necessarie per la registrazione e l'amministrazione di un account, l'accesso ai servizi o le informazioni di contatto per fornire assistenza tramite il supporto clienti). In tutti gli altri casi il titolare dei dati è il cliente.	Si.net agisce da titolare del trattamento dei dati quando raccoglie dati personali e determina le finalità e le modalità per il loro trattamento (ad esempio, quando Si.net memorizza le informazioni necessarie per la registrazione e l'amministrazione di un account, l'accesso ai servizi o le informazioni di contatto per fornire assistenza tramite il supporto clienti). In tutti gli altri casi il titolare dei dati è il cliente.	Si.net agisce da titolare del trattamento dei dati quando raccoglie dati personali e determina le finalità e le modalità per il loro trattamento (ad esempio, quando Si.net memorizza le informazioni necessarie per la registrazione e l'amministrazione di un account, l'accesso ai servizi o le informazioni di contatto per fornire assistenza tramite il supporto clienti). In tutti gli altri casi il titolare dei dati è il cliente.	I CSP specificano nella loro documentazione le specifiche relative alla titolarità dei dati ed al loro trattamento. (es. portale GDPR)
I dati personali processati sotto contratto non devono essere processati per motivi al di fuori dell'ambito. L'eventuale processing di dati personali per motivazioni tecniche deve comunque rispettare i principi di informativa e consenso: infatti Il processor agisce "soltanto su istruzione documentata del titolare del trattamento" secondo quanto riportato dall'Art.28 punto 3.a (GDPR). (controllo 27018 A.2.1)	Si.net non tratta mai i dati dei clienti in alcun caso al di fuori dell'ambito di erogazione del servizio e della messa in sicurezza delle informazioni. I trattamenti tecnici di quest'ultimo tipo sono formalizzati in fase contrattuale.	Si.net non tratta mai i dati dei clienti in alcun caso al di fuori dell'ambito di erogazione del servizio e della messa in sicurezza delle informazioni. I trattamenti tecnici di quest'ultimo tipo sono formalizzati in fase contrattuale.	Si.net non tratta mai i dati dei clienti in alcun caso al di fuori dell'ambito di erogazione del servizio e della messa in sicurezza delle informazioni. I trattamenti tecnici di quest'ultimo tipo sono formalizzati in fase contrattuale.	Si.net non tratta mai i dati dei clienti in alcun caso al di fuori dell'ambito di erogazione del servizio e della messa in sicurezza delle informazioni. I trattamenti tecnici di quest'ultimo tipo sono formalizzati in fase contrattuale.	I CSP agiscono come processor garantendo la loro conformità a quanto richiesto attraverso la certificazione ISO 27018.
Il processor non può definire ulteriori finalità nell'ambito del rapporto con il Customer, ad esempio con finalità di marketing. (controllo 27018 A.2.2)	Si.net non definisce nessuna ulteriore finalità.	Si.net non definisce nessuna ulteriore finalità.	Si.net non definisce nessuna ulteriore finalità.	Si.net non definisce nessuna ulteriore finalità.	I CSP documentano le loro finalità all'interno di documentazione specifica (es. "GDPR DATA PROCESSING ADDENDUM") o all'interno del contratto con Si.net.
Scrivere e rispettare una procedura che descrive le modalità e i criteri di cancellazione dei file temporanei sul cloud, incluso un periodo di tempo definito e documentabile. (controllo 27018 A.4.1)	I file temporanei degli applicativi Si.net sono distrutti, assieme a tutti gli altri dati e a tutte le strutture e le risorse al termine del contratto con il cliente. Prima di questo periodo Si.net potrebbe eliminare i dati temporanei per motivi di ottimizzazione delle performance o evoluzione del sistema. Al contempo il cliente può in qualunque momento tramite ticket richiedere la cancellazione dei propri file temporanei.	I file temporanei degli applicativi Si.net sono distrutti, assieme a tutti gli altri dati e a tutte le strutture e le risorse al termine del contratto con il cliente. Prima di questo periodo Si.net potrebbe eliminare i dati temporanei per motivi di ottimizzazione delle performance o evoluzione del sistema. Al contempo il cliente può in qualunque momento tramite ticket richiedere la cancellazione dei propri file temporanei.	I file temporanei degli applicativi Si.net sono distrutti, assieme a tutti gli altri dati e a tutte le strutture e le risorse al termine del contratto con il cliente. Prima di questo periodo Si.net potrebbe eliminare i dati temporanei per motivi di ottimizzazione delle performance o evoluzione del sistema. Al contempo il cliente può in qualunque momento tramite ticket richiedere la cancellazione dei propri file temporanei.	I file temporanei degli applicativi Si.net sono distrutti, assieme a tutti gli altri dati e a tutte le strutture e le risorse al termine del contratto con il cliente. Prima di questo periodo Si.net potrebbe eliminare i dati temporanei per motivi di ottimizzazione delle performance o evoluzione del sistema. Al contempo il cliente può in qualunque momento tramite ticket richiedere la cancellazione dei propri file temporanei.	I CSP, laddove previsto nei servizi offerti a Si.net, specificano per-servizio, tempistiche e modalità di ritenzione dei file temporanei.
Il **contratto tra il cloud provider e customer deve prevedere che il provider debba notificare al cliente del servizio cloud, in conformità a qualsiasi procedura e periodo di tempo concordato nel contratto, qualsiasi richiesta legalmente vincolante di divulgazione di dati personali da parte di un'autorità giudiziaria, a meno che tale divulgazione non sia altrimenti vietata. Analogamente, il trasferimento dei dati personali da parte del Processor deve essere opportunamente normato a livello contrattuale salvo gli obblighi previsti per legge.** (controllo 27018 A.5.1)	Si.net riporta contrattualmente quanto richiesto sia per quanto riguarda la notifica di accesso che per il trasferimento dai dati da parte di Si.net ai CSP.	Si.net riporta contrattualmente quanto richiesto sia per quanto riguarda la notifica di accesso che per il trasferimento dai dati da parte di Si.net ai CSP.	Si.net riporta contrattualmente quanto richiesto sia per quanto riguarda la notifica di accesso che per il trasferimento dai dati da parte di Si.net ai CSP.	Si.net riporta contrattualmente quanto richiesto sia per quanto riguarda la notifica di accesso che per il trasferimento dai dati da parte di Si.net ai CSP.	I CSP specificano nella loro documentazione (es. "GDPR DATA PROCESSING ADDENDUM") e tramite la loro certificazione ISO 27018 la conformità a quanto richiesto.
Registrare le diffusioni di dati personali alle terze parti, inclusi quali, a chi, quando e con quali strumenti (in relazione alle richieste delle autorità di controllo pertinenti). E' utilizzabile ad esempio un log delle richieste di trasferimento. (controllo 27018 A.5.2)	Si.net non effettua diffusioni di dati personali al di fuori della collaborazione con il sub-fornitore CSP.	Si.net non effettua diffusioni di dati personali al di fuori della collaborazione con il sub-fornitore CSP.	Si.net non effettua diffusioni di dati personali al di fuori della collaborazione con il sub-fornitore CSP.	Si.net non effettua diffusioni di dati personali al di fuori della collaborazione con il sub-fornitore CSP.	I CSP specificano nella loro documentazione (es. "GDPR DATA PROCESSING ADDENDUM") e tramite la loro certificazione ISO 27018 la conformità a quanto richiesto.

Il ricorso ad un sub-fornitore deve essere espressamente concordato con il customer. Il Processor rimane responsabile di quanto svolto dai sub contractor e pertanto le clausole contrattuali dovranno ribaltare in maniera appropriata gli obblighi di ciascuna parte interessata (Art.28 Punto 4 GDPR). Ad esempio, se un fornitore SaaS si appoggia su un Cloud Service Provider esterno (p.e. per le componenti IAAS e/o PAAS), devono essere formalizzati a livello contrattuale tutti gli obblighi nella supply chain. (controllo 27018 A.7.1)	Si.net formalizza a livello contrattuale il CSP di riferimento per il singolo contratto e ne riflette i riferimenti di sicurezza e conformità.	Si.net formalizza a livello contrattuale il CSP di riferimento per il singolo contratto e ne riflette i riferimenti di sicurezza e conformità.	Si.net formalizza a livello contrattuale il CSP di riferimento per il singolo contratto e ne riflette i riferimenti di sicurezza e conformità.	Si.net formalizza a livello contrattuale il CSP di riferimento per il singolo contratto e ne riflette i riferimenti di sicurezza e conformità.	I CSP specificano nella loro documentazione (es. "GDPR DATA PROCESSING ADDENDUM") e tramite la loro certificazione ISO 27018 la conformità a quanto richiesto.
Il processor deve prontamente contattare il customer in caso di non autorizzato accesso ai dati personali contenuti nel servizio cloud o a asset di equipaggiamento/strutture del customer comportanti perdita, diffusione o alterazione di dati personali. Ci deve essere una gestione degli incident e degli eventi che possono portare a un possibile data breach. Il processor deve in ogni caso ottemperare il GDPR. (controllo 27018 A.9.1)	SI.net effettua la gestione di breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato tramite ticket specifico o canale di comunicazione.	SI.net effettua la gestione di breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato tramite ticket specifico o canale di comunicazione.	SI.net effettua la gestione di breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato tramite ticket specifico o canale di comunicazione.	SI.net effettua la gestione di breach in conformità con quanto normato nel GDPR; In caso di incidente il cliente viene tempestivamente avvisato tramite ticket specifico o canale di comunicazione.	I CSP, in confrmità al GDPR e alla certificazione 20018 sono tenuti a comunicare a Si.net il verificarsi di eventi di breach.
Le copie delle policy e procedure di sicurezza vanno conservate per uno specifico e documentato periodo dopo il rilascio di una nuova versione. La norma 27018 suggerisce 5 anni, mentre il GDPR non fornisce un dettaglio. (controllo 27018 A.9.2)	Si.net conserva le copie secondo quando descritto nelle procedure di gestione della documentazione del sistema.	Si.net conserva le copie secondo quando descritto nelle procedure di gestione della documentazione del sistema.	Si.net conserva le copie secondo quando descritto nelle procedure di gestione della documentazione del sistema.	Si.net conserva le copie secondo quando descritto nelle procedure di gestione della documentazione del sistema.	I CSP rispettano quanto richiesto certificando la loro procedura di conservazione tramite ISO 27018.
Definire una politica che presenti le modalità di restituzione, trasferimento e dismissione degli asset contenenti dati personali del customer, relativi al servizio cloud erogato. (controllo 27018 A.9.3)	Si.net definisce contrattualmente la distruzione completa di tutti gli asset collegati al cliente nel momento del termine del contratto. Il cliente può in qualunque momento, durante la durata dell'accordo, richiedere assistenza a Si.net per organizzare procedure di trasferimento e/o restituzione di eventuale materiale ospitato da Si.net.	Si.net definisce contrattualmente la distruzione completa di tutti gli asset collegati al cliente nel momento del termine del contratto. Il cliente può in qualunque momento, durante la durata dell'accordo, richiedere assistenza a Si.net per organizzare procedure di trasferimento e/o restituzione di eventuale materiale ospitato da Si.net.	Si.net definisce contrattualmente la distruzione completa di tutti gli asset collegati al cliente nel momento del termine del contratto. Il cliente può in qualunque momento, durante la durata dell'accordo, richiedere assistenza a Si.net per organizzare procedure di trasferimento e/o restituzione di eventuale materiale ospitato da Si.net.	Si.net definisce contrattualmente la distruzione completa di tutti gli asset collegati al cliente nel momento del termine del contratto. Il cliente può in qualunque momento, durante la durata dell'accordo, richiedere assistenza a Si.net per organizzare procedure di trasferimento e/o restituzione di eventuale materiale ospitato da Si.net.	I CSP presentano processi certificati ISO 27018 per la distruzione degli asset. Trasferimento e restituzione dei contenuti avvengono attraverso i servizi messi a disposizione dai CSP a Si.net.
Sincerarsi che chi ha accesso ai dati personali firmi un accordo di riservatezza. (controllo 27018 A.10.1)	Chi accede ai dati personali è stato autorizzato attraverso opportuni documenti di autorizzazione al trattamento interne a Si.net.	Chi accede ai dati personali è stato autorizzato attraverso opportuni documenti di autorizzazione al trattamento interne a Si.net.	Chi accede ai dati personali è stato autorizzato attraverso opportuni documenti di autorizzazione al trattamento interne a Si.net.	Chi accede ai dati personali è stato autorizzato attraverso opportuni documenti di autorizzazione al trattamento interne a Si.net.	I CSP garantiscono le politiche di riservatezza interne attraverso apposita documentazione (es. "GDPR DATA PROCESSING ADDENDUM").
Implementare una procedura e produrre evidenze (log) riguardante il restoring dei dati personali. (controllo 27018 A.10.3)	Si.net permette al cliente di sfruttare i dati di backup (così come configurati contrattualmente) per il ripristino tramite richiesta via ticket. Il cliente può richiedere nel ticket stesso la produzione di log relativi al processo. Il cliente è comunque sempre invitato a effettuare tramite gli strumenti messi a disposizione copie personali dei propri dati per una maggiore sicurezza, velocità ed indipendenza nel ripristino.	Si.net permette al cliente di sfruttare i dati di backup (così come configurati contrattualmente) per il ripristino tramite richiesta via ticket. Il cliente può richiedere nel ticket stesso la produzione di log relativi al processo. Il cliente è comunque sempre invitato a effettuare tramite gli strumenti messi a disposizione copie personali dei propri dati per una maggiore sicurezza, velocità ed indipendenza nel ripristino.	Si.net permette al cliente di sfruttare i dati di backup (così come configurati contrattualmente) per il ripristino tramite richiesta via ticket. Il cliente può richiedere nel ticket stesso la produzione di log relativi al processo. Il cliente è comunque sempre invitato a effettuare copie personali dei propri dati per una maggiore sicurezza, velocità ed indipendenza nel ripristino.	In ambiente managed, Si.net permette al cliente di sfruttare i dati di backup (così come configurati contrattualmente) per il ripristino tramite richiesta via ticket. Il cliente può richiedere nel ticket stesso la produzione di log relativi al processo. In ambiente gestito dal cliente quest'ultimo è tenuto a configurare da sè i servizi e i processi di backup necessari e specifici per il suo caso. Si.net in fase di formazione consiglia al cliente metodologie e strumenti di backup senza però operare attività all'interno dell'ambiente.	I CSP mettono a disposizione di Si.net strumenti specifici per le operazioni di restore, tali strumenti colloquiano con i tool di logging per garantire trasparenza nell'attività di recupero.
Definire una procedura di autorizzazione riguardante i dispositivi contenenti dati personali che lasciano (fisicamente) l'organizzazione, per far si che non siano accessibili a nessuno oltre al personale autorizzato. (controllo 27018 A.10.4)	Si.net riflette le procedure attuate dai CSP sul cliente per l'eventuale utilizzo di dispositivi fisici di import/export sfruttando servizi ad hoc offerti dal CSP.	Si.net riflette le procedure attuate dai CSP sul cliente per l'eventuale utilizzo di dispositivi fisici di import/export sfruttando servizi ad hoc offerti dal CSP.	Si.net riflette le procedure attuate dai CSP sul cliente per l'eventuale utilizzo di dispositivi fisici di import/export sfruttando servizi ad hoc offerti dal CSP.	Si.net riflette le procedure attuate dai CSP sul cliente per l'eventuale utilizzo di dispositivi fisici di import/export sfruttando servizi ad hoc offerti dal CSP.	I CSP che offrono servizi legati a dispositivi fisici operano secondo procedure altamente controllate che garantiscono la sicurezza dei dati e la chain of custody.
Non utilizzare dispositivi portatili che non permettono la crittografia dei dati eccetto i casi inevitabili, da documentare. (controllo 27018 A.10.5)	Si.net non utilizza dispositivi portatili non crittografati nell'ambiente operativo cloud.	Si.net non utilizza dispositivi portatili non crittografati nell'ambiente operativo cloud.	Si.net non utilizza dispositivi portatili non crittografati nell'ambiente operativo cloud.	Si.net non utilizza dispositivi portatili non crittografati nell'ambiente operativo cloud.	I CSP utilizzati da Si.net non utilizzano dispositivi portatili non crittografati nell'ambiente operativo cloud offerto.
Mantenere un elenco aggiornato di utenti e profili di utenti che hanno accesso ai sistemi informativi (i.e. servizi cloud erogati). (controllo 27018 A.10.9)	All'interno degli applicativi Si.net gestisce un componente di autenticazione che raccoglie le utenze abilitate all'accesso ed i relativi livelli di permesso.	All'interno degli applicativi Si.net gestisce un componente di autenticazione che raccoglie le utenze abilitate all'accesso ed i relativi livelli di permesso.	Si.net sfrutta gli strumenti messi a disposizione dai CSP per gestire e monitorare gli oggetti di autenticazione ed autorizzazione attivi e storici all'interno dell'ambiente cloud.	Si.net sfrutta gli strumenti messi a disposizione dai CSP per gestire e monitorare gli oggetti di autenticazione ed autorizzazione attivi e storici all'interno dell'ambiente cloud.	I CSP mantengono con Si.net account di sicurezza più o meno organizzati tramite i quali Si.net opera in un organizzazione ad albero. Al di sopra del principale account Si.net i CSP garantiscono la validità di questo controllo tramite conformità ISO.

Le utenze dismesse o scadute non devono essere riassegnate a nuovi utenti. (controllo 27018 A.10.10)	Si.net utilizza esclusivamente utenze personali istanziate ad hoc per-persona e per-contesto, la stessa utenza non viene mai riassegnata se disabilitata. Utenze impersonali sono utilizzate esclusivamente per automazioni e devono essere richieste ed autorizzate come da Politica di sicurezza.	Si.net utilizza esclusivamente utenze personali istanziate ad hoc per-persona e per-contesto, la stessa utenza non viene mai riassegnata se disabilitata. Utenze impersonali sono utilizzate esclusivamente per automazioni e devono essere richieste ed autorizzate come da Politica di sicurezza.	Si.net utilizza esclusivamente utenze personali istanziate ad hoc per-persona e per-contesto, la stessa utenza non viene mai riassegnata. Utenze impersonali sono utilizzate esclusivamente per automazioni e devono essere richieste ed autorizzate come da Politica di sicurezza.	Si.net utilizza esclusivamente utenze personali istanziate ad hoc per-persona e per-contesto, la stessa utenza non viene mai riassegnata. Utenze impersonali sono utilizzate esclusivamente per automazioni e devono essere richieste ed autorizzate come da Politica di sicurezza.	I CSP utilizzano account ID unici che impediscono la riassegnazione della stessa utenza in caso di chiusura precedente di un account gemello.
Ribaltare gli obblighi di mantenimento dei requisiti di sicurezza verso la catena dei fornitori (controllo 27018 A.10.12)	Si.net riflette gli obblighi di sicurezza verso i fornitori attraverso l'obbligatorietà per i CSP di essere in possesso di tutte le conformità richiesta a Si.net tra cui le certificazioni ISO e la compliance al GDPR.	Si.net riflette gli obblighi di sicurezza verso i fornitori attraverso l'obbligatorietà per i CSP di essere in possesso di tutte le conformità richiesta a Si.net tra cui le certificazioni ISO e la compliance al GDPR.	Si.net riflette gli obblighi di sicurezza verso i fornitori attraverso l'obbligatorietà per i CSP di essere in possesso di tutte le conformità richiesta a Si.net tra cui le certificazioni ISO e la compliance al GDPR.	Si.net riflette gli obblighi di sicurezza verso i fornitori attraverso l'obbligatorietà per i CSP di essere in possesso di tutte le conformità richiesta a Si.net tra cui le certificazioni ISO e la compliance al GDPR.	I CSP ribaltano verso i propri fornitori tutte le caratteristiche di sicurezza necessarie come obbligo di conformità alla ISO 27018.
Il processor deve assicurare che quando assegna uno spazio a un customer, qualsiasi dato precedentemente conservato nello stesso spazio non è ora visibile al customer, con opportune misure tecniche. (controllo 27018 A.10.13)	Si.net assicura, per riflesso alla conformità da parte dei CSP, lo stato di completa assenza di qualsivoglia dato all'interno degli ambienti consegnati ai clienti. Le istanze Saas, anche se in multi-tenancy, sono consegnate completamente vuote come descritto contrattualmente.	Si.net assicura, per riflesso alla conformità da parte dei CSP, lo stato di completa assenza di qualsivoglia dato all'interno degli ambienti consegnati ai clienti. Le istanze Saas, anche se in multi-tenancy, sono consegnate completamente vuote come descritto contrattualmente.	Si.net assicura, per riflesso alla conformità da parte dei CSP, lo stato di completa assenza di qualsivoglia dato all'interno degli ambienti consegnati ai clienti. Le istanze Paas, anche se in multi-tenancy, sono consegnate completamente vuote.	Si.net assicura, per riflesso alla conformità da parte dei CSP, lo stato di completa assenza di qualsivoglia dato all'interno degli ambienti consegnati ai clienti. Le istanze Iaas, anche se in multi-tenancy, sono consegnate completamente vuote.	La conformità alla norma ISO 27018 garantisce a Si.net come cliente l'assenza di dati precedentemente salvati all'interno delle risorse da Si.net utilizzate e quindi rivendute.
Il processor deve definire i paesi in cui i dati del customer possono essere conservati. (controllo 27018 A.11.1)	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I dati sono fisicamente ospitati in differenti datacenter dislocati in Europa in conformità con il regolamento GDPR, dettagli sulle regioni geografiche utilizzate sono disponibili all'interno della Politica di sicurezza e del Contratto di servizio.	I CSP offrono diverse location geografiche per l'utilizzo dei servizi offerti, il CSP garantisce che tutte le regioni utilizzate da Si.net e specificate all'interno della Politica di sicurezza siano conformi al GDPR e alle certificazioni ISO 27001, 27017 e 27018.
I dati personali trasmessi su una rete devono essere soggetti a appropriati controlli per verificare che raggiungano la destinazione (effettuati test da parte del provider). (controllo 27018 A.11.2)	Si.net riflette sui propri clienti la conformità alla verifica di raggiungimento della destinazione effettuata dai CSP e certificata tramite normativa ISO 27018.	Si.net riflette sui propri clienti la conformità alla verifica di raggiungimento della destinazione effettuata dai CSP e certificata tramite normativa ISO 27018.	Si.net riflette sui propri clienti la conformità alla verifica di raggiungimento della destinazione effettuata dai CSP e certificata tramite normativa ISO 27018.	Si.net riflette sui propri clienti la conformità alla verifica di raggiungimento della destinazione effettuata dai CSP e certificata tramite normativa ISO 27018.	Il CSP garantisce di aver effettuato test di raggiungimento delle destinazioni di riferimento attraverso la conformità alla ISO 27018.