Alla c.a. della Dirigente Scolastica dell'Istituto di Istruzione Superiore "Marco Fanno", Dott.ssa Sabrina Caterina Antiga

Con riferimento al modello predisposto dal suo Istituto per la valutazione dei rischi relativamente al trattamento di dati connesso all'attività di didattica a distanza (qui allegato), il sottoscritto Dott. Federico Croso, quale Responsabile Protezione dati della scuola, ha provveduto ad esaminare la correttezza dell'analisi di rischio condotta.

Considerato

lo strumento utilizzato dall'istituto per condurre la valutazione dei rischi (i.e. Modello validato dall'ENISA) che garantisce un elevato standard di affidabilità ed oggettività dei risultati ottenuti;

il grado di responsabilità (accountability) dimostrata dal Titolare del Trattamento nel verificare l'adeguatezza delle misure adottate circa il trattamento in esame;

tenuto conto

del Provvedimento dell'Autorità Garante Nazionale per la protezione dei dati del 26 marzo 2020 avente ad oggetto "Didattica a distanza: prime indicazioni", ove viene precisato che *"la valutazione di impatto, che l'art. 35 del Regolamento richiede per i casi di rischi elevati, non è necessaria se il trattamento effettuato dalle istituzioni scolastiche e universitarie, ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici)"*;

ESPRIME

il suo parere favorevole circa l'analisi di rischio svolta, ritenendola attendibile anche in ragione delle puntuali notazioni fornite in risposta alle questioni proposte dal modello Enisa utilizzato per la valutazione e

INVITA

L'Istituto Scolastico ad implementare, scrupolosamente, le misure tecniche e organizzative propostevi sulla base del Modello ENISA, in relazione al livello di rischio riscontrato.

In conclusione,

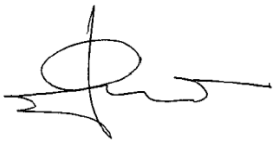
poiché dall'analisi di rischio condotta non risultano riscontrate le condizioni di elevato rischio per i diritti e le libertà degli interessati coinvolti nell'attività di Didattica a distanza, si concorda nel non doversi procedere alla Valutazione d'impatto su detto trattamento

Consiglio, infine, in ottica di rendicontazione, di conservare, unitamente all'analisi di rischio effettuata, il presente parere del DPO, al fine di comprovare le ragioni dell'assenza di DPIA.

Prato Sesia, 09.04.2020

Il responsabile della protezione dei dati

Dott. Federico Croso



Misure di sicurezza

L'adeguatezza delle misure a livelli di rischio specifici non deve essere percepita come assoluta.

A seconda del contesto del trattamento dei dati personali, l'organizzazione può prendere in considerazione l'adozione di misure aggiuntive, anche se assegnate a un livello di rischio più elevato.

Inoltre, l'elenco proposto di misure non tiene conto di altri requisiti di sicurezza specifici del settore, nonché di specifici obblighi normativi, derivanti ad esempio dalla direttiva e-privacy o dalla direttiva NIS.

Nel tentativo di facilitare ulteriormente questa procedura è inclusa anche una mappatura del gruppo di misure proposto con i controlli di sicurezza ISO / IEC 27001: 2013.

Di seguito è riportato un elenco di misure tecniche e organizzative proposte per l'attività di trattamento in esame, sulla base del livello di rischio risultante dalla valutazione effettuata.

Politica di sicurezza e procedure per la protezione dei dati personali

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
A.1	L'organizzazione dovrebbe documentare la propria politica in materia di trattamento dei dati personali nell'ambito della propria politica di sicurezza delle informazioni.	
A.2	La politica di sicurezza dovrebbe essere rivista e rivista, se necessario, su base annuale.	
A.3	L'organizzazione dovrebbe documentare una politica di sicurezza dedicata separata in relazione al trattamento dei dati personali. La politica deve essere approvata dalla direzione e comunicata a tutti i dipendenti e alle parti esterne interessate	
A.4	La politica di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.	
A.5	È necessario creare e mantenere un inventario di politiche / procedure specifiche relative alla sicurezza dei dati personali, sulla base della politica di sicurezza generale	

Relativo a ISO 27001: 2013 - A.5 Politica di sicurezza

Ruoli e responsabilità

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
B.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.	
B.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di lavoro, la revoca dei diritti e delle responsabilità con le rispettive procedure di consegna dovrebbe essere chiaramente definita.	
B.3	Dovrebbe essere eseguita una chiara nomina delle persone incaricate di specifici compiti di sicurezza, inclusa la nomina di un responsabile della sicurezza.	

Relativo a ISO 27001: 2013 - A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni

Politica di controllo dell'accesso

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
C.1	Diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento dei dati personali) in seguito alla necessità di conoscere il principio.	
C.2	Una politica di controllo dell'accesso dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole appropriate per il controllo degli accessi, i diritti di accesso e le restrizioni per ruoli utente specifici verso i processi e le procedure relative ai dati personali.	
C.3	La separazione dei ruoli di controllo dell'accesso (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione dell'accesso) deve essere chiaramente definita e documentata.	

Relativo a ISO 27001: 2013 - A.9.1.1 Politica di controllo dell'accesso

Gestione risorse / risorse

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
D.1	L'organizzazione dovrebbe disporre di un registro delle risorse IT utilizzate per l'elaborazione dei dati personali (hardware, software e rete). Il registro potrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). A una persona specifica dovrebbe essere assegnato il compito di mantenere e aggiornare il registro (ad es. Responsabile IT).	
D.2	Le risorse IT dovrebbero essere riviste e aggiornate su base regolare.	

D.3	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	

Relativo a ISO 27001: 2013 - A.8 Gestione delle risorse

Cambio gestione

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
E.1	L'organizzazione dovrebbe assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad es. IT o responsabile della sicurezza). Dovrebbe essere effettuato un monitoraggio regolare di questo processo.	
E.2	Lo sviluppo del software deve essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire il test, è necessario utilizzare dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, devono essere predisposte procedure specifiche per la protezione dei dati personali utilizzati durante i test.	
E.3	È necessario predisporre una politica di modifica dettagliata e documentata. Dovrebbe includere: un processo per l'introduzione delle modifiche, i ruoli / utenti che dispongono dei diritti di modifica, le tempistiche per l'introduzione delle modifiche. La politica di modifica dovrebbe essere regolarmente aggiornata.	

Relativo a ISO 27001: 2013 - A. 12.1 Procedure operative e responsabilità

Responsabili del trattamento dei dati

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
F.1	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il responsabile del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Tali linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali previsto dalla politica di sicurezza dell'organizzazione.	
F.2	Dopo aver scoperto una violazione dei dati personali, il responsabile del trattamento informa il responsabile del trattamento senza indebito ritardo.	
F.3	Requisiti e obblighi formali dovrebbero essere concordati formalmente tra il responsabile del trattamento e il responsabile	

	del trattamento. Il responsabile del trattamento dei dati dovrebbe fornire prove documentate sufficienti della conformità.	
F.4	L'organizzazione del responsabile del trattamento dei dati dovrebbe verificare periodicamente la conformità del responsabile del trattamento al livello concordato di requisiti e obblighi.	

Relativo a ISO 27001: 2013 - A.15 Rapporti con i fornitori

Gestione degli incidenti / Violazione dei dati personali

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
G.1	È necessario definire un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.	
G.2	Le violazioni dei dati personali devono essere segnalate immediatamente alla direzione. Dovrebbero essere predisposte procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.	
G.3	Il piano di risposta agli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e chiara assegnazione di ruoli.	

Relativo a ISO 27001: 2013 - A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni

Business continuity

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
H.1	L'organizzazione dovrebbe stabilire le principali procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema IT che elabora i dati personali (in caso di incidente / violazione dei dati personali).	
H.2	Un BCP deve essere dettagliato e documentato (seguendo la politica di sicurezza generale). Dovrebbe includere azioni chiare e assegnazione di ruoli.	
H.3	Un livello di qualità garantita del servizio dovrebbe essere definito nel BCP per i processi aziendali core che prevedono la sicurezza dei dati personali.	

Relativo a ISO 27001: 2013 - A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa

Riservatezza del personale

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
I.1	L'organizzazione dovrebbe garantire che tutti i dipendenti comprendano le proprie responsabilità e obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità dovrebbero essere chiaramente comunicati durante il processo di pre-assunzione e / o di inserimento.	
I.2	Prima di assumere le proprie funzioni, i dipendenti devono essere invitati a rivedere e concordare la politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e non divulgazione.	

Relativo a ISO 27001: 2013 - A.7 Sicurezza delle risorse umane

Formazione

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
J.1	L'organizzazione dovrebbe garantire che tutti i dipendenti siano adeguatamente informati sui controlli di sicurezza del sistema IT relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati sui requisiti pertinenti in materia di protezione dei dati e sugli obblighi legali attraverso regolari campagne di sensibilizzazione.	
J.2	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi programmatori specifici per l'induzione (in materia di protezione dei dati) dei nuovi arrivati.	

Relativo a ISO 27001: 2013 - A.7.2.2 Consapevolezza, istruzione e formazione della sicurezza delle informazioni

Controllo accessi e autenticazione

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
K.1	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	
K.2	L'uso di account utente comuni dovrebbe essere evitato. Nei casi in cui ciò è necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	

K.3	Dovrebbe essere istituito un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). È necessario almeno una combinazione nome utente / password. Le password devono rispettare un certo livello (configurabile) di complessità.	
K.4 Il	sistema di controllo degli accessi dovrebbe avere la capacità di rilevare e non consentire l'uso di password che non rispettano un certo livello (configurabile) di complessità.	
K.5	È necessario definire e documentare una specifica politica delle password. La politica dovrebbe includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.	
K.6	Le password degli utenti devono essere archiviate in un formato "con hash".	

Relativo a ISO 27001: 2013 - A.9 Controllo degli accessi

Registrazione e monitoraggio

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
L.1	I file di registro devono essere attivati per ciascun sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	
L.2	I file di registro devono essere timestamp e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con una singola sorgente temporale di riferimento	
L.3	Dovrebbero essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, tra cui l'aggiunta / cancellazione / modifica dei diritti dell'utente.	
L.4	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. L'accesso ai file di registro deve essere registrato oltre al monitoraggio per rilevare attività insolite.	
L.5	Un sistema di monitoraggio dovrebbe elaborare i file di registro e produrre report sullo stato del sistema e notificare eventuali avvisi.	

Relativo a ISO 27001: 2013 - A.12.4 Registrazione e monitoraggio

Sicurezza server / database

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO

M.1	I server di database e applicazioni devono essere configurati per essere eseguiti utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	
M.2	I database e i server delle applicazioni devono elaborare solo i dati personali che sono effettivamente necessari al fine di raggiungere i suoi scopi di elaborazione.	
M.3	Le soluzioni di crittografia devono essere considerate su file o record specifici attraverso l'implementazione di software o hardware.	
M.4	È necessario prendere in considerazione la crittografia delle unità di archiviazione	
M.5	Le tecniche di pseudonimizzazione dovrebbero essere applicate mediante la separazione dei dati dagli identificatori diretti per evitare il collegamento all'interessato senza ulteriori informazioni	

Relativo a ISO 27001: 2013 - A. 12 Sicurezza operativa

Sicurezza della workstation

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
N.1	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	
N.2	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base settimanale.	
N.3	Gli utenti non dovrebbero avere privilegi per installare o disattivare applicazioni software non autorizzate.	
N.4	Il sistema dovrebbe avere dei timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	
N.5	Gli aggiornamenti critici per la sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	
N.6	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.	

Relativo a ISO 27001: 2013 - A. 14.1 Requisiti di sicurezza dei sistemi di informazione

Sicurezza di rete / comunicazione

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
O.1	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	

O.2	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e processi specifici. Dovrebbe essere protetto da meccanismi di	
O.3	In generale, l'accesso remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò è assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dell'organizzazione (ad es. Amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.crittografia.	
O.4	Il traffico da e verso il sistema IT deve essere monitorato e controllato attraverso i firewall e i sistemi di rilevamento delle intrusioni.	

Relativo a ISO 27001: 2013 - A.13 Sicurezza delle comunicazioni

Back-up

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
P.1	Le procedure di backup e ripristino dei dati dovrebbero essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	
P.2	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati ai dati di origine.	
P.3	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	
P.4	I backup completi devono essere eseguiti regolarmente.	
P.5	I supporti di backup devono essere testati periodicamente per assicurarsi che possano essere utilizzati in caso di emergenza.	
P.6	I backup incrementali pianificati devono essere eseguiti almeno su base giornaliera.	
P.7	Le copie del backup devono essere archiviate in modo sicuro in posizioni diverse.	
P.8	Nel caso in cui venga utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare del trattamento.	

Relativo a ISO 27001: 2013 - A.12.3 Backup

Dispositivi mobili / portatili

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO

Q.1	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	
Q.2	I dispositivi mobili autorizzati ad accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.	
Q.3	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli di procedure di controllo dell'accesso (al sistema di elaborazione dati) delle altre apparecchiature terminali.	
Q.4	Ruoli e responsabilità specifici riguardanti la gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.	
Q.5	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi alla sua operazione di elaborazione) su un dispositivo mobile che è stato compromesso.	
Q.6	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e commerciale del dispositivo attraverso contenitori software sicuri.	
Q.7	I dispositivi mobili devono essere protetti fisicamente dal furto quando non vengono utilizzati.	

Relativo a ISO 27001: 2013 - A. 6.2 Dispositivi mobili e telelavoro

Sicurezza del ciclo di vita delle applicazioni

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
R.1	Durante il ciclo di vita dello sviluppo dovrebbero essere seguite le migliori pratiche, quadri e standard di sviluppo sicuri ben noti e all'avanguardia.	
R.2	Requisiti specifici di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	
R.3	Tecnologie e tecniche specifiche progettate per supportare la privacy e la protezione dei dati (anche denominate Tecnologie per il miglioramento della privacy (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	
R.4	Devono essere seguiti standard e pratiche di codifica sicuri.	
R.5	Durante lo sviluppo, dovrebbero essere eseguiti test e validazione contro l'implementazione dei requisiti di sicurezza iniziali.	
R.6	La valutazione della vulnerabilità, i test di penetrazione di applicazioni e infrastrutture devono essere eseguiti da una terza parte attendibile prima dell'adozione operativa. La domanda non deve essere adottata se non viene raggiunto il livello di sicurezza richiesto.	

R.7	È necessario eseguire periodicamente test di penetrazione.	
R.8	È necessario ottenere informazioni sulle vulnerabilità tecniche dei sistemi di informazione utilizzati.	
R.9	Le patch del software devono essere testate e valutate prima di essere installate in un ambiente operativo.	

Relativo a ISO 27001: 2013 - A.12.6 Gestione delle vulnerabilità tecniche e A.14.2 Sicurezza nei processi di sviluppo e supporto

Cancellazione / smaltimento dei dati

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
S.1	La sovrascrittura basata su software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non sia possibile (CD, DVD, ecc.) Dovrebbe essere eseguita la distruzione fisica.	
S.2	Deve essere eseguita la triturazione della carta e dei supporti portatili utilizzati per archiviare i dati personali.	
S.3	Passaggi multipli di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere eliminati.	
S.4	Se i servizi di una terza parte vengono utilizzati per smaltire in modo sicuro supporti basati su supporti cartacei o cartacei, dovrebbe essere stipulato un contratto di servizio e, se del caso, deve essere prodotto un registro di distruzione dei documenti.	

Relativo a ISO 27001: 2013 - A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento sicuro o riutilizzo delle apparecchiature

Sicurezza fisica

IDENTIFICATORE DI MISURA	DESCRIZIONE DELLA MISURA	LIVELLO DI RISCHIO
T.1	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile a personale non autorizzato.	
T.2	Dovrebbe essere stabilita un'identificazione chiara, mediante mezzi appropriati, ad esempio badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, a seconda dei casi.	
T.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un diario di bordo fisico o una pista di controllo elettronico di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro	

T.4	I sistemi di rilevamento delle intrusioni dovrebbero essere installati in tutte le zone di sicurezza.	
T.5	Eventuali barriere fisiche dovrebbero essere costruite per impedire l'accesso fisico non autorizzato.	
T.6	Le aree sicure libere devono essere bloccate fisicamente e riviste periodicamente	
T.7	Nella sala server dovrebbero essere implementati un sistema automatico di soppressione incendi, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS)	
T.8	Il personale di servizio esterno di supporto alle parti dovrebbe avere accesso limitato alle aree sicure.	

Relativo a ISO 27001: 2013 - A.11 - Sicurezza fisica e ambientale