VALUTAZIONE DEL RISCHIO E MISURA DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI

Valutazione del livello di rischio per le operazioni di trattamento

Il trattamento in esame riguarda la gestione dei dati degli alunni e delle loro famiglie di natura personale, sensibile e giudiziaria con lo scopo di dare corretta esecuzione alla funzione istituzionale svolta dall'Istituzione Scolastica.

e una proposta di adeguate misure tecniche e organizzative di sicurezza.

Sezione I – Definizione e contesto del trattamento

DESCRIZIONE DELL'OPERAZIONE DI TRATTAMENTO	RISPOSTA	
Dati personali trattati	Dati anagrafici, dati di contatto, carriera scolastica, stato occupazionale della famiglia. Dati Particolari: l'origine razziale ed etnica; Le convinzioni religiose, fisiologiche e di altro genere; Lo stato di salute, Assistenza sanitaria: Dati giudiziari se raccolti.	
Finalità del trattamento	Iscrizione e gestione percorso scolastico studenti	
Soggetto dei dati	Alunni, Genitori e Tutori	
Mezzi di trattamento	Trattamento in modalità cartacea e Trattamento in modalità informatica	
Destinatari dei dati personali	Interno	Personale autorizzato al trattamento
	Esterno	Pubblica amministrazione(MI-SIDI) Fornitori di servizi Web, Fornitori Servizi elettronici
Responsabile del trattamento utilizzato	Gruppo Spaggiari spa per Registro Elettronico e Segreteria Digitale Sidi per la gestione degli alunni GWSE per la gestione della formazione digitale Namirial spa per la conservazione documentale	

Sezione II – Valutazione dell'impatto

Valutazione d'impatto sulla riservatezza: Alta
Vengono trattati dati appartenenti a categorie particolari ex art. 9 del GDPR

Valutazione dell'impatto sull'integrità: Media
Dati errati e non aggiornati potrebbero influire sulla valutazione dell'operato di dipendenti e studenti

Valutazione dell'impatto sulla disponibilità: Alta
In caso di perdita e distruzione dei dati, non si potrebbe assicurare il diritto all'istruzione previsto dalla costituzione.

VALUTAZIONE D'IMPATTO		
Riservatezza	**Integrità**	**Disponibilità**
Alto	Medio	Alto
	Valutazione d'impatto globale	Alto

Sezione III – Analisi delle minacce per area di valutazione

Probabilità di minaccia delle risorse tecniche e di rete: bassa

- **Fa parte del trattamento dei dati personali attraverso Internet? Sì**
  Il trattamento utilizza servizi in cloud per la gestione della segreteria digitale, registro elettronico e didattica digitale integrata
- **È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)? Sì**
  L'accesso è effettuato tramite rete locale e rete wifii sicure
- **Il sistema di trattamento dei dati personali è interconnesso a un altro sistema o servizio IT esterno o interno (alla tua organizzazione)? Sì**
  Nella rete sono presenti pc e server, le reti fisiche didattica e segreteria sono separate
- **Le persone non autorizzate possono accedere facilmente all'ambiente di elaborazione dei dati? No**
  Il locale è sorvegliato dagli addetti di segreteria
- **Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori pratiche documentate pertinenti? No**

Processi/Procedure relativi al trattamento dei dati personali probabilità di minaccia: Bassa

- **I ruoli e le responsabilità in relazione al trattamento dei dati personali sono vaghi o non chiaramente definiti? No**
  Viene Mantenuta una organizzazione interna aggiornata
- **L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito? No**
  E' presente un sistema di gestione di protezione dei dati
- **I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali? No**
- **I dipendenti sono autorizzati a trasferire, archiviare o altrimenti elaborare dati personali al di fuori dei locali dell'organizzazione? No**
- **Le attività di trattamento dei dati personali possono essere eseguite senza creare file di log? No**
  Sui sistemi di segreteria digitale e registro elettronico sono presenti i log e il tracciamento delle operazioni

Soggetti/Persone coinvolte nel trattamento dei dati personali probabilità di minaccia: Bassa

- **Il trattamento dei dati personali viene effettuato da un numero indefinito di dipendenti? No**
  Ad ogni persona viene consegnata una lettera di autorizzazione al trattamento
- **Fa parte dell'operazione di trattamento dei dati eseguita da un appaltatore/terza parte (responsabile del trattamento dei dati)? Sì**
- **Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente indicati? No**
- **Il personale coinvolto nel trattamento dei dati personali non ha familiarità con le questioni di sicurezza? No**
- **Le persone/le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali? No**

Settore di attività e scala della probabilità di minaccia di elaborazione : bassa

- **Ritiene che il vostro settore di attività sia soggetto ad attacchi informatici? No**
- **La tua organizzazione ha subito attacchi informatici o altri tipi di violazione della sicurezza negli ultimi due anni? No**
- **Hai ricevuto segnalazioni e/o reclami in merito alla sicurezza del sistema informatico (utilizzato per il trattamento dei dati personali) nell'ultimo anno? No**
- **Il trattamento riguarda un grande volume di persone e/o dati personali? Sì**

AREA DI VALUTAZIONE	PROBABILITÀ	
Rete e risorse tecniche	Basso	1
Processi/Procedure connessi al trattamento dei dati personali	Basso	1
Soggetti/Soggetti coinvolti nel trattamento dei dati personali	Basso	1
Settore di attività **e scala di lavorazione**	Basso	1
Probabilità complessiva di **accadimento della minaccia**	Bassa (4)	

Sezione IV – Valutazione del rischio

	LIVELLO DI IMPATTO			
PROBABILITÀ DI ACCADIMENTO DELLA MINACCIA		Basso	Medio	Alto / Molto Alto
	Basso			X
	Medio			
	Alto			

Sezione V – Misure di sicurezza organizzative

Va notato che l'adeguatezza delle misure a specifici livelli di rischio 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 di misure proposto non tiene conto di altri ulteriori requisiti di sicurezza specifici del settore, nonché di obblighi normativi specifici, derivanti ad esempio dalla direttiva ePrivacy o dalla direttiva NIS. Nel tentativo di facilitare ulteriormente questa procedura , è inclusa ancheuna mappatura del gruppo di misure proposto con i controlli di sicurezza ISO/IEC 27001:2013 .

Politica di sicurezza e procedure per la protezione dei dati personali

Identificatore di misura	Misura Descrizione	Livello di rischio
A.1	L'organizzazione dovrebbe documentare la propria politica relativa al trattamento dei dati personali come parte della propria politica di sicurezza delle informazioni.	ADOTTATA
A.2	La politica di sicurezza dovrebbe essere rivista e rivista, se necessario, su base annuale.	ADOTTATA
R.3	L'organizzazione dovrebbe documentare una politica di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La politica dovrebbe essere approvata dalla direzione e comunicata a tutti i dipendenti e alle parti esterne interessate	ADOTTATA
R.4	La politica di sicurezza dovrebbe fare almeno riferimento a: ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, responsabili del trattamento o altri soggetti terzi coinvolti nel trattamento dei dati personali.	ADOTTATA
R.5	Dovrebbe essere creato e mantenuto un inventario di politiche/procedure specifiche relative alla sicurezza dei dati personali, sulla base della politica di sicurezza generale.	ADOTTATA
R.6	La politica di sicurezza dovrebbe essere rivista e rivista, se necessario, su base semestrale.	ADOTTATA
	Relativo a ISO 27001:2013 - A.5 Politica di sicurezza	

Ruoli e responsabilità

Identificatore di misura	Misura Descrizione	Livello di rischio
B.1	Ruoli e responsabilità relativi al trattamento dei dati personali dovrebbero essere chiaramente definiti e assegnati conformemente alla politica di sicurezza.	ADOTTATA
B.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di rapporto di lavoro, la revoca dei diritti e delle responsabilità con le relative procedure di trasferimento dovrebbe essere chiaramente definita.	
B.3	Dovrebbe essere effettuata una chiara nomina di persone incaricate di specifici compiti di sicurezza, compresa la nomina di un responsabile della sicurezza.	
B.4	Il responsabile della sicurezza dovrebbe essere formalmente nominato (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.	
B.5	I compiti e le aree di responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separati per ridurre le opportunità di modifica non autorizzata o involontaria o uso improprio dei dati personali.	
	Relativo a ISO 27001:2013 - A.6.1.1 Ruoli e responsabilità per la sicurezza delle informazioni	

Politica di controllo degli accessi

Identificatore di misura	Misura Descrizione	Livello di rischio
C.1	A ciascun ruolo (coinvolto nel trattamento dei dati personali) dovrebbero essere assegnati specifici diritti di controllo dell'accesso in base al principio della necessità di conoscere.	ADOTTATA
C.2	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo degli accessi, i diritti di accesso e le restrizioni appropriati per specifici ruoli utente nei confronti dei processi e delle procedure relative ai dati personali.	
C.3	La segregazione dei ruoli di controllo dell'accesso (ad es. richiesta di accesso, autorizzazione all'accesso, amministrazione dell'accesso) dovrebbe essere chiaramente definita e documentata.	
C.4	I ruoli con diritti di accesso eccessivi dovrebbero essere chiaramente definiti e assegnati a un numero limitato di membri specifici del personale.	
	Relativo a ISO 27001:2013 - A.9.1.1 Politica di controllo degli accessi	

Gestione delle risorse/asset

Identificatore di misura	Misura Descrizione	Livello di rischio
D.1	L'organizzazione dovrebbe disporre di un registro delle risorse informatiche utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro potrebbe includere almeno le seguenti informazioni: risorsa informatica, tipo (ad es. server, postazione di lavoro), ubicazione (fisica o elettronica). A una persona specifica dovrebbe essere assegnato il compito di mantenere e aggiornare il registro (ad es. responsabile informatico).	ADOTTATA
D.2	Le risorse IT dovrebbero essere riviste e aggiornate regolarmente.	
D.3	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	
D.4	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.	
	Relativo alla ISO 27001:2013 - A.8 Asset management	

Cambio gestione

Identificatore di misura	Misura Descrizione	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 aver luogo un monitoraggio regolare di questo processo.	ADOTTATA
E.2	Lo sviluppo del software deve essere eseguito in un ambiente speciale non connesso al sistema informatico utilizzato per il trattamento dei dati personali. Quando è necessario il test, dovrebbero essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere messe in atto procedure specifiche per la protezione dei dati personali utilizzati nei test.	
E.3	Dovrebbe essere in atto una politica di cambiamento dettagliata e documentata. Dovrebbe includere: un processo per l'introduzione delle modifiche, i ruoli/utenti che hanno diritti di modifica, tempistiche per l'introduzione delle modifiche. La politica di cambiamento dovrebbe essere regolarmente aggiornata.	
	Relativo alla ISO 27001:2013 - A. 12.1 Procedure operative e responsabilità	

Responsabili del trattamento dei dati

Identificatore di misura	Misura Descrizione	Livello di rischio
F.1	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori/outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento dei dati prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali previsto dalla politica di sicurezza dell'organizzazione.	ADOTTATA
F.2	Alla scoperta di una violazione dei dati personali, il responsabile del trattamento deve informare il responsabile del trattamento senza indebito ritardo.	ADOTTATA
F.3	I requisiti e gli obblighi formali dovrebbero essere formalmente concordati tra il titolare del trattamento e il responsabile del trattamento. Il responsabile del trattamento dei dati dovrebbe fornire sufficienti prove documentate di conformità.	ADOTTATA
F.4	L'organizzazione del titolare del trattamento dovrebbe verificare regolarmente la conformità del responsabile del trattamento al livello concordato di requisiti e obblighi.	ADOTTATA
F.5	I dipendenti del responsabile del trattamento che trattano dati personali dovrebbero essere soggetti a specifici accordi di riservatezza/non divulgazione documentati.	ADOTTATA
	Relativo a ISO 27001:2013 - A.15 Rapporti con i fornitori	

Gestione degli incidenti / Violazioni dei dati personali

Identificatore di misura	Misura Descrizione	Livello di rischio
G.1	Dovrebbe essere definito un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.	ADOTTATA
G.2	Le violazioni dei dati personali devono essere segnalate immediatamente alla direzione. Dovrebbero essere previste procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.	ADOTTATA
G.3	Il piano di risposta agli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	
G.4	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli relativi all'evento e alle successive azioni di mitigazione eseguite.	
	Relativo a ISO 27001:2013 - A.16 Gestione degli incidenti di sicurezza delle informazioni	

Continuità operativa

Identificatore di misura	Misura Descrizione	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 informatico che elabora i dati personali (in caso di incidente/violazione dei dati personali).	ADOTTATA
H.2	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica di sicurezza generale). Dovrebbe includere azioni chiare e assegnazione di ruoli.	
H.3	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	
H.4	Dovrebbe essere nominato personale specifico con la responsabilità, l'autorità e la competenza necessarie per gestire la continuità operativa in caso di incidente/violazione dei dati personali.	
H.5	Dovrebbe essere presa in considerazione una struttura alternativa, a seconda dell'organizzazione e del tempo di inattività accettabile del sistema IT.	
	Relativo a ISO 27001:2013 - A. 17 Aspetti di sicurezza delle informazioni nella gestione della continuità operativa	

Riservatezza del personale

Identificatore di misura	Misura Descrizione	Livello di rischio
Io.1	L'organizzazione dovrebbe garantire che tutti i dipendenti comprendano le proprie responsabilità e obblighi relativi al trattamento dei dati personali. Ruoli e responsabilità dovrebbero essere chiaramente comunicati durante il processo di pre-assunzione e/o di inserimento.	ADOTTATA
Io.2	Prima di assumere le loro funzioni, ai dipendenti dovrebbe essere chiesto di rivedere e concordare la politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e non divulgazione.	
I.3	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).	
	Relativo alla ISO 27001:2013 - A.7 Sicurezza delle risorse umane	

Formazione

Identificatore di misura	Misura Descrizione	Livello di rischio
J.1	L'organizzazione dovrebbe garantire che tutti i dipendenti siano adeguatamente informati sui controlli di sicurezza del sistema informatico che riguardano il loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati sui pertinenti requisiti in materia di protezione dei dati e sugli obblighi giuridici attraverso regolari campagne di sensibilizzazione.	ADOTTATA
J.2	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, inclusi programmatori specifici per l'inserimento (in materia di protezione dei dati) dei nuovi arrivati.	
J.3	Un piano di formazione con scopi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	
	Relativo a ISO 27001:2013 - A.7.2.2 Consapevolezza, istruzione e formazione sulla sicurezza delle informazioni	

Controllo accessi e autenticazione

Identificatore di misura	Misura Descrizione	Livello di rischio
K.1	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema informatico. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	ADOTTATA
K.2	L'uso di account utente comuni dovrebbe essere evitato. Nei casi in cui ciò sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	
K.3	Dovrebbe essere in atto un meccanismo di autenticazione che consenta l'accesso al sistema informatico (basato sulla politica e sul sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione nome utente/password. Le password devono rispettare un certo livello di complessità (configurabile).	
K.4	Il sistema di controllo degli accessi dovrebbe avere la capacità di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	
K.5	È necessario definire e documentare una politica specifica per le password. La politica dovrebbe includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso falliti accettabili.	
K.6	Le password degli utenti devono essere memorizzate in un formato "hash".	
K.7	L'autenticazione a due fattori dovrebbe essere preferibilmente utilizzata per accedere ai sistemi che elaborano dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.	

Identificatore di misura	Misura Descrizione	Livello di rischio
K.8	L'autenticazione del dispositivo dovrebbe essere utilizzata per garantire che il trattamento dei dati personali venga eseguito solo attraverso risorse specifiche nella rete.	
	Relativo a ISO 27001:2013 - A.9 Controllo degli accessi	

Registrazione e monitoraggio

Identificatore di misura	Misura Descrizione	Livello di rischio
L.1	I file di log devono essere attivati per ogni 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 contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi devono essere sincronizzati con un'unica sorgente temporale di riferimento	
L.3	Le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta/eliminazione/ modifica dei diritti dell'utente, devono essere registrate.	
L.4	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Oltre al monitoraggio per il rilevamento di attività insolite, è necessario registrare anche l'accesso ai file di registro.	
L.5	Un sistema di monitoraggio dovrebbe elaborare i file di registro e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	
	Relativo a ISO 27001:2013 - A.12.4 Registrazione e monitoraggio	

Sicurezza del server/database

Identificatore di misura	Misura Descrizione	Livello di rischio
M.1	I server di database e applicazioni devono essere configurati per essere eseguiti utilizzando un account separato, con privilegi minimi del sistema operativo per funzionare correttamente.	
M.2	I database e i server delle applicazioni dovrebbero elaborare solo i dati personali che sono effettivamente necessari per il trattamento al fine di raggiungere gli scopi del trattamento.	
M.3	Le soluzioni di crittografia dovrebbero essere prese in considerazione 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 separando i dati dagli identificatori diretti per evitare il collegamento all'interessato senza ulteriori informazioni	
M.6	Dovrebbero essere prese in considerazione le tecniche che supportano la privacy a livello di database, come query autorizzate, query di database che preservano la privacy, crittografia ricercabile, ecc.	
	Relativo alla ISO 27001:2013 - A. 12 Sicurezza delle operazioni	

Sicurezza della postazione di lavoro

Identificatore di misura	Misura Descrizione	Livello di rischio
N.1	Gli utenti non dovrebbero essere in grado di disattivare o aggirare 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 devono disporre dei privilegi per installare o disattivare applicazioni software non autorizzate.	

Identificatore di misura	Misura Descrizione	Livello di rischio
N.4	Il sistema dovrebbe disporre di timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	
N.5	Gli aggiornamenti di sicurezza critici rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	
N.6	Le applicazioni antivirus e le firme di rilevamento devono essere configurate quotidianamente.	
N.7	Non dovrebbe essere consentito il trasferimento di dati personali dalle postazioni di lavoro a dispositivi di archiviazione esterni (ad es. USB, DVD, dischi rigidi esterni).	
N.8	Le postazioni di lavoro utilizzate per il trattamento dei dati personali non dovrebbero preferibilmente essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali in archivio.	
N.9	La crittografia completa del disco deve essere abilitata sulle unità del sistema operativo della workstation	
	Relativo alla ISO 27001:2013 - A. 14.1 Requisiti di sicurezza dei sistemi informativi	

Sicurezza di rete/comunicazione

Identificatore di misura	Misura Descrizione	Livello di rischio
O.1	Ogni volta che l'accesso avviene tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS/SSL).	
O.2	L'accesso wireless al sistema informatico dovrebbe essere consentito solo a utenti e processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.	
O.3	L'accesso remoto al sistema informatico dovrebbe in generale essere evitato. Nei casi in cui ciò sia 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.	
O.4	Il traffico da e verso il sistema IT dovrebbe essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.	
O.5	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.	
O.6	La rete del sistema informativo dovrebbe essere separata dalle altre reti del titolare del trattamento.	
O.7	L'accesso al sistema informatico dovrebbe essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtraggio MAC o il controllo di accesso alla rete (NAC)	
	Relativo a ISO 27001:2013 - A.13 Sicurezza delle comunicazioni	

Backup

Identificatore di misura	Misura Descrizione	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 fornito un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati ai dati originari.	
P.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	
P.4	I backup completi devono essere eseguiti regolarmente.	

Identificatore di misura	Misura Descrizione	Livello di rischio
P.5	I supporti di backup devono essere testati regolarmente per garantire 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.	
S.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.	
P.9	Le copie dei backup devono essere crittografate e archiviate in modo sicuro anche offline.	
	Rispetto a ISO 27001:2013 - A.12.3 Backup	

Dispositivi mobili/portatili

Identificatore di misura	Misura Descrizione	Livello di rischio
D.1	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	
D.2	I dispositivi mobili che possono accedere al sistema informativo devono essere preregistrati e preautorizzati.	
D.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.	
D.4	Ruoli e responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.	
D.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.	
D.6	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.	
D.7	I dispositivi mobili dovrebbero essere protetti fisicamente contro il furto quando non sono in uso.	
D.8	L'autenticazione a due fattori dovrebbe essere considerata per l'accesso ai dispositivi mobili	
D.9	I dati personali memorizzati sul dispositivo mobile (come parte dell'operazione di elaborazione dei dati dell'organizzazione) devono essere crittografati.	
	Relativo alla ISO 27001:2013 - A. 6.2 Dispositivi mobili e telelavoro	

Sicurezza del ciclo di vita delle applicazioni

Identificatore di misura	Misura Descrizione	Livello di rischio
R.1	Durante il ciclo di vita dello sviluppo dovrebbero essere seguite le migliori pratiche, lo stato dell'arte e le pratiche, i quadri o gli standard di sviluppo sicuri ben riconosciuti.	
R.2	Requisiti di sicurezza specifici 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 (denominate anche tecnologie di miglioramento della privacy (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	
R.4	È necessario seguire gli standard e le pratiche di codifica sicura.	
R.5	Durante lo sviluppo, è necessario eseguire test e convalida rispetto all'implementazione dei requisiti di sicurezza iniziali.	

Identificatore di misura	Misura Descrizione	Livello di rischio
R.6	La valutazione della vulnerabilità, i test di penetrazione delle applicazioni e dell'infrastruttura devono essere eseguiti da una terza parte fidata prima dell'adozione operativa. La domanda non può essere adottata se non viene raggiunto il livello di sicurezza richiesto.	
R.7	Devono essere eseguiti test di penetrazione periodici.	
R.8	È necessario ottenere informazioni sulle vulnerabilità tecniche dei sistemi di informazione utilizzati.	
R.9	Le patch software devono essere testate e valutate prima di essere installate in un ambiente operativo.	
	Relativo a ISO 27001:2013 - A.12.6 Gestione tecnica delle vulnerabilità e A.14.2 Sicurezza nei processi di sviluppo e supporto	

Cancellazione/eliminazione dei dati

Identificatore di misura	Misura Descrizione	Livello di rischio
S.1	La sovrascrittura basata su software deve essere eseguita su tutti i supporti prima del loro smaltimento. Nei casi in cui ciò non sia possibile (CD, DVD, ecc.) deve essere eseguita la distruzione fisica.	
S.2	Verrà effettuata la triturazione della carta e dei supporti portatili utilizzati per conservare i dati personali.	
S.3	È necessario eseguire più passaggi di sovrascrittura basata su software su tutti i supporti prima dello smaltimento.	
S.4	Se i servizi di una terza parte vengono utilizzati per smaltire in modo sicuro i supporti o le registrazioni cartacee, dovrebbe essere in vigore un accordo di servizio e dovrebbe essere prodotto un record di distruzione dei record come appropriato.	
S.5	Dopo la cancellazione del software, è necessario eseguire ulteriori misure basate sull'hardware come la smagnetizzazione. A seconda dei casi, dovrebbe essere considerata anche la distruzione fisica.	
S.6	Qualora per la distruzione di supporti o archivi cartacei ci si avvalga di un soggetto terzo, quindi responsabile del trattamento, si deve ritenere che il trattamento avvenga presso la sede del titolare del trattamento (ed evitare il trasferimento fuori sede dei dati personali.	
	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	Misura Descrizione	Livello di rischio
T.1	Il perimetro fisico dell'infrastruttura del sistema informatico non dovrebbe essere accessibile a personale non autorizzato.	
T.2	Dovrebbe essere stabilita, a seconda dei casi, una chiara identificazione, mediante mezzi appropriati, ad esempio badge identificativi, per tutto il personale ei visitatori che accedono ai locali dell'organizzazione.	
T.3	Le zone sicure dovrebbero essere definite e protette da adeguati controlli di accesso. Un registro fisico o una traccia di controllo elettronica di tutti gli accessi dovrebbe essere mantenuto e monitorato in modo sicuro	
T.4	I sistemi di rilevamento degli intrusi devono essere installati in tutte le zone di sicurezza.	
T.5	Ove applicabile, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	
T.6	Le aree sicure libere devono essere fisicamente chiuse e riviste periodicamente	
T.7	Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere implementati nella sala server	

Identificatore di misura	Misura Descrizione	Livello di rischio
T.8	Al personale del servizio di supporto di parti esterne dovrebbe essere concesso un accesso limitato alle aree sicure.	
	Relativo alla ISO 27001:2013 - A.11 – Sicurezza fisica e ambientale	