Valutazione d’impatto sulla protezione dei dati

DPIA Studio osservazionale ambispettico, no-profit, multicentrico, senza farmaco - Studio "ENDOcancer-DATA"

03/03/2025

Indice

1. Introduzione.....
2. Informazioni essenziali.....
3. Stima del rischio e pre-assessment.....
4. Informazioni sul trattamento.....
5. Valutazione della proporzionalità in relazione alla finalità.....
6. Diritti e principi fondamentali.....
7. Valutazione del rischio.....
    7.1 Misure di sicurezza.....
    7.2 Valutazione del rischio.....
8. Coinvolgimento delle parti interessate.....
9. Note.....

1. Introduzione

Il presente documento “DPIA Studio osservazionale ambispettico, no-profit, multicentrico, senza farmaco - Studio "ENDOcancer-DATA"” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “Studio ENDOcancer-DATA”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

2. Informazioni essenziali

Data di creazione dell’analisi	30/09/2024
Data generazione documento	03/03/2025
Data del prossimo controllo	20/02/2026
Stato	Definitivo
Reporter	Stefania Crivellari ; Alessandra Risso

3. Stima del rischio e pre-assessment

Pre-Assessment

Tipologia del trattamento	Risposta
Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti dell’interessato.	No

Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).	No
Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.	No
Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 Regolamento UE 2016/679 interconnessi con altri dati personali raccolti per finalità diverse.	No
Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).	No
Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).	Sì
Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).	Sì

Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 (criteri WP 29).	No
Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).	No
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	No
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	No
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	Sì

Stima del rischio

Criteri utilizzati per la stima del rischio	Risposta
Il trattamento comporta la valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione	No
Il trattamento prevede un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	No
Il trattamento consiste in un'attività di monitoraggio sistematico	No
Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale	Sì
Il trattamento di dati avviene su larga scala	No

Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	No
Il trattamento coinvolge categorie di interessati vulnerabili	Sì
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	No
Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	No
Elevato	

4. Informazioni sul trattamento

Codice identificativo	Nome	Data di creazione	Data dell'ultima modifica
130	Studio ENDOcancer-DATA	30/09/2024	03/03/2025
Descrizione			

L'obiettivo primario di questo studio nazionale sul carcinoma dell'endometrio è analizzare l'impatto del profilo immuno-molecolare e clinico del tumore dell'endometrio sugli outcome di Disease-Free Survival (DFS) e di Overall Survival (OS), sul tipo e sulla localizzazione di recidiva, sul profilo istopatologico, sulla risposta alla terapia adiuvante e sull'adeguatezza dell'approccio chirurgico scelto.

Verranno quindi riportate e registrate tutte le informazioni epidemiologico-cliniche, istopatologiche e molecolari dei casi di carcinoma diagnosticati e trattati nei centri oncologici di riferimento sul territorio nazionale. Conseguentemente, i dati di tale studio permetteranno di valutare l'impatto nella real-life e in termini di spesa e salute pubblica degli sforzi di prevenzione, di diagnosi e di terapia del carcinoma dell'endometrio, al fine di dare seguito a un processo di standardizzazione e di perfezionamento degli iter diagnostico-terapeutici di tale patologia in Italia.

A seguito della raccolta del consenso informato scritto del paziente, i Titolari tratteranno i seguenti dati personali: dati demografici e dati relativi allo stato di salute.

Per i soli pazienti per cui l'ASL CN2 (Centro sperimentatore) è impossibilitata alla raccolta del consenso (deceduti o non contattabili) verrà applicato l'Art 110 Codice privacy.

I dati saranno inseriti in forma pseudonimizzata sulla piattaforma RedCap messa a disposizione dal Promotore dello studio, la Fondazione Policlinico Universitario A. Gemelli, IRCCS, Roma. Lo sperimentatore principale (Dott. Buda di ASL CN2) riceve dal Promotore, tramite email, le proprie credenziali (utente e password per il primo accesso).

Lo studio avrà l'obiettivo di analizzare 6200 casi in 10 anni di arruolamento. Come da normativa vigente relativa agli studi non farmacologici (Linee guida GCP), i dati saranno conservati per 7 anni dopo la chiusura dello studio.

Finalità del trattamento	
Studio osservazionale retrospettivo e prospettico (ambispettico) sui dati personali pseudonimizzati delle pazienti con diagnosi di carcinoma dell'endometrio diagnosticato e trattato nei centri partecipanti allo studio dal 01/01/2015.	
Basi giuridiche	Articolo 6 a) – l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità
	Articolo 9 a) – l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche

	Articolo 9 j) – il trattamento è necessario a fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89 paragrafo 1 sulla base del diritto dell'Unione o nazionale
Riferimenti normativi	Per i soli pazienti per cui l'ASL CN2 è impossibilitata alla raccolta del consenso (deceduti o non contattabili) verrà applicato l'Art 110 Codice privacy (ricerca epidemiologica che non consente la raccolta del consenso in quanto impossibile o implica uno sforzo sproporzionato nel raccoglierlo) in combinato disposto art. 9 par. 2 l. J)

Origine dei dati	
Raccolti presso l'interessato	
Modalità del trattamento	
Cartaceo	Informatizzato

Categorie di dati	
Dati personali comuni	Dati identificativi
Categorie particolari di dati personali	Dati relativi alla salute
	Informazioni risultanti da genetica
Categorie di interessati	
Assistiti	

Titolare	ASL CN 2
Contitolari	Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Responsabile della protezione dei dati	Studio Legale Associato LCG Lecis Cannella Grassi ; Giuseppe Cannella
Diffusione	Non viene effettuata la diffusione dei dati.
Trasferimenti e comunicazioni di dati	
Il trattamento prevede il trasferimento o la comunicazione di dati	

Trasferimenti e comunicazioni di dati		
Ambito	**Destinatari**	**Note sui trasferimenti**
Intra-UE	Il progetto prevede la creazione di un sistema di raccolta e gestione dati elettronico attraverso la piattaforma REDcap. Tale database raccoglierà i dati di tutte le pazienti con diagnosi di carcinoma dell'endometrio diagnosticato e trattato nei centri partecipanti alllo studio. Il software prescelto sarà utilizzato per la raccolta prospettica della casistica, nonché per l'integrazione con una banca dati retrospettiva relativa al periodo dal 1 gennaio 2015. Si precisa inoltre che essendo tale raccolta dati anonima, l'estrazione dei dati non prevederà alcuna misura l'identificazione del soggetto.	I dati saranno inseriti sulla piattaforma RedCap messa a disposizione dal Promotore dello studio, la Fondazione Policlinico Universitario A. Gemelli, IRCCS, Roma. L'utente del centro sperimentatore riceve dal Promotore, tramite email, le proprie credenziali (utente e password per il primo accesso). Al primo accesso la password deve necessariamente essere modificata.
Ambito	**Destinatari**	**Note sui trasferimenti**
Intra-UE	Altri organismi ; Fondazione Policlinico Universitario Agostino Gemelli IRCCS	Trasferimento di dati pseudonimizzati

Periodo di conservazione dei dati personali	
7 anni - Studi osservazionali non farmacologici	
Descrizione del periodo di conservazione dei dati	Come da normativa vigente relativa agli studi non farmacologici (Linee guida GCP). Lo Studio prevede la raccolta dei dati per 10 anni. Al termine di tale periodo, i dati verranno conservati per ulteriori 7 anni.
Applicativi	RedCap
Note	
I dati raccolti verranno riportati sulla piattaforma RedCap messa a disposizione dal Promotore, il cui accesso, protetto da password, è consentito al solo Sperimentatore Principale o a persone da lui designate per il data entry. I dati inseriti non conterranno informazioni che possano identificare le pazienti, ma saranno pseudononimizzati e verrà mantenuto il “site patient log” in formato cartaceo, conservato a parte, dovutamente archiviato e protetto.	

Descrizione sistematica delle componenti del trattamento

Descrizione delle diverse componenti tecnologiche, fisiche ed organizzative che partecipano dell’attività di trattamento valutata.

Componenti organizzative

Componente	Descrizione
Soggetti Interni	**Descrizione sintetica (es. soggetti facenti parte o meno del personale tecnico informatico, descrizione delle attività svolte in relazione ai trattamenti in esame, formazione ricevuta, procedure che ne disciplinano le mansioni, relazioni con altre componenti**
	Soggetti autorizzati al trattamento dei dati da parte dello Sperimentatore Principale (Dott. Alessandro Antonio Buda - SC Ostetricia e Ginecologia e Ginecologia Oncologica - ASL CN2)
Soggetti Esterni	**Descrizione sintetica (es. caratteristiche del servizio erogato o del titolo che giustifica il coinvolgimento di tale soggetto, presenza di un accordo sul trattamento di dati, relazioni con altre componenti)**

	Promotore dello studio: Fondazione Policlinico Universitario A. Gemelli, IRCCS, Roma

Componenti tecnologiche

Componente	Descrizione
Applicazioni	**Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)**
	RedCap
Infrastrutture IT	**Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)**
	Repository aziendale
Rete	**Descrizione sintetica (es. tipologia di rete, tecnologie utilizzate, relazioni con altre componenti)**
	Rete aziendale

Componenti fisiche

Componente	Descrizione
Risorse ed asset materiali	**Descrizione (es. principali caratteristiche, tipologia di asset non latamente inteso come informatico, relazioni con altre componenti)**
	Faldoni di studio per archiviazione della documentazione completa.
Sedi fisiche	**Descrizione (es. ubicazione delle sedi anche distaccate o periferiche, principale utilizzo, relazioni con altre componenti)**
	Locali aziendali del Presidio Ospedaliero Michele e Pietro Ferrero di Verduno

5. Valutazione della proporzionalità in relazione alla finalità

Tenuto conto che l'attività di trattamento sottoposta a valutazione comporta il trattamento delle categorie di dati personali sopra menzionati, in relazione alle categorie di interessati precedentemente citati, il titolare ritiene che dette categorie di dati siano necessarie e proporzionali al perseguimento della finalità:

Studio osservazionale retrospettivo e prospettico (ambispettico) sui dati personali pseudonimizzati delle pazienti con diagnosi di carcinoma dell'endometrio diagnosticato e trattato nei centri partecipanti allo studio dal 01/01/2015.

6. Diritti e principi fondamentali

Diritti

Accesso	In relazione al trattamento dei dati personali degli interessati, il Capo III del Regolamento UE 2016/679 riconosce specifici diritti ai soggetti reclutati e, in particolare, il diritto, se applicabile, di accedere ai dati personali e alle informazioni relative agli stessi
Rettifica	In relazione al trattamento dei dati personali degli interessati, il Capo III del Regolamento UE 2016/679 riconosce specifici diritti ai soggetti reclutati e, in particolare, il diritto, se applicabile, di chiedere l'aggiornamento, la rettifica dei dati inesatti e l'integrazione di quelli incompleti. I soggetti coinvolti possono esercitare i loro diritti di rettifica.
Cancellazione	In relazione al trattamento dei dati personali degli interessati, il Capo III del Regolamento UE 2016/679 riconosce specifici diritti ai soggetti reclutati e, in particolare, il diritto, se applicabile, di chiedere la cancellazione dei dati personali che lo riguardano al verificarsi di una delle condizioni indicate all'art. 17, paragrafo 1 del GDPR e nel rispetto delle eccezioni previste al paragrafo 3 del medesimo articolo e purché non sussistano obblighi di conservazione del dato previsti dalla legge. I soggetti coinvolti possono esercitare i loro diritti di cancellazione.
Portabilità	Il diritto alla portabilità non è applicabile poiché i mezzi non sono automatizzati.

Opposizione	Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.
Limitazione di trattamento	L'interessato può imporre al titolare del trattamento una restrizione al trattamento dei dati (es. laddove siano previste più finalità l'interessato può limitare il trattamento soltanto ad alcune di queste).
Revoca del consenso	Il soggetto può rifiutarsi di partecipare o ritirarsi dallo studio, in qualsiasi momento, senza pregiudicarne le cure future. Si precisa, tuttavia, che non sarà possibile rimuovere le informazioni personali già elaborate per lo Studio prima della revoca.
Diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato	Non sono previsti trattamenti automatizzati.

Principi

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato	La raccolta dei dati verrà effettuata dalle cartelle cliniche cartacee, dalla diaria del paziente (effettuata durante i ricoveri) e dalle visite/esami già disponibili. La registrazione, conservazione e modificazione dei dati personali avverrà attraverso strumenti manuali e informatici con logiche strettamente correlate alle finalità indicate dallo studio. I dati verranno trattati con modalità atte a garantire la riservatezza e la sicurezza delle informazioni, ai sensi degli artt. 25 e 32 del GDPR. Tutte le operazioni in materia, effettuate solo da personale debitamente istruito e autorizzato dal Titolare o suo delegato, avverranno nel rispetto del segreto professionale, del segreto d'ufficio e dei principi di Liceità, Correttezza e Trasparenza, secondo quanto disposto dalla normativa vigente.

I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità	I dati saranno raccolti per finalità di ricerca scientifica, come descritto nel foglio informativo per il paziente.
I dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati	I dati personali raccolti nell'ambito di questo studio verranno conservati presso i locali aziendali dell'ASL CN2 ad accesso riservato ai soli soggetti autorizzati, per un periodo di 7 anni (come da normativa vigente) dopo la conclusione della Sperimentazione o per un periodo più lungo, se necessario, nel rispetto degli obblighi di legge, cui è tenuto il Titolare.
I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali	I dati identificativi del soggetto arruolato verranno sottoposti a pseudonimizzazione con codice univoco. I dati dello studio verranno raccolti sulla piattaforma RedCap messa a disposizione dal Promotore dello studio. Contemporaneamente verrà creato un ulteriore foglio (database anagrafico) che conterrà la corrispondenza tra codice univoco e dati identificativi del soggetto, che verrà salvato protetto da password, nonché stampato e conservato in armadio chiuso presso il titolare del centro sperimentatore.

7. Valutazione del rischio

Al fine di calcolare la magnitudo di un rischio e si adotta una formula del tipo

$R_1 = f(M, p)$

IMPATTO (M)	
LIEVE	1
MEDIO	2
ALTO	3
ALTISSIMO	4

X

PROBABILITÀ (p)

IMPROBABILE	1
POCO PROBABILE	2
PROBABILE	3
ALTAMENTE PROBABILE	4

=

RISCHIO INIZIALE (R)

BASSO	1 - 2
MEDIO	3 - 4
ALTO	5 - 8
ALTISSIMO	9 - 16

Dove per:

- **R** si intende il livello di rischio non mitigato;
- **M** si intende l'impatto per i diritti e le libertà degli interessati che viene indicato assegnando un valore da uno a quattro secondo la seguente scala:

Lieve	Gli interessati non saranno coinvolti o nella peggiore delle ipotesi potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema.
Medio	Gli interessati potrebbero incontrare degli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà
Grave	Gli interessati potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di far fronte seppur con gravi difficoltà
Gravissimo	Gli interessati potrebbero confrontarsi con conseguenze significative o irreversibili.

- **p** si intende la probabilità di accadimento del rischio che viene indicata assegnando un valore da uno a quattro secondo la seguente scala:

Improbabile	L'avverarsi della minaccia non sembra possibile
Poco Probabile	L'avverarsi della minaccia sembra difficile
Probabile	L'avverarsi della minaccia sembra possibile
Altamente Probabile	L'avverarsi della minaccia sembra probabile

Un controllo o misura di sicurezza può agire sulla probabilità o l'impatto (o su entrambi) di una minaccia secondo la seguente logica:

$$R_2 = R_1 - (M_n)$$

dove per:

- R_2 si intende il rischio finale, ovverosia il rischio a valle dell'inserimento dei controlli o misure di sicurezza;
- R_1 si intende il rischio iniziale come definito più sopra;
- M_n si intende il controllo o la misura di sicurezza.

All'interno del presente passaggio saranno presenti, in ordine

1. l'elenco di misure di sicurezza, suddivise in misure associate in via diretta all'attività di trattamento (misure di sicurezza c.d. "su trattamenti") ed in misure associate ad un asset (misure di sicurezza su "componenti IT", "applicativi" e "luoghi fisici") correlato a propria volta all'attività di trattamento;
2. l'elenco delle minacce comprensivo di: nome assegnato alla minaccia, fonte del rischio (la quale può essere, anche cumulativamente, umana se relativa a soggetti appartenenti all'organizzazione di colui che effettua la valutazione d'impatto, di contesto se relativa a soggetti non appartenenti all'organizzazione del soggetto che effettua la valutazione d'impatto, afferente a strumenti se correlata a malfunzionamenti di strumentazione anche se dipendenti da eventi esterni quali disastri naturali), area di impatto (disponibilità, integrità, riservatezza, anche cumulativamente), valori relativi ad impatto e probabilità (con eventuale motivazione sulle scelte effettuate) e valore specifico del rischio non mitigato;
3. i controlli o misure di sicurezza adottate o valutate nonché la loro incidenza su impatto e probabilità della minaccia.

   https://doc.privacymanager.eu/manuale/valutazione_impatto.html#mitigazione-del-rischio-iniziale-valore-minore
4. Rischio residuo (mitigato).

7.1 Misure di sicurezza

Misure di sicurezza trasversali relative ai trattamenti

Categoria	Misura di sicurezza	Stato di adozione e implementazione

Protezione dei Dati	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata I documenti cartacei contenenti dati personali sono conservati in locale chiuso a chiave e ad accesso riservato al solo personale autorizzato

Misure di sicurezza trasversali relative agli asset

Categoria	Misura di sicurezza	Stato di adozione e implementazione
Misure di sicurezza correlate con i luoghi fisici		
Protezione dei Dati	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata I documenti cartacei contenenti dati personali sono conservati in locale chiuso a chiave e ad accesso riservato al solo personale autorizzato

Misure di sicurezza specifiche relative al trattamento

Categoria	Misura	Stato di adozione e implementazione
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	Applicata
	Le chiavi private sono adeguatamente protette	Applicata
	Formazione relativa alla cifratura	Applicata

Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	Applicata
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata
Politiche, regolamenti e manuali	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata

Misure di sicurezza specifiche relative agli asset correlati con il trattamento

Nessun elemento selezionato

7.2 Valutazione del rischio

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Malfunzionamento o distruzione di strumentazione it (client)	Hardware e Software	Disponibilità ; Riservatezza ; Integrità	Strumenti
Descrizione			
Hardware e software			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%

Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%

	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%

Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%

	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
100%		100%	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Malfunzionamento o distruzione di strumentazione it (server)	Hardware e Software	Disponibilità ; Riservatezza ; Integrità	Strumenti
Descrizione			
Hardware e software			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%

	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%

	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%

	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%

Elemento	Valore finale numerico	Valore finale
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
100%	100%	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Malfunzionamento o distruzione di strumentazione it (rete)	Hardware e Software	Disponibilità ; Riservatezza ; Integrità	Strumenti
Descrizione			
Hardware e software			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%

	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%

	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%

	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%

Elemento	Valore finale numerico	Valore finale
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
100%	100%	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Distruzione o furto di strumentazione	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Uso non autorizzato della strumentazione	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano
Descrizione			
Incluso accesso non autorizzato alla rete			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%

	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%

	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%

	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%

Elemento	Valore finale numerico	Valore finale
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
100%	100%	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Divulgazione accidentale di informazioni	Comportamenti umani	Riservatezza	Umano
Descrizione			
Anche da parte dei dipendenti			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%

	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%

	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%

	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%

Elemento	Valore finale numerico	Valore finale
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
100%	100%	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Infezioni da virus, malware	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Allagamento	Eventi naturali	Disponibilità	Contesto
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Incendio	Eventi naturali	Disponibilità	Contesto
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Terremoti, eruzioni vulcaniche	Eventi naturali	Disponibilità	Contesto
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Danno per la reputazione	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Discriminazione	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Furto d'identità	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Danni fisici o psicologici	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Perdita di controllo dei dati	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Accesso illegittimo ai dati	CNIL	Riservatezza	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Modifiche indesiderate dei dati	CNIL	Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Perdita di dati	CNIL	Disponibilità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	100%	100%
	Le chiavi private sono adeguatamente protette	100%	100%
	Formazione relativa alla cifratura	100%	100%
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%

Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	100%	100%
	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	100%	100%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	100%	100%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%

Politiche, regolamenti e manuali	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure per garantire la minimizzazione dei dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%

	Sono in vigore procedure minimizzare la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Conservazione in locale ad accesso riservato chiuso a chiave	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Riassunto ed esito dell'analisi del rischio

Minaccia	Rischio iniziale	Rischio residuo
Malfunzionamento o distruzione di strumentazione it (client)	1	1
Malfunzionamento o distruzione di strumentazione it (server)	1	1
Malfunzionamento o distruzione di strumentazione it (rete)	1	1
Distruzione o furto di strumentazione	1	1
Uso non autorizzato della strumentazione	1	1
Divulgazione accidentale di informazioni	1	1
Infezioni da virus, malware	1	1
Allagamento	1	1
Incendio	1	1
Terremoti, eruzioni vulcaniche	1	1
Danno per la reputazione	1	1
Discriminazione	1	1
Furto d'identità	1	1
Danni fisici o psicologici	1	1
Perdita di controllo dei dati	1	1

Accesso illegittimo ai dati	1	1
Modifiche indesiderate dei dati	1	1
Perdita di dati	1	1

Livello di rischio complessivo per area

Area di impatto	**Livello di rischio**
Disponibilità	Basso
Riservatezza	Basso
Integrità	Basso

Livello di rischio complessivo residuo

Basso
Considerazioni sul rischio finale
Il Trattamento dei dati personali avviene comunque all'interno del perimetro aziendale applicando le dovute misure di sicurezza tecniche, nonché organizzative.

8. Coinvolgimento delle parti interessate

Domanda	**Risposta**
Sono state raccolte le opinioni degli interessati o dei loro rappresentanti?	Sì

Gli interessati verranno coinvolti a partecipare mediante il consenso informato allo studio, somministrato in occasione della prima visita utile. Verrrà inoltre fornita apposita informativa privacy contenente apposito modulo per la raccolta del consenso al trattamento dei dati. Per i soli pazienti per cui l'ASL CN2 è impossibilitata alla raccolta del consenso (deceduti o non contattabili) verrà applicato l'Art 110 Codice privacy (ricerca epidemiologica che non consente la raccolta del consenso in quanto impossibile o implica uno sforzo sproporzionato nel raccoglierlo) in combinato disposto art. 9 par. 2 l. J)

È stato coinvolto il Responsabile della Protezione dei Dati?	Sì
Sì	

9. Note

Il Titolare del trattamento

ASL CN 2