ASL CN2

ASL CN 2
12051
Via Vida 10
ALBA

C.F.- P.IVA 02419170044

t. 0172-1408040
F.----------
W. https://www.aslcn2.it
aslcn2@legalmail.it

Valutazione d’impatto sulla protezione dei dati

Valutazione d’impatto - 182 - ESCAPE

11/02/2026

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 “Valutazione d’impatto - 182 - ESCAPE” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “ESCAPE”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

2. Informazioni essenziali

Data di creazione dell’analisi	09/02/2026
Data generazione documento	11/02/2026
Data del prossimo controllo	07/02/2027
Stato	In attesa di revisione
Reporter	Chiara Grasso

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.	Sì
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).	No
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.	No

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
182	ESCAPE	09/02/2026	11/02/2026

Descrizione

L'osteoartrite del ginocchio, o gonartrosi, è una condizione piuttosto comune nella popolazione anziana. È una malattia degenerativa delle articolazioni di origine multifattoriale, risultante da un'usura progressiva e un danno della cartilagine articolare. La protesi totale di ginocchio (PTG) rappresenta il trattamento più efficace per il trattamento della gonartrosi di grado severo e sintomatica; in particolar modo, la più recente protesi bicruciate retaining (BCR) a conservazione di entrambi i legamenti crociati può rappresentare una soluzione efficace per ripristinare una cinematica del ginocchio il più possibile fisiologica, e superare l'insoddisfazione dei pazienti segnalata dopo l'impianto protesico. Inoltre, tale protesi ha mostrato tassi di sopravvivenza a lungo termine dell'impianto piuttosto elevati.

La protesi S&N Journey II XR (Smith & Nephew, Inc.; Memphis, TN, USA) rappresenta una delle soluzioni più avanzate nel campo delle protesi BCR di seconda generazione. Questa protesi è stata progettata con l'obiettivo di replicare il più fedelmente possibile la cinematica naturale del ginocchio, combinando un design anatomico con tecnologie all'avanguardia, superando così i limiti dei precedenti impianti BCR e riducendo così il tasso di complicanze e revisioni.

Attualmente, in letteratura esistono ancora pochi studi nei quali è stata indagata nel dettaglio la sopravvivenza post-intervento della protesi Journey II XR, ma con un follow-up di soli due anni. In tali lavori, la sopravvivenza della protesi è intesa in relazione all'esecuzione o meno della revisione dell'impianto o la rimozione di un qualsiasi componente del dispositivo durante il follow-up, ed è stata stimata pari al 96.2 e al 97,9% ai due anni post-intervento. Gli unici due lavori che hanno esplorato il tasso di revisione con un follow-up più esteso (5 anni), senza tuttavia specificare nel dettaglio le caratteristiche della protesi utilizzata, riportano un tasso di sopravvivenza pari rispettivamente al 95% e al 98.4%

Considerato che l'impianto S&N Journey II XR è l'unica protesi a preservazione dei crociati attualmente in uso presso la Struttura Complessa (SC) di Ortopedia e Chirurgia Protesica dell'Ospedale Michele e Pietro Ferrero di Verduno, ASL CN2 e che presso lo stesso Centro sono seguiti pazienti che hanno eseguito l'intervento di artroplastica presso altri centri ma con lo stesso tipo di protesi, la raccolta di informazioni derivanti dalle visite di controllo di questi pazienti permetterebbe di incrementare le evidenze di letteratura.

L'obiettivo generale dello studio è condurre un'indagine retrospettiva su una coorte di pazienti affetti da gonartrosi che, nel periodo compreso tra il gennaio 2018 e marzo 2021, sono stati sottoposti ad intervento di

protesi di ginocchio con l'impianto S&N BCR Journey II XR senza l'utilizzo di assistenza robotica, e che poi hanno effettuato almeno una visita ortopedica di controllo presso la SC Ortopedia e Chirurgia Protesica dell'Ospedale Michele e Pietro Ferrero di Verduno, ASL CN2. Nello specifico, l'obiettivo primario consiste nel valutare la longevità dell'impianto protesico BCR monitorando la probabilità di sopravvivenza priva di revisioni a 5 anni dall'intervento.

Valutazioni secondarie prevedono:

• valutare la longevità dell'impianto protesico BCR fino alla massima durata osservata (massimo 8 anni);

• valutare la variazione dei punteggi ottenuti dai PROMs (KSS, WOMAC, FJS), somministrati da pratica clinica durante le visite di follow-up rispetto ai punteggi ottenuti con gli stessi questionari immediatamente prima dell'intervento di artroplastica, ove disponibili;

• valutazione del grado di correlazione tra i diversi punteggi ottenuti tra i diversi questionari all'interno di ciascuna visita di follow-up;

• valutare la longevità dell'impianto protesico BCR monitorando la percentuale di revisioni di protesi effettuate entro i 5 anni successivi all'intervento confrontando il sottogruppo di pazienti con allineamento parafisiologico marcato dell'arto vs i pazienti con allineamento fisiologico dell'arto;

• stimare l'incidenza cumulativa e la tipologia di complicanze minori protesi-correlate entro 5 anni dall'intervento di artroplastica.

Lo studio è osservazionale di coorte retrospettivo no profit, il Promotore è la Struttura Complessa di Ortopedia e Chirurgia Protesica dell'Ospedale Michele e Pietro Ferrero di Verduno, ASL CN2.

Lo studio prevede l'arruolamento di una coorte di 50-60 pazienti maggiorenni di entrambi i sessi, che nel periodo compreso tra gennaio 2018 e gennaio 2021 sono stati sottoposti a intervento di protesi totale di ginocchio BCR con impianto S&N Journey II XR, e che poi hanno effettuato almeno una visita di follow-up post-operatorio presso la SC Ortopedia e Chirurgia Protesica dell'Ospedale Michele e Pietro Ferrero di Verduno, ASL CN2. Ai pazienti eleggibili e che risultano vivi e contattabili al momento dell'arruolamento lo Sperimentatore Principale o suoi delegati illustrerà il disegno dello studio, e verrà richiesta la firma sul consenso informato specifico per lo studio.

Tutte le informazioni che saranno raccolte ai fini del presente studio saranno ricavate dalle cartelle relative all'intervento di protesica, incluse le cartelle inerenti agli eventuali successivi ricoveri per il trattamento delle complicanze nel post – operatorio, e dai referti ambulatoriali delle visite ortopediche di controllo. Nel caso in

cui l'intervento di protesica (o l'eventuale intervento di revisione) sia stato eseguito in un altro Centro italiano differente dalla SC Ortopedia e Chirurgia Protesica dell'ASL CN2, i dati necessari per l'esecuzione dello studio verranno recuperati dalla documentazione in possesso dal paziente, e da questi fornita al Centro ASL CN2 in occasione delle visite di follow-up.

I dati demografici e clinici necessari per perseguire gli obiettivi dello studio sono elencati di seguito.

Dati demografici come nome, cognome, data e luogo di nascita, età all'intervento, età al reclutamento, sesso, stato in vita al follow-up;

Dati clinici come: indice di massa corporea (BMI) al momento dell'intervento, comorbilità al momento dell'intervento, lato dell'intervento (destro o sinistro), durata dell'intervento, numero e tipologia di complicanze insorte nel post-operatorio e durante il follow-up, esito delle complicanze (es. revisione della protesi);

Dati radiografici: dati ottenuti dalle radiografie pre- e post-operatorie. Verranno estrapolati dati come l'allineamento meccanico (HKA – Hip-Knee-Ankle) pre- e postoperatorio, lo stato articolare preoperatorio, la deformità articolare preoperatoria, la pendenza del piatto tibiale, o slope, nel pre- e post-operatorio;

Score clinici dei PROMs: score finali dei questionari PROMs utilizzati ai fini del presente studio, somministrati nel preoperatorio e nelle varie visite di follow-up. Saranno raccolti gli score definitivi dei questionari KSS, WOMAC, FJS, quest'ultimo raccolto solo nel post-operatorio.

I dati raccolti dalle cartelle cliniche di ricovero e dalle relazioni delle visite di follow-up saranno trasferiti in maniera pseudonimizzata in un database appositamente creato per lo studio attraverso una scheda di raccolta dati protetta da password costruita sull'applicativo REDCap aziendale. Solo lo Sperimentatore Principale ASL CN2 (Dott. ssa Galletta SC Ortopedia e Chirurgia Protesica) e il personale da lei autorizzato potranno accedere al database con propria username e password. All'interno del database non verranno inseriti dati identificativi propri dei pazienti, ma verranno registrati con un codice. Il trattamento di pseudonimizzazione verrà effettuato su documento cartaceo custodito nei faldoni di studio. Solo lo Sperimentatore Principale e il personale da lei autorizzato potranno risalire all'identità del soggetto.

Lo studio ha l'obiettivo di reclutare 50-60 casi in circa 1 mese di arruolamento. I dati saranno conservati per 7 anni dopo la chiusura dello studio.

Finalità del trattamento

Studio osservazionale retrospettivo monocentrico sui dati personali pseudonimizzati di pazienti maggiorenni di entrambi i sessi affetti da gonartrosi che, nel periodo compreso tra il gennaio 2018 e marzo 2021, sono stati sottoposti ad intervento di protesi di ginocchio con l'impianto S&N BCR Journey II XR senza l'utilizzo di assistenza robotica, e che poi hanno effettuato almeno una visita ortopedica di controllo presso la SC Ortopedia e Chirurgia Protesica dell'Ospedale Michele e Pietro Ferrero di Verduno, ASL CN2.	
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	
Origine dei dati	
Raccolti presso l'interessato	
Dati già raccolti (Cartelle cliniche di ricovero ospedaliero; relazioni di visite ambulatoriali; referti di esami specialistici)	
Modalità del trattamento	
Cartaceo	Informatizzato
Categorie di dati	
Dati personali comuni	
Dati identificativi	
Categorie particolari di dati personali	
Dati relativi alla salute	
Categorie di interessati	Assistiti
Titolare	ASL CN 2
Responsabile della protezione dei dati	Studio Legale Associato LCG Lecis Cannella Grassi ; Giuseppe Cannella
Diffusione dei dati	Non viene effettuata la diffusione dei dati.
Trasferimenti e comunicazioni dei dati	

Non si effettua il trasferimento o la comunicazione dei dati	
Periodo di conservazione dei dati personali	7 anni
Descrizione del periodo di conservazione dei dati	
Lo Studio prevede la raccolta dei dati per circa 1 mese, e due mesi ulteriori per analisi dei dati e stesura del report. Alla chiusura dello studio, i dati verranno conservati per ulteriori 7 anni.	
Applicativi	RedCap
Note	
I dati raccolti sono pseudonimizzati su supporto cartaceo ("site patient log"). I dati pseudonimizzati sono riportati sulla CRF (scheda raccolta dati) elettronica REDCAP, il cui accesso, protetto da username e password, è consentito al solo Sperimentatore Principale o a persone da lei designate per il data entry. Il “site patient log” in formato cartaceo è conservato a parte nell'Investigator Site Folder, dovutamente archiviato e protetto presso i locali della ASL CN2.	

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. ssa Claudia Galletta - SC Ortopedia e Chirurgia Protesica, Ospedale Michele e Pietro Ferrero, Verduno - 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)**
	non presenti

Componenti tecnologiche

Componente	Descrizione
Applicazioni	**Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)**
	Piattaforma RedCap, una piattaforma web che permette di progettare, costruire e mettere in opera, in tempi rapidi, database per la raccolta strutturata dei dati e surveys. È un sistema elettronico altamente sicuro, conforme alle normative vigenti in materia di studi clinici e privacy. La piattaforma dispone di una traccia di controllo (logging), pertanto tutte le modifiche sono registrate e tracciate elettronicamente, è protetta contro l'accesso non autorizzato e consente di creare profilazioni diverse con diritti di accesso diversificati (profilazioni in modalità di scrittura o di sola lettura). Inoltre, è regolarmente sottoposta a backup automatico. L'interfaccia web consente di gestire la qualità del dato grazie a scelte singole o multiple e menù a tendina configurando il sistema in modo da minimizzare gli errori nel data entry (formato delle celle, ranges di normalità, dati obbligatori, etc.…). I reports realizzati o l'intero database nel quale verranno memorizzati i dati possono essere esportati in Excel o nei formati compatibili ai principali pacchetti di statistica (SPSS, SAS, Stata, R). Possono inoltre essere costruiti calendari di progetto e reporting tools. Per ulteriori informazioni: https://www.project-redcap.org/.
Infrastrutture IT	**Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)**
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 monocentrico sui dati personali pseudonimizzati di pazienti maggiorenni di entrambi i sessi affetti da gonartrosi che, nel periodo compreso tra il gennaio 2018 e marzo 2021, sono stati sottoposti ad intervento di protesi di ginocchio con l'impianto S&N BCR Journey II XR senza l'utilizzo di assistenza robotica, e che poi hanno effettuato almeno una visita ortopedica di controllo presso la SC Ortopedia e Chirurgia Protesica dell'Ospedale Michele e Pietro Ferrero di Verduno, ASL CN2.

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 per tale attività di trattamento.
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 di controllo effettuati durante il follow-up 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 dopo la conclusione dello studio 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. La pseudonimizzazione verrà effettuata su un documento cartaceo (database anagrafico o "site patient log"). Tale documento conterrà la corrispondenza tra codice univoco e dati identificativi del soggetto, verrà conservato nei faldoni di studio in armadio chiuso a chiave presso il Titolare. Solo lo Sperimentatore e staff da lei delegato saranno in grado di collegare il codice ai dati identificativi del soggetto. I dati necessari allo studio verranno raccolti in forma pseudonimizzata sul database REDCAP, protetto da password univoca.

ASL CN 2
12051
Via Vida 10
ALBA

C.F.- P.IVA 02419170044

t. 0172-1408040
F.----------
W. https://www.aslcn2.it
aslcn2@legalmail.it

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-qualitativa-con-rischio-residuo-libero
4. Rischio residuo (mitigato).

7.1 Misure di sicurezza

Misure di sicurezza trasversali relative ai trattamenti

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

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	Le chiavi private sono adeguatamente protette	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 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
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata
	Formazione relativa al processo/applicativo in esame	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**
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	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

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	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

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	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

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		2	Poco probabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata

	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata

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

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

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	2	Basso

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		2	Poco probabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata

	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata

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

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

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	2	Basso

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		2	Poco probabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata

	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata

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

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

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	2	Basso

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso

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	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso

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		2	Poco probabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Accesso illegittimo ai dati	CNIL	Riservatezza	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso

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	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Perdita di dati	CNIL	Disponibilità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso

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	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		2	Basso

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	Le chiavi private sono adeguatamente protette	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata	Applicata
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata	Applicata

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata	Applicata
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata

	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata	Applicata
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata	Applicata
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso

Riassunto ed esito dell'analisi del rischio

Minaccia	Rischio iniziale	Rischio residuo
Allagamento	1	1
Incendio	1	1
Terremoti, eruzioni vulcaniche	1	1
Malfunzionamento o distruzione di strumentazione it (client)	2	2
Malfunzionamento o distruzione di strumentazione it (server)	2	2
Malfunzionamento o distruzione di strumentazione it (rete)	2	2
Distruzione o furto di strumentazione	4	2
Uso non autorizzato della strumentazione	1	1
Divulgazione accidentale di informazioni	4	2
Infezioni da virus, malware	2	1
Accesso illegittimo ai dati	4	2
Modifiche indesiderate dei dati	1	1
Perdita di dati	4	2
Danno per la reputazione	4	2
Discriminazione	4	2
Furto d'identità	1	1
Danni fisici o psicologici	4	2
Perdita di controllo dei 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

8. Coinvolgimento delle parti interessate

Domanda	Risposta
Sono state raccolte le opinioni degli interessati o dei loro rappresentanti?	Sì
no	
È stato coinvolto il Responsabile della Protezione dei Dati?	Sì
si	

9. Note

Il Titolare del trattamento

ASL CN 2