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 - 184 - OTTIMIZZAZIONE DELLA RETE EMERGENZA-URGENZA

17/09/2026

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 - 184 - OTTIMIZZAZIONE DELLA RETE EMERGENZA-URGENZA” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “OTTIMIZZAZIONE DELLA RETE EMERGENZA-URGENZA”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

2. Informazioni essenziali

Data di creazione dell’analisi	24/02/2026
Data generazione documento	17/09/2026
Data del prossimo controllo	17/09/2027
Stato	Definitivo
Reporter	Manuela Alessio

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).	Sì

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.	Sì
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).	Sì
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).	Sì

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	Sì
Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	Sì
Il trattamento coinvolge categorie di interessati vulnerabili	Sì
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	Sì
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
184	OTTIMIZZAZIONE DELLA RETE EMERGENZA-URGENZA	23/02/2026	10/08/2026

Descrizione

Il Pronto Soccorso rappresenta un nodo nevralgico della rete sanitaria, in quanto costituisce il principale punto di accesso per le urgenze e le emergenze, ma al tempo stesso assorbe una quota rilevante di pazienti che potrebbero essere gestiti in setting assistenziali differenti. Il fenomeno del sovraffollamento non è quindi riconducibile esclusivamente a inefficienze interne, bensì a criticità più ampie legate alla gestione dell'intero percorso di cura e alla capacità complessiva del sistema ospedale-territorio di rispondere in modo appropriato ai bisogni di salute della popolazione. Ne deriva la necessità di affrontare la problematica con un approccio sistemico, superando una visione limitata al solo Pronto Soccorso.

Il PROGETTO DI RICERCA VOLTO ALLA RIORGANIZZAZIONE/OTTIMIZZAZIONE DELL RETE EMERGENZA-URGENZA propone l'adozione di un modello di programmazione e monitoraggio a 360°, fondato su un approccio innovativo, scientifico e data-driven, supportato da strumenti di simulazione dinamica, intelligenza artificiale e machine learning. L'obiettivo è ottimizzare non solo i processi interni del Pronto Soccorso, ma l'intera rete dell'emergenza-urgenza, individuando soluzioni organizzative e strategiche coerenti con i bisogni attuali e prospettici della popolazione. Attraverso strumenti avanzati di raccolta, integrazione e analisi dei dati, dashboard interattive e sistemi di calcolo multiparametrico, il modello consente di analizzare scenari complessi, effettuare valutazioni predittive e supportare decisioni basate su evidenze concrete.

L'approccio metodologico si articola in diverse fasi integrate. In primo luogo, viene effettuata un'analisi e validazione strutturata dei dati, che comprende la verifica della coerenza rispetto ai vincoli di processo, il trattamento dei dati mancanti con algoritmi di imputazione contestualizzati, l'individuazione e correzione degli outlier attraverso metodi statistici integrati con la conoscenza del dominio e l'integrazione di fonti eterogenee tramite tecniche di data fusion e feature engineering. Successivamente si procede alla costruzione del modello di simulazione, identificando gli elementi fondamentali del sistema, formalizzando le relazioni tra variabili mediante equazioni matematiche, reti decisionali o regole logiche e integrando algoritmi di machine learning per l'analisi supervisionata e non supervisionata dei dati. Il modello viene implementato in un ambiente computazionale capace di gestire dinamiche complesse e validato attraverso un processo iterativo che include confronto con dati storici, analisi degli errori, cross-validation temporale, analisi di sensibilità e simulazioni Monte Carlo.

La fase di simulazione prevede la definizione di scenari deterministici, stocastici e di stress testing, l'esecuzione di simulazioni multi-run e l'analisi delle performance attraverso metriche specifiche e strumenti di interpretazione avanzata. Sulla base dei risultati ottenuti, vengono definite le strategie operative e fornito supporto tecnico all'implementazione delle azioni individuate. Parallelamente, viene attivato un sistema continuo di monitoraggio fondato su KPI formalizzati, soglie di allerta e cruscotti periodici, che consente di analizzare eventuali scostamenti rispetto ai target, ritarare le strategie e attivare meccanismi di feedback strutturato, garantendo un miglioramento continuo e adattivo del sistema.

I risultati attesi includono decisioni più informate e trasparenti, maggiore velocità e flessibilità nell'analisi delle alternative strategiche, un efficientamento nell'utilizzo delle risorse disponibili con conseguente riduzione delle liste d'attesa, una diminuzione dei rischi clinici e organizzativi, un supporto concreto ai processi di change management grazie alla possibilità di testare le decisioni in ambiente virtuale e un rafforzamento della legittimazione delle scelte attraverso evidenze oggettive.

Il progetto di ricerca, strutturato in fasi graduali, si prefigge l'obiettivo di riordinare, attraverso un approccio innovativo, scientifico e supportato da moderne soluzioni tecnologiche (Simulazione Dinamica, Intelligenza Artificiale, Machine Learning, BI, ecc.), l'intera rete di Emergenza-Urgenza della Città di Torino e dell'ASL CN2, adottando una visione integrata che coniuga le esigenze di efficientamento sia della rete territoriale sia della rete ospedaliera.

Il progetto è ritenuto strategico e si colloca in linea con quanto previsto dal nuovo Piano socio-sanitario regionale 2025-2030 della Regione Piemonte (approvato con Deliberazione 22 Dicembre 2025, n. 137 – 27771) e con la D.G.R. Piemonte 19 gennaio 2026, n. 9-2154, che tra gli obiettivi gestionali assegnati ai direttori generali per l'anno 2026 ne annovera uno specifico relativo al boarding in Pronto Soccorso.

Non vengono utilizzati algoritmi di IA generativa. I dati non vengono utilizzati per allenare alcun algoritmo di IA.

L'ASL CN2 ricopre il ruolo di Titolare autonomo all'interno del progetto di ricerca.

Il trattamento dei dati pseudonimizzati verrà effettuato da AGM Project Consulting S.r.l., in qualità di Responsabile, che consiste nel fornire all'ASL CN2 attività consulenziali aventi come obiettivo la reingegnerizzazione dei processi di Pronto Soccorso, mediante lo sviluppo e l'applicazione di modelli di simulazione dinamica integrati con tecniche di intelligenza artificiale.

Il Titolare tratterà i dati personali dei pazienti/utenti di seguito descritti e relativi agli anni 2024 e 2025:

- dati identificativi (codice fiscale crittografato, anno di nascita paziente, sesso, Codice Comune Residenza, data di arrivo al PS, ora di arrivo al PS, Modalità di arrivo al PS, cittadinanza, numero SDO); - dati relativi allo stato di salute (ad esempio, dati relativi agli accessi al Pronto Soccorso, nonché alle correlate prestazioni di Radiologia, Consulenza e Laboratorio Analisi, e dati contenuti nella Scheda di Dimissione Ospedaliera). Prima della comunicazione dei dati al Responsabile del trattamento, i dati identificativi raccolti vengono sottoposti a un processo di pseudonimizzazione attraverso l'utilizzo del sistema crittografico SHA-256 (Secure Hash Algorithm 256-bit): è una funzione di hash crittografica che trasforma qualsiasi input di dati (testo, file, immagini) in una stringa univoca di 64 caratteri esadecimali (256 bit). È deterministico, non invertibile e progettato per essere estremamente resistente alle collisioni: anche la minima modifica all'input genera un hash completamente diverso. Il Responsabile non potrà pertanto identificare in modo diretto gli Interessati.
Finalità del trattamento
Attuazione di un modello di programmazione e monitoraggio della rete di emergenza-urgenza che, attraverso soluzioni tecnologiche (Simulazione Dinamica, Intelligenza Artificiale, Machine Learning, ecc.), consenta di individuare soluzioni di efficientamento sia della rete territoriale sia della rete ospedaliera., Il trattamento è finalizzato esclusivamente all'ottimizzazione dei processi organizzativi ed operativi del Titolare del trattamento, mediante:, - l'analisi dei tempi di attesa nelle diverse fasi del percorso di emergenza-urgenza e del percorso prestazionale;, - la valutazione dei flussi di accesso e dimissione degli utenti;, - il monitoraggio dei tempi di esecuzione delle prestazioni sanitarie e degli esami diagnostici;, - l'individuazione di criticità organizzative e colli di bottiglia nei processi assistenziali., Le finalità risultano pertanto chiaramente determinate e circoscritte, non generiche né indeterminate, e non comprendono utilizzi ulteriori o incompatibili dei dati personali trattati.
Basi giuridiche
Articolo 6 e) – il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
Articolo 9 g) – il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri che deve essere proporzionato alla finalità perseguita
Articolo 9 h) – il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro valutazione della capacità lavorativa del dipendente diagnosi assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari
Riferimenti normativi

La finalità del trattamento in oggetto si colloca in linea con quanto previsto dal Piano sociosanitario regionale 2025-2030 della Regione Piemonte (approvato con Deliberazione 22 Dicembre 2025, n. 137 – 2777), nonché dalla D.G.R. Piemonte 19 gennaio 2026, n. 9-2154 avente ad oggetto "Assegnazione ai direttori generali/commissari delle aziende sanitarie regionali, ai sensi dell'art. 2, comma 2, D.Lgs n. 171/2016 e s.m.i. e dell'art. 1, comma 865, l. n. 145/2018, degli obiettivi economici-gestionali, di salute e di funzionamento dei servizi finalizzati all'attribuzione della quota integrativa al trattamento economico per l'anno 2026 e conferma dei criteri per il monitoraggio e la valutazione degli obiettivi di mandato assegnati alla nomina art. 2, comma 4, D.Lgs n. 171/2016 e s.m.i.", Inoltre, la pseudonimizzazione dei dati personali, anche appartenenti alle categorie particolari di cui all'articolo 9, paragrafo 1, del medesimo regolamento (UE) 2016/679, ai sensi dell'art. 8 co. 3 della L. 132/2025 è sempre consentito per le finalità di cui all'articolo 2-sexies, comma 2, lettera v), del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, ovvero l'attività di "programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale"
Origine dei dati
Dati già raccolti (Il Titolare tratterà i dati personali dei pazienti/utenti relativi agli accessi al Pronto Soccorso negli anni 2024 e 2025.)
Modalità del trattamento
Informatizzato
Categorie di dati
Dati personali comuni
Dati identificativi
Categorie particolari di dati personali
Dati relativi alla salute
Categorie di interessati
Assistiti ; Utenti

Titolare	ASL CN 2
Responsabili del trattamento	AGM Project Consulting srl
Sub-responsabili	Microsoft. ; Qlik
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		
Il trattamento prevede il trasferimento o la comunicazione di dati		
Comunicazioni		
Destinatari	**Note**	
AGM Project Consulting srl Via Giotto, 36 – Milano P.IVA e C.F. 06272040962.	I dati saranno trasmessi al Responsabile del Trattamento solo dopo essere stati pseudonimizzati dall'ASL CN2.	
Descrizione del periodo di conservazione dei dati		
I dati personali oggetto del trattamento saranno comunicati previa procedura di pseudonimizzazione degli stessi. Nello specifico, i dati identificativi univoci dei pazienti (i.e. codice fiscale) saranno trasmessi al Responsabile in forma crittografata. I dati vengono conservati e archiviati dal Responsabile del trattamento per il tempo necessario al fine di portare a termine gli obiettivi prefissati. Su richiesta del Titolare, i dati possono essere conservati per un successivo raffronto, al fine di verificare la misura del raggiungimento degli obiettivi.		
Applicativi	AnyLogic - Software per la costruzione di modelli di simulazione dinamica, capaci di rappresentare il funzionamento complessivo della rete e testare scenari alternativi. ; Qlik - Creazione di dashboard interattive e report dinamici, utili a visualizzare sia i dati analizzati sia i risultati delle simulazioni.	
Note		

L'integrazione tra i vari strumenti garantisce un flusso metodologico continuo e coerente: i dati analizzati e validati in Python vengono visualizzati su Qlik e costituiscono l'input per la valutazione dei singoli PS e dell'intera rete di emergenza-urgenza effettuata tramite i Modelli di Matematica Clinica, nonché per il modello di simulazione sviluppato in AnyLogic; gli algoritmi di ottimizzazione (Python e Anylogic) alimentano scenari alternativi che vengono testati in ambiente simulativo; infine, Qlik viene nuovamente utilizzato per visualizzare e confrontare i risultati delle simulazioni.
I dati oggetto del progetto sono trattati esclusivamente all'interno dello Spazio Economico Europeo (SEE), in funzione della localizzazione dei data center Microsoft utilizzati. Non sono previsti trattamenti sistematici di dati personali al di fuori del SEE.
I sistemi applicativi e i database utilizzati dal Responsabile per il progetto sono ospitati su infrastruttura Microsoft, tramite ambienti server-based. I data center sono localizzati all'interno dell'Unione Europea, in conformità alle policy di Microsoft EU Data Boundary. I provider infrastrutturali terzi(Qlik) hanno tutti sede in UE.
I dati sono logicamente segregati all'interno dell'infrastruttura cloud Microsoft mediante meccanismi di tenant isolation. L'accesso ai dati è limitato agli ambienti e alle risorse espressamente autorizzate.
I dati sono cifrati:
I. a riposo (encryption at rest),
II. in transito (encryption in transit),
utilizzando algoritmi crittografici conformi agli standard internazionali.
La gestione delle chiavi di cifratura avviene secondo i servizi di key management messi a disposizione da Microsoft, con possibilità di controllo da parte dell'ASL CN2 (Crittografia in Microsoft 365|Microsoft Learn).
Inoltre, tutti i dati sensibili vengono inviati crittografati al Responsabile del trattamento, attraverso algoritmo SHA-256.
Il logging è centralizzato dagli accessi ai sistemi. Esiste il tracciamento di qualsiasi operazione effettuata sui dati ed il monitoraggio continuo tramite strumenti nativi Microsoft.
d. L'accesso ai dati è consentito esclusivamente al personale autorizzato attraverso autenticazione tramite account nominali con revoca immediata degli accessi in caso di cessazione/cambio ruolo.

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**
	Titolare del trattamento è l'ASL CN2 Alba-Bra, con sede in Via Vida, 10 – 12051 Alba – CN (PEC: aslcn2@legalmail.it)
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)**
	Responsabile esterno al trattamento dei dati: AGM Project Consulting srl Via Giotto, 36 – Milano P.IVA e C.F. 06272040962

Componenti tecnologiche

Componente	**Descrizione**
Applicazioni	**Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)**
	AnyLogic: per la costruzione di modelli di simulazione dinamica, capaci di rappresentare il funzionamento complessivo della rete e testare scenari alternativi; Qlik: per la creazione di dashboard interattive e report dinamici, utili a visualizzare sia i dati analizzati sia i risultati delle simulazioni.
Infrastrutture IT	**Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)**
	Modelli di Matematica Clinica: per formalizzare vincoli clinici e organizzativi, calcolare parametri di capacità e saturazione e supportare decisioni evidence-based.
Rete	**Descrizione sintetica (es. tipologia di rete, tecnologie utilizzate, relazioni con altre componenti)**
	Rete aziendale ASL CN2 Rete del Responsabile del trattamento

Componenti fisiche

Componente	**Descrizione**

Risorse ed asset materiali	**Descrizione (es. principali caratteristiche, tipologia di asset non latamente inteso come informatico, relazioni con altre componenti)**
	a. AnyLogic: per la costruzione di modelli di simulazione dinamica, capaci di rappresentare il funzionamento complessivo della rete e testare scenari alternativi; b. Python: per l'elaborazione dei dati, lo sviluppo di algoritmi predittivi e modelli di ottimizzazione che alimentano gli scenari simulativi; c. Qlik: per la creazione di dashboard interattive e report dinamici, utili a visualizzare sia i dati analizzati sia i risultati delle simulazioni; d. Modelli di Matematica Clinica: per formalizzare vincoli clinici e organizzativi, calcolare parametri di capacità e saturazione e supportare decisioni evidence-based.
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 Sede fisica operativa del Responsabile: Via Giotto, 36 – 20145 Milano (MI)) e sedi dei Sub Responsabili del trattamento (Microsft e Qlik)

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:

Attuazione di un modello di programmazione e monitoraggio della rete di emergenza-urgenza che, attraverso soluzioni tecnologiche (Simulazione Dinamica, Intelligenza Artificiale, Machine Learning, ecc.), consenta di individuare soluzioni di efficientamento sia della rete territoriale sia della rete ospedaliera.
Il trattamento è finalizzato esclusivamente all'ottimizzazione dei processi organizzativi ed operativi del Titolare del trattamento, mediante:
- l'analisi dei tempi di attesa nelle diverse fasi del percorso di emergenza-urgenza e del percorso prestazionale;
- la valutazione dei flussi di accesso e dimissione degli utenti;
- il monitoraggio dei tempi di esecuzione delle prestazioni sanitarie e degli esami diagnostici;
- l'individuazione di criticità organizzative e colli di bottiglia nei processi assistenziali.
Le finalità risultano pertanto chiaramente determinate e circoscritte, non generiche né indeterminate, e non comprendono utilizzi ulteriori o incompatibili dei dati personali trattati.

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	Il diritto di opposizione ex art. 21 GDPR, in base al quale l'interessato ha il diritto di ottenere la cessazione del trattamento ulteriore dei dati personali da parte del Titolare, salvo che quest'ultimo dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
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 diritto alla revoca non è applicabile per tale attività di trattamento.

Diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato	Il titolare del trattamento garantisce che nessun interessato sia sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo nei casi previsti dall'art. 22, par. 2 GDPR (consenso esplicito, contratto, obbligo di legge). Nei casi in cui il trattamento sia lecito, sono garantite misure adeguate per la tutela dei diritti dell'interessato, tra cui il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione.

Principi

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato	I dati personali degli interessati verranno trattati dal Titolare ai sensi dell'art. 5 del GDPR e nel rispetto dei principi di liceità, correttezza e trasparenza. Inoltre, il trattamento sarà effettuato in conformità all'art. 32 del GDPR, garantendo un livello di sicurezza adeguato ai rischi per gli interessati, attraverso misure tecniche e organizzative idonee a proteggere i dati personali da distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato. I dati personali oggetto del trattamento saranno comunicati previa procedura di pseudonimizzazione degli stessi. Nello specifico, i dati identificativi univoci dei pazienti (i.e. codice fiscale) saranno trasmessi al Responsabile in forma crittografata. In ogni caso, viene assicurata l'adozione di ogni misura tecnica e organizzativa adeguata a garantire la sicurezza dei dati personali ai sensi del GDPR.
I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità	Il Titolare tratterà i dati personali dei pazienti/utenti unicamente per l'attuazione di un modello di programmazione e monitoraggio della rete di emergenza-urgenza che, attraverso soluzioni tecnologiche (Simulazione Dinamica, Intelligenza Artificiale, Machine Learning, ecc.), consenta di individuare soluzioni di efficientamento sia della rete territoriale sia della rete ospedaliera.

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 degli interessati verranno trattati dal Titolare ai sensi dell'art. 5 del GDPR e nel rispetto dei principi di liceità, correttezza e trasparenza. Inoltre, il trattamento sarà effettuato in conformità all'art. 32 del GDPR, garantendo un livello di sicurezza adeguato ai rischi per gli interessati, attraverso misure tecniche e organizzative idonee a proteggere i dati personali da distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato. I dati personali oggetto del trattamento saranno comunicati previa procedura di pseudonimizzazione degli stessi. Nello specifico, i dati identificativi univoci dei pazienti (i.e. codice fiscale) saranno trasmessi al Responsabile in forma crittografata. In ogni caso, viene assicurata l'adozione di ogni misura tecnica e organizzativa adeguata a garantire la sicurezza dei dati personali ai sensi del GDPR: i dati inviati al Responsabile del trattamento saranno cancellati da questo una volta elaborati e al più tardi al termine del contratto.
I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali	Prima della comunicazione dei dati al Responsabile del trattamento i dati identificativi raccolti vengono sottoposti a un processo di pseudonimizzazione attraverso l'utilizzo di un sistema crittografico. Il Responsabile, esecutore del progetto di ricerca, non potrà pertanto identificare in modo diretto gli interessati.

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:

$$R_2 = R_1 - \left(M_n\right)$$

dove per:

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

All'interno del presente passaggio saranno presenti, in ordine

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

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

7.1 Misure di sicurezza

Misure di sicurezza trasversali relative ai trattamenti

Misura di sicurezza	Stato di adozione e implementazione

Politiche, regolamenti e manuali	
È stato definito un manuale per la gestione del protocollo informatico	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
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
Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	Applicata
Protezione dei Dati	
Sono in vigore procedure gestire la conservazione dei dati.	Applicata
Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata
Conservazione in locale ad accesso riservato chiuso a chiave	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

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

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

Misure di sicurezza specifiche relative al trattamento

Categoria	Misura	Stato di adozione e implementazione
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata
	Le chiavi private sono adeguatamente protette	Applicata
	Formazione relativa alla cifratura	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata
	È stato redatto un manuale per la conservazione digitale	Applicata

	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata
Gestione utenze	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	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
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata
	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	Applicata

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata

	È stato redatto un manuale per la conservazione digitale	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

Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata
	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 gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata

	È stato redatto un manuale per la conservazione digitale	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

Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata
	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 gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata

	È stato redatto un manuale per la conservazione digitale	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

Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata
	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 gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata

	È stato redatto un manuale per la conservazione digitale	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

Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata
	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 gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata

	È stato redatto un manuale per la conservazione digitale	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

Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata
	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 gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata

	È stato redatto un manuale per la conservazione digitale	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

Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata
	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 gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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		2	Medio
Probabilità		3	Probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Modifiche indesiderate dei dati	CNIL	Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		1	Improbabile
Livello di rischio iniziale		2	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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		2	Medio
Probabilità		2	Poco probabile
Livello di rischio iniziale		4	Medio
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	È stato redatto un manuale per la conservazione digitale	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
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	Applicata	Applicata

	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 gestire la conservazione dei dati.	Applicata	Applicata

	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata	Applicata
	Conservazione in locale ad accesso riservato chiuso a chiave	Applicata	Applicata

	Il server è situato in territorio UE Descrizione: Il server è situato in territorio UE; Sono previste procedure di business continuity per quanto riguarda l'infrastruttura centralizzata (console e processor). Nei Data Centerr sono presenti firewall perimetrali con funzionalità UTM attive sugli accessi dall'esterno che sono comunque filtrati sugli ip dei clienti del fornitore. E' svolto patching periodico o di emergenza in caso di segnalazioni di vulnerabilità gravi da parte del vendor.	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
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	
Totale	Totale	

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)	4	1
Malfunzionamento o distruzione di strumentazione it (server)	4	1
Malfunzionamento o distruzione di strumentazione it (rete)	4	1
Distruzione o furto di strumentazione	4	1
Uso non autorizzato della strumentazione	4	1
Divulgazione accidentale di informazioni	4	1
Infezioni da virus, malware	6	1
Accesso illegittimo ai dati	4	1
Modifiche indesiderate dei dati	2	1
Perdita di dati	4	1
Danno per la reputazione	4	1
Discriminazione	4	1
Furto d'identità	4	1
Danni fisici o psicologici	4	1
Perdita di controllo dei dati	4	1

Livello di rischio complessivo per area

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

Livello di rischio complessivo iniziale

Alto

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