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 - 191 - GIVITI: Progetto Indicatori - monitoraggio e miglioramento della qualità dell’assistenza in terapia intensiva

24/07/2026

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 - 191 - GIVITI: Progetto Indicatori - monitoraggio e miglioramento della qualità dell’assistenza in terapia intensiva” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “GIVITI: Progetto Indicatori - monitoraggio e miglioramento della qualità dell’assistenza in terapia intensiva”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

2. Informazioni essenziali

Data di creazione dell’analisi	26/04/2026
Data generazione documento	24/07/2026
Stato	In lavorazione
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).	No

Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.	No
Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 Regolamento UE 2016/679 interconnessi con altri dati personali raccolti per finalità diverse.	Sì
Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).	No
Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).	Sì
Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).	Sì
Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 (criteri WP 29).	No

Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).	No
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	No
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	No
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	No

Stima del rischio

Criteri utilizzati per la stima del rischio	Risposta
Il trattamento comporta la valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione	No
Il trattamento prevede un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	No
Il trattamento consiste in un'attività di monitoraggio sistematico	No
Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale	Sì
Il trattamento di dati avviene su larga scala	No
Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	No
Il trattamento coinvolge categorie di interessati vulnerabili	Sì
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	No
Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	No
Elevato	

4. Informazioni sul trattamento

Codice identificativo	Nome	Data di creazione	Data dell'ultima modifica
191	GIVITI: Progetto Indicatori - monitoraggio e miglioramento della qualità dell'assistenza in terapia intensiva	26/04/2026	05/06/2026

Descrizione

Al fine di rafforzare e rendere più efficaci i programmi di miglioramento della qualità dell'assistenza e di promuovere un utilizzo appropriato delle risorse sanitarie, l'Istituto di Ricerche Farmacologiche Mario Negri IRCCS (IRFMN) e GiViTI (Gruppo italiano per la valutazione degli interventi in Terapia Intensiva) hanno sviluppato nel tempo numerose collaborazioni a livello istituzionale, regionale e nazionale. In questo contesto, Regione Toscana e Regione Piemonte hanno stipulato specifiche convenzioni con IRFMN per la realizzazione di programmi strutturati di miglioramento della qualità dell'assistenza e dell'appropriatezza nell'utilizzo delle risorse in Terapia Intensiva (TI). In attuazione della DGR 35-2072 del 22 dicembre 2025, la Regione Piemonte ha autorizzato la realizzazione del Progetto "Indicatori: monitoraggio e miglioramento della qualità dell'assistenza in terapia intensiva" in collaborazione con l'IRFMN finalizzato al monitoraggio e al miglioramento della qualità dell'assistenza in terapia intensiva mediante l'utilizzo di indicatori standardizzati. L'IRFMN è stato nominato Responsabile del trattamento dei dati, previa sottoscrizione della nomina da parte di ciascuna Azienda coinvolta, ai sensi della normativa vigente, in relazione al progetto "Indicatori: monitoraggio e miglioramento della qualità dell'assistenza in terapia intensiva".

Oltre al supporto diretto ai processi di miglioramento, il progetto contribuisce a colmare importanti debiti informativi a livello provinciale, regionale e nazionale su diversi aspetti della gestione del paziente critico, quali la sorveglianza delle infezioni correlate all'assistenza (ICA) e il consumo di antibiotici.

Le attività progettuali si basano sulla raccolta sistematica di dati clinici e di informazioni organizzative relative agli ospedali e alle Terapie Intensive aderenti.

Un elemento centrale dell'intero progetto è rappresentato dalla qualità dei dati analizzati, garantita sia dal design dei sistemi informatici di raccolta – basati sul software PROSAFE, sviluppato da GiViTI e IRFMN – sia dai controlli applicati in fase di elaborazione dai ricercatori IRFMN. La raccolta e la gestione dei dati avvengono in forma pseudonimizzata, nel pieno rispetto della normativa nazionale ed europea in materia di protezione dei dati personali.

Nell'ambito del Progetto Indicatori sono stati inoltre sviluppati specifici sottoprogetti tematici, finalizzati ad approfondire aspetti rilevanti della gestione del paziente critico e a supportare interventi mirati di miglioramento.

• Sorveglianza delle infezioni e dell'antimicrobico-resistenza con particolare riferimento all'epidemiologia e all'incidenza delle infezioni in Terapia Intensiva e nelle aree cliniche coinvolte dal progetto. Rientrano in questo ambito anche le analisi finalizzate all'implementazione di programmi di Antimicrobial Stewardship e al miglioramento del processo diagnostico-terapeutico del paziente critico affetto da sepsi, con l'obiettivo di migliorare gli outcome clinici e ridurre la diffusione di patogeni (Multi-Drug Resistant (MDR).

• Studio sull'Appropriatezza dei Ricoveri in Terapia Intensiva (StART) che si pone l'obiettivo di migliorare l'appropriatezza dei ricoveri e delle giornate di degenza in TI. In continuità con le finalità regionali di gestione operativa, il progetto mira a supportare la pianificazione dinamica degli asset condivisi, la programmazione delle risorse infrastrutturali e il monitoraggio dell'efficienza operativa, mettendo in relazione i livelli di assistenza potenzialmente erogabili da ciascuna TI, sulla base delle risorse disponibili, con quelli effettivamente erogati.

Gli indicatori scelti dall'ASL CN2 all'interno del progetto per impostare un obiettivo di miglioramento sono: la mortalità (indicatore individuato come obiettivo comune a livello regionale, definito attraverso una discussione collegiale) e l'infezione (batteriemia) CVC (catetere venoso centrale) correlata.

Ai fini dell'attuazione del progetto sono pertanto previsti i seguenti passaggi:

1. nomina dell'Istituto di Ricerche Farmacologiche Mario Negri (IRCCS) quale responsabile esterno del trattamento dei dati da parte dell'ASL.

2. attivazione del software PROSAFEWeb, accessibile direttamente online e senza necessità di installare applicazioni sui computer locali, sui sistemi informativi dell'ASL CN2.

3. inserimento nel software dei dati relativi ai pazienti ammessi negli anni 2025-2026.

Responsabile del progetto presso l'ASL CN2 è il dott. Andrea Della Selva, operante presso la S.C. Anestesia e Rianimazione e Responsabile della S.S. Rianimazione.

Tramite l'applicativo PROSAFE vengono raccolti e trattati i seguenti tipi di dati dei pazienti coinvolti:

- Dati personali ai sensi dell'art. 4, n. 1, del GDPR: dall'ASL CN2 vengono trattati nome e cognome, luogo e data di nascita, numero di tessera sanitaria, codice fiscale, numero di cellulare, indirizzo e-mail, recapiti

telefonici dei familiari, nome e recapito telefonico del medico di medicina generale, residenza e domicilio; dall'IRFMN vengono trattati il livello di istruzione, lo stato civile, la situazione di convivenza e la situazione lavorativa;

- dati rientranti nelle categorie “particolari” di dati personali (dati personali che rivelino l'origine razziale o etnica, gruppo sanguigno e fattore Rh, dati relativi alla salute, quali comorbidità, patologie, parametri fisiopatologici, trattamenti ricevuti e esiti clinici) di cui all’art. 9 del GDPR.

Inoltre, vengono trattati i seguenti tipi di dati dei dipendenti/collaboratori coinvolti, non accessibili a IRFMN, ma solo da ASL CN2:

- Indirizzo e-mail (necessario per la registrazione)

- Password (gestita dal sistema in modalità sicura)

- Tracciamento degli accessi e delle operazioni effettuate nell’applicativo (log di autenticazione e attività dei compilatori).

Il Responsabile del trattamento dei dati verrà a conoscenza esclusivamente di informazioni relative a turni, assegnazioni, presenza in servizio e attività assistenziali.

L'ASL CN2 può visualizzare esclusivamente i propri dati, sia all’interno della dashboard sia nei report annuali. I dati a livello regionale saranno resi disponibili unicamente in forma aggregata e anonima, e quindi non riconducibili ai singoli centri.

Finalità del trattamento

La finalità del presente Progetto è il miglioramento della qualità dell’assistenza e dell’impiego delle risorse nell’ambito dei reparti di terapia intensiva delle Aziende Sanitarie e ospedaliere piemontesi attraverso la prosecuzione per gli anni 2025-2027 del “Progetto di valutazione della performance e dell’appropriatezza d’uso delle risorse delle terapie intensive regionali”., Le finalità di cui sopra sono ricomprese tra quelle previste all’art. 2 sexies co. 2 lett. v) D.Lgs. 196/2003 e s.m.i. “v) 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” e comportano il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante.

Basi giuridiche

Articolo 2 - sexies comma 2 lett. v) - Nuovo Codice Privacy

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	
Origine dei dati	
Dati già raccolti	
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 ; Collaboratori ; Dipendenti	
Titolare	ASL CN 2
Responsabili del trattamento	Istituto di Ricerche Farmacologiche Mario Negri IRCCS
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**
Istituto di Ricerche Mario negri IRCCS	i dati pseudonimizzati vengono inviati al Responsabile del trattamento dei dati tramite piattaforma web PROSAFE.
Periodo di conservazione dei dati personali	

1 anno
Descrizione del periodo di conservazione dei dati
Il presente progetto ha validità fino al 31 dicembre 2027; alla sua scadenza il progetto si intende terminato, ma potrà essere prorogato, tenuto conto del livello di raggiungimento degli obiettivi del progetto stesso, dietro presentazione di formale e motivata richiesta, sottoscritta e inviata dal Responsabile scientifico al competente Settore della Regione Piemonte. L'atto di nomina dell'IRFMN ha validità per la durata della convezione con Regione Piemonte, quindi fino al 31 dicembre 2027, e per un anno successivo alla sua conclusione, al fine di garantire una corretta analisi dei dati e la prosecuzione delle attività affidate al Responsabile.

Applicativi	ProsafeWeb - Il ProsafeWeb è il nuovo software messo a disposizione dell'Istituto di Ricerche Farmacologiche Mario Negri per raccogliere i dati dei progetti GiViTI. Utilizza una logica Web-based è accessibile all'interno della rete ospedaliera tramite l'uso di browser aggiornati.

Note
Il ProsafeWeb è il nuovo software messo a disposizione dell'Istituto di Ricerche Farmacologiche Mario Negri per raccogliere i dati dei progetti GiViTI. Utilizza una logica Web-based è accessibile all'interno della rete ospedaliera tramite l'uso di browser aggiornati. Prosafe fornisce solo la parte applicativa, tutta la parte sistemistica (server, sistema operativo, rete, etc.) e le relative policy e impostazioni di sicurezza sono a carico del centro, in quanto ogni centro avrà la sua installazione separata. Questo garantisce di non far uscire i dati sensibili dalla rete del centro. I dati sono salvati su database SQLite, separati e cifrati per livello di accesso. I dati raccolti sono salvati nel database principale ("Case Data Store") cifrati attraverso una chiave diversa per ogni ricovero e livello di accesso. Questo significa che i dati sensibili del ricovero (il livello di accesso più restrittivo) saranno cifrati separatamente con una chiave diversa rispetto agli altri dati clinici, garantendo a priori una segregazione logica. Le chiavi di cifratura sono salvate in un database separato ("Keys Store") rispetto a quello dei dati clinici, ed anche i dati sensibili possono essere salvati in un database separato ("Sensitive Data Store") se viene richiesta una segregazione fisica dei dati per maggiore sicurezza. Allo stesso modo, i moduli di backend che forniscono all'applicazione web i dati clinici ("Case Data Store") e le chiavi ("Keys Store") possono essere installati su due server fisicamente separati, per garantire un tipo diverso sicurezza in caso di breach. Le chiavi di cifratura sono lunghe 256 bit e l'algoritmo utilizzato per la cifratura è AES-GCM. Ogni reparto inoltre possiede una coppia di chiavi asimmetriche (pubblica / privata) a 2048 bit per poter trasferire dati fra i reparti e verso l’archivio centralizzato presso il centro di coordinamento GiViTI. Vengono trasferiti solo i dati che corrispondono a livelli di accesso NON sensibili. Le chiavi asimmetriche hanno lunghezza 2048 bit e l'algoritmo utilizzato per la cifratura è RSA.

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), responsabile aziendale del progetto è il dott. Della Selva Andrea, Responsabile della S.S. Rianimazione del P.O. "Michele e Pietro Ferrero" di Verduno.
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: Istituto di Ricerche Farmacologiche Mario Negri IRCCS, con sede legale in via Mario Negri, 2 -20156 Milano.

Componenti tecnologiche

Componente	Descrizione
Applicazioni	**Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)**
	Prosafe è un'applicazione web specificamente sviluppata per le raccolte dati GiViTI. Si basa su Dandelion, framework per la costruzione di raccolte dati strutturate, ed è composta da un frontend web e da uno o più moduli di web server (backend) localizzati all'interno di ciascun ospedale; i moduli di backend forniscono funzionalità di login, archivio dei dati, messa a disposizione di configurazioni, pagine web e di tutte le risorse necessarie alla raccolta dati.
Infrastrutture IT	**Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)**

	Prosafe, in base alle sue CRF (case report form), può essere utilizzato in contesti di ricerca differenti. È composto da diversi moduli: - DataStore, che contiene tutti i dati clinici - KeyStore, che contiene le chiavi di cifratura dei singoli casi - Webserver + Webapp (frontend), che costituisce l'interfaccia dell'applicativo I moduli possono essere installati su uno o più server web (anche virtualizzati). L'installazione standard prevede un unico server, ma è possibile ad esempio separare DataStore e KeyStore su server diversi nel caso fosse necessario un maggiore grado di sicurezza. Tutti i moduli sono basati su .NET Core e utilizzano Kestrel come server web, è supportato l'utilizzo di altri reverse Proxy (Nginx/ Apache / IIS). L'applicativo utilizza una logica Web-based ed è accessibile all'interno della rete ospedaliera tramite l'uso di browser aggiornati.
Rete	**Descrizione sintetica (es. tipologia di rete, tecnologie utilizzate, relazioni con altre componenti)**
	Rete aziendale: si accede all'applicativo tramite la rete ospedaliera. Rete del Responsabile del trattamento: tutti i dati sono fisicamente sui server nella sala server della sede in Via Mario Negri 2 - 20156 Milano. Il personale della sede di Ranica (sede operativa) si collega con connessione sicura ai server di Milano.

Componenti fisiche

Componente	Descrizione
Risorse ed asset materiali	**Descrizione (es. principali caratteristiche, tipologia di asset non latamente inteso come informatico, relazioni con altre componenti)**
	PC AZIENDALE PROSAFEWEB: - DataStore, che contiene tutti i dati clinici - KeyStore, che contiene le chiavi di cifratura dei singoli casi - Webserver + Webapp (frontend), che costituisce l'interfaccia dell'applicativo
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: Villa Camozzi, Via GB Camozzi 3 - 24020 Ranica (BG).

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:

La finalità del presente Progetto è il miglioramento della qualità dell'assistenza e dell'impiego delle risorse nell'ambito dei reparti di terapia intensiva delle Aziende Sanitarie e ospedaliere piemontesi attraverso la prosecuzione per gli anni 2025-2027 del "Progetto di valutazione della performance e dell'appropriatezza d'uso delle risorse delle terapie intensive regionali".
Le finalità di cui sopra sono ricomprese tra quelle previste all'art. 2 sexies co. 2 lett. v) D.Lgs. 196/2003 e s.m.i. "v) 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" e comportano il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante.

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. 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/dipendenti/collaboratori unicamente per un progetto di miglioramento della qualità della assistenza nell'ambito del reparto di terapia intensiva dell'ASL CN2.
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 (non identificativi) oggetto del trattamento saranno comunicati previa procedura di pseudonimizzazione degli stessi. 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 dopo un anno dal termine del contratto, al fine di garantire una corretta analisi dei dati e la prosecuzione delle attività affidante al Responsabile.
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 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
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata
	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata

	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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	MFA con scadenza Descrizione: MFA con scadenza	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		1	Lieve
Probabilità		2	Poco probabile
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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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 è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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
Attacchi di ingegneria sociale	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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
Intercettazione del traffico	Hardware e Software	Riservatezza ; Integrità	Umano ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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 è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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 è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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
Perdite finanziare	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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		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
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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
Altri svantaggi economici o sociali	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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
Impossibilità di esercitare diritti, servizi o opportunità	Garante Protezione dei dati	Disponibilità ; Riservatezza ; Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio iniziale		1	Basso
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	Applicata	Applicata
	È implementato un sistema di gestione delle chiavi crittografiche	Applicata	Applicata
	Le chiavi private sono adeguatamente protette	Applicata	Applicata
	Formazione relativa alla cifratura	Applicata	Applicata
	I log sono mantenuti in formato cifrato Descrizione: I log sono mantenuti in formato cifrato all' interno dei processor criptati.	Applicata	Applicata

	Sono presenti backup dei processor e sono cifrati Descrizione: Sono presenti backup dei processor e sono cifrati	Applicata	Applicata
	Cifratura TLS 1.2/1.3 Descrizione: tutti i dati sono crittografati con TLS 1.2/1.3 tra client e server.	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

	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
	MFA con scadenza Descrizione: MFA con scadenza	Applicata	Applicata
	Autenticazione a due fattori (2FA) Descrizione: Autenticazione a due fattori (2FA)	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
	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)	2	1
Malfunzionamento o distruzione di strumentazione it (server)	1	1
Malfunzionamento o distruzione di strumentazione it (rete)	1	1
Distruzione o furto di strumentazione	1	1
Uso non autorizzato della strumentazione	1	1
Divulgazione accidentale di informazioni	1	1
Infezioni da virus, malware	1	1
Attacchi di ingegneria sociale	1	1
Intercettazione del traffico	1	1
Accesso illegittimo ai dati	1	1
Modifiche indesiderate dei dati	1	1
Perdita di dati	1	1
Danno per la reputazione	1	1
Discriminazione	1	1
Furto d'identità	1	1
Perdite finanziare	1	1

Danni fisici o psicologici	1	1
Perdita di controllo dei dati	1	1
Altri svantaggi economici o sociali	1	1
Impossibilità di esercitare diritti, servizi o opportunità	1	1

Livello di rischio complessivo per area

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

Livello di rischio complessivo iniziale

Basso

Livello di rischio complessivo residuo

Basso

8. Coinvolgimento delle parti interessate

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

9. Note

Il Titolare del trattamento

ASL CN 2