Valutazione d’impatto sulla protezione dei dati

Valutazione d’impatto Trattamento progetto Trust Alert

05/02/2025

Indice

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

1. Introduzione

Il presente documento “Valutazione d’impatto Trattamento progetto Trust Alert” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “Trattamento progetto Trust Alert”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

2. Informazioni essenziali

Data di creazione dell’analisi	03/07/2024
Data generazione documento	05/02/2025
Data del prossimo controllo	06/08/2025
Stato	Definitivo
Reporter	Gioacchino Cimino ; Elisabetta Zicarelli

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).	Sì
Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).	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	Sì

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
117	Trattamento progetto Trust Alert	03/07/2024	04/12/2024
Descrizione			

Il Progetto TrustAlert consiste nel:

• mappare lo stato di salute e i pattern di morbilità e vulnerabilità nella popolazione mediante lo studio di una serie di indicatori quantitativi, utilizzando tecniche di Intelligenza Artificiale applicate ai dati sanitari amministrativi anonimizzati mediante l'integrazione di tecniche statistiche tradizionali per i dati strutturati, ed estrazioni di informazioni (feature) mediante tecniche di NLP (natural language processing) per i dati non pre-codificati;

• implementare nuove soluzioni tecniche di Intelligenza Artificiale per estrarre informazioni cliniche affidabili da dati strutturati e non strutturati e implementare un sistema di event detection e alerting di emergenze sanitarie in arrivo;

• sviluppare un living lab come ambiente per condurre micro e macro-simulazioni al fine di implementare scenari di tipo what-if, che consentano di ottimizzare l'allocazione delle risorse in caso di emergenza sanitaria e di valutare l'impatto delle misure di prevenzione.

Dal punto di vista della protezione dei dati personali, il trattamento consiste nel processo di anonimizzazione del data set contenente dati personali di pazienti dell'ASL CN2, estratti dalle loro cartelle cliniche archiviate dal 2019 al 2024. Tale processo di anonimizzazione avverrà all'interno del perimetro dell'infrastruttura IT del Titolare del trattamento, attraverso una macchina virtuale che pertanto renderà accessibile al fornitore (Computer Angels s.r.l.s.) i soli dati selezionati che compongono il suddetto data set. Il processo di anonimizzazione prevede l'applicazione di un algoritmo di hashing, non invertibile. Non sarà infatti possibile ricostruire il dato originale a partire dalla stringa che viene restituita in output. Pertanto, il dato personale viene trattato soltanto all'interno di un ambiente che già gestisce i medesimi dati. Tutte le elaborazioni successive saranno effettuate esclusivamente su dati anonimi.

Finalità del trattamento	
Anonimizzazione del data set oggetto del progetto Trust Alert	
Basi giuridiche	Articolo 9 j) – il trattamento è necessario a fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89 paragrafo 1 sulla base del diritto dell'Unione o nazionale
Riferimenti normativi	Art 110 Codice privacy (ricerca epidemiologica che non consente la raccolta del consenso in quanto implica uno sforzo sproporzionato) in combinato disposto art. 9 par. 2 l. J)
Origine dei dati	

Raccolti presso l'interessato	
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	
Minori	
Titolare	ASL CN 2
Responsabili del trattamento	Computer Angels s.r.l.s
Responsabile della protezione dei dati	Studio Legale Associato LCG Lecis Cannella Grassi ; Giuseppe Cannella
Periodo di conservazione dei dati personali	
Come da massimario di scarto	
Descrizione del periodo di conservazione dei dati	Il data set predisposto per la realizzazione del progetto sarà accessibile soltanto per il tempo necessario per l'anonimizzazione. Resta inteso che i dati contenuti nel data set seguono le tempistiche di conservazione del massimario di scarto.
Applicativi	KEYFORM - KEYFORM di Computer Angels srls
Note	
Il software Trust Alert è sviluppato per il progetto in linguaggio python. La componente IT individuata è il nominativo assegnato alla macchina virtuale.	

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
Sedi fisiche	**Descrizione (es. ubicazione delle sedi anche distaccate o periferiche, principale utilizzo, relazioni con altre componenti)**
	CED ASL CN2

Componenti tecnologiche

Componente	Descrizione
Applicazioni	**Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)**
	N.A.
Infrastrutture IT	**Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)**
	l'accesso al data set predisposto ad hoc per il progetto è possibile attraverso una macchina virtuale all'interno del CED.

Componenti fisiche

Componente	Descrizione
Soggetti Interni	**Descrizione sintetica (es. soggetti facenti parte o meno del personale tecnico informatico, descrizione delle attività svolte in relazione ai trattamenti in esame, formazione ricevuta, procedure che ne disciplinano le mansioni, relazioni con altre componenti**

	soggetti autorizzati afferenti alla S.S. Progetti innovativi e supporto al controllo di gestione dell'ASL CN2. il Responsabile del progetto è la dott.ssa Giuliana Chiesa. Tutti i soggetti sono autorizzati ai sensi dell'art. 29 GDPR.
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)**
	Computer Angels S.r.l.s.

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:

Anonimizzazione del data set oggetto del progetto Trust Alert

6. Diritti e principi fondamentali

Diritti

Accesso	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.

Rettifica	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.
Cancellazione	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.
Portabilità	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.
Opposizione	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.

Limitazione di trattamento	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.
Revoca del consenso	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.
Diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato	Il trattamento di dati oggetto del presente progetto di ricerca trova il proprio fondamento di liceità nel combinato disposto nell'art. 9 par. 2 l. j) GDPR con l'articolo 110 del codice privacy. Non è infatti possibile informare (ferma la pubblicazione dell'informativa ex art. 13 GDPR sul sito istituzionale dell'ASL) e raccogliere il consenso presso ciascun interessato a causa dello sforzo sproporzionato per contattarli. Il trattamento dei dati consiste nella sola anonimizzazione degli stessi. Pertanto, una volta effettuata l'anonimizzazione dei dati non sarà più possibile risalire all'identità degli interessati che dunque non potranno esercitare il presente diritto.

Principi

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato	Liceità: combinato disposto dell'art. 9 par. 2 l. j) GDPR con l'art. 110 del codice privacy; Correttezza e trasparenza: informativa ex art.13 GDPR pubblicata sul sito internet istituzionale dell'ASL.

I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità	la limitazione delle finalità è garantita dal fatto che i dati personali verranno trattati al solo dine di renderli anonimi.
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	il dato personale verrà trattato al solo scopo di renderlo anonimo per il tempo necessario al raggiungimento di tale finalità.
I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali	il trattamento dei dati personale avviene all'interno del perimetro aziendale, attraverso la messa a disposizione di una macchina virtuale contenente un data set che verrà elaborato per l'anonimizzazione dei dati.

7. Valutazione del rischio

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

$R_1 = f(M, p)$

IMPATTO (M)

LIEVE	1
MEDIO	2
ALTO	3
ALTISSIMO	4

X

PROBABILITÀ (p)

IMPROBABILE	1
POCO PROBABILE	2
PROBABILE	3
ALTAMENTE PROBABILE	4

=

RISCHIO INIZIALE (R)

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

Dove per:

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

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

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

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

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

$$R_2 = R_1 - (M_n)$$

dove per:

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

All'interno del presente passaggio saranno presenti, in ordine

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

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

7.1 Misure di sicurezza

Misure di sicurezza trasversali relative ai trattamenti

Categoria	Misura di sicurezza	Stato di adozione e implementazione

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

Misure di sicurezza trasversali relative agli asset

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

Misure di sicurezza specifiche relative al trattamento

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

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

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

Misure di sicurezza specifiche relative agli asset correlati con il trattamento

Nessun elemento selezionato

7.2 Valutazione del rischio

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

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

	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata	Applicata
	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata

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**	
Nessuna		Nessuna	

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

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

	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna		Nessuna	

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

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

	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna		Nessuna	

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	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
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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

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

	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna		Nessuna	

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

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

	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna		Nessuna	

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

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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	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
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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	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
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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	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
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata	Applicata

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

Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata

	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna	Nessuna	

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	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
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	Applicata	Applicata

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

	È mantenuto un inventario delle utenze amministrative.	Applicata	Applicata
	Le utenze amministrative sono formalmente autorizzate.	Applicata	Applicata
Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata	Applicata
	Documento/ regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	Applicata	Applicata
	Formazione relativa al processo/applicativo in esame	Applicata	Applicata
	Formazione relativa alla normativa sulla protezione dei dati	Applicata	Applicata
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata	Applicata

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata	Applicata
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	Applicata	Applicata
	Sono in vigore procedure per garantire la minimizzazione dei dati	Applicata	Applicata
	Sono in vigore procedure gestire la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure minimizzare la conservazione dei dati.	Applicata	Applicata
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata	Applicata
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**	
Nessuna		Nessuna	

Riassunto ed esito dell'analisi del rischio

Minaccia	Rischio iniziale	Rischio residuo
Malfunzionamento o distruzione di strumentazione it (client)	1	1
Malfunzionamento o distruzione di strumentazione it (server)	1	1
Malfunzionamento o distruzione di strumentazione it (rete)	1	1
Intercettazione del traffico	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
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 residuo

Basso

8. Coinvolgimento delle parti interessate

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

9. Note

Il Titolare del trattamento

ASL CN 2