



VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

DPIA (Data Protection Impact Assessment)

Trattamento in esame: Ricerca e sperimentazione clinica Sindrome di Rett (RTT)

Descrizione del trattamento

Attività di Ricerca e sperimentazione clinica sulla sindrome di Rett (RTT), nonché le attività amministrative connesse dell'ISTC e dell'AIRETT.

Team elaborazione DPIA

Il presente documento è stato elaborato da un gruppo multidisciplinare.

Composizione del Gruppo di Lavoro:
Maurizzi Giada e Brusadin Tania

All'interno del GdL il DPO Ragagni Davide ha fornito consulenza e supporto giuridico.

Contitolare del trattamento

Consiglio Nazionale delle Ricerche (CNR) e dall'Associazione Italiana Sindrome di Rett (AIRETT).

RPD/DPO

Maurizzi Giada e Brusadin Tania

Data di avvio

01 gennaio 2024

Data validazione

26 giugno 2024

Frequenza di aggiornamento prevista

Annuale

Sommario

PREMESSA	2
ANALISI DEL CONTESTO	3
1. Quale è il trattamento preso in considerazione?	3
1.2 Quali sono le responsabilità connesse al trattamento?	3
1.3 Ci sono standard applicabili al trattamento?	5
1.4 Quali sono i dati trattati?	5
1.5 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?	5
1.6 Quali sono le risorse di supporto ai dati?	6
PRINCIPI FONDAMENTALI	7
2.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?	7
2.2. Quali sono le basi legali che rendono lecito il trattamento?	7
2.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	7
2.4 I dati sono esatti e aggiornati?	8
2.5 Qual è il periodo di conservazione dei dati?	8
2.6 Come sono informati del trattamento gli interessati?	8
2.7 Ove applicabile: come si ottiene il consenso degli interessati?	8
2.8 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?	8
2.9 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	9
2.10 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	9
2.11 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	9
RISCHI	9
3.1 Rischio in caso di accesso illegittimo ai dati	10
3.2 Rischio in caso di modifiche indesiderate dei dati	11
3.3 Rischio in caso di perdita di dati	12

PREMESSA

Presso l'Azienda l'attività di Ricerca è svolta in piena coerenza con le disposizioni dell'ordinamento in materia di protezione dei dati.

Nella norma, per ogni Ricerca è sottoposto all'autorizzazione del Comitato Etico (CE) competente un protocollo corredato di un dettagliato documento informativo per l'acquisizione del consenso informato, ove previsto.

È prevista, anche, la consegna di una Informativa per il trattamento dei dati personali dedicata, redatta ai sensi dell'art. 13 del GDPR (o dell'art. 14 qualora i dati siano stati raccolti presso altro titolare). Analogamente è prevista l'acquisizione di uno specifico Consenso al trattamento dei dati personali, ove necessario e possibile ai sensi degli artt. 110 e 110-bis del Codice privacy.

Coerentemente con il Provvedimento dell'Autorità Garante n. 146 del 5 giugno 2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101" (cfr provvedimento AG per la protezione dei dati personali) per ogni Ricerca è prevista la redazione del progetto denominato, in Area Vasta Emilia Centrale, come "Data Confidentiality and Security Plan" (DCSP). Documento che dà conto della tipologia dei dati trattati e delle operazioni più significative da realizzare col trattamento in questione.

Inoltre, nel caso in cui il protocollo preveda la comunicazione dei dati personali tra i centri partecipanti/collaboranti, di norma sono stipulati specifici accordi per la protezione dei dati.

ANALISI DEL CONTESTO

1. Quale è il trattamento preso in considerazione?

Il trattamento dei dati personali nel contesto della sperimentazione riguarda la raccolta, l'elaborazione e la conservazione dei dati relativi ai soggetti di età compresa tra **3 e 30 anni** con Sindrome di Rett (RTT) coinvolti nello studio. La sperimentazione è condotta dall'Istituto di Scienze e Tecnologie della Cognizione (ISTC) del CNR in collaborazione con l'Associazione Italiana Sindrome di Rett (AIRETT). I dati saranno raccolti tramite moduli di consenso informato, osservazioni dirette e video registrazioni durante le sedute sperimentali; a tal fine si prevede l'utilizzo di risorse interne dell'ISTC-CNR e piattaforme cloud per la condivisione e conservazione dei dati. Le finalità del trattamento includono:

- Valutazione dell'efficacia: Misurare l'impatto dei giochi interattivi sulle competenze senso-motorie e sociali dei partecipanti.
- Ricerca scientifica: Contribuire alla comprensione delle esigenze e delle capacità dei soggetti con RTT attraverso studi scientifici.
- Conservazione per ricerche future: Archiviare i dati raccolti per futuri studi e analisi scientifiche.

Il progetto ha una durata di **36 mesi**. I dati saranno conservati per un periodo di **7 anni** oltre la fine del progetto per consentire ulteriori analisi e pubblicazioni scientifiche.

Ci si aspetta che la sperimentazione e il relativo trattamento dei dati personali dei soggetti coinvolti porti ad un miglioramento delle competenze senso-motorie e sociali nei soggetti con RTT e alla produzione di dati scientifici utili per ulteriori studi sulla Sindrome RTT e per la validazione dei giochi interattivi come strumenti terapeutici.

1.2 Quali sono le responsabilità connesse al trattamento?

Il trattamento è condotto congiuntamente dall'ISTC del CNR e dall'Associazione Italiana Sindrome di Rett, **contitolari** del trattamento ai sensi dell'art. 26 del GDPR. Dati di contatto:

- il CNR – Consiglio Nazionale delle Ricerche con sede legale in Piazzale Aldo Moro - 00185, Roma (RM) raggiungibile al seguente indirizzo PEC: protocollo-ammcen@pec.cnr.it rappresentante per il presente trattamento l'Istituto di Scienze e Tecnologie della Cognizione (ISTC).
- l'AIRETT - Associazione Italiana Sindrome di Rett con sede legale in Viale Bracci, 1 - 53100 Siena raggiungibile al seguente indirizzo e-mail: centrorett@airett.it

Tra le responsabilità dei Titolari del trattamento figurano:

- Determinazione delle **finalità** e dei **mezzi del trattamento** e informare adeguatamente i partecipanti e i loro tutori legali sulle modalità e le finalità del trattamento dei dati personali;
- Definire le **misure tecniche e organizzative** adeguate per garantire un livello di **sicurezza** adeguato al rischio;
- Garantire che i **diritti degli interessati** siano rispettati e facilmente esercitabili;
- Condurre **valutazioni di impatto** per identificare e mitigare i rischi associati al trattamento dei dati personali;
- Garantire che il trattamento dei dati personali sia conforme al **GDPR** e ad altre normative applicabili;
- Designare i **Responsabile del trattamento** ai sensi dell'art. 28 del GDPR;
- Entrambe le organizzazioni devono designare un **DPO**, essendo enti/organismi pubblici, che fungerà da punto di contatto per qualsiasi questione relativa alla protezione dei dati personali dei partecipanti;

Dati di contatto dei responsabili della protezione dei dati (RPD):

- Punto di contatto del responsabile del CNR per l'esercizio dei diritti dell'interessato per i trattamenti di cui alla presente informativa è Tania Brusadin raggiungibile al seguente indirizzo PEC: brusadin.tania@pec.cnr.it
- Punto di contatto del responsabile dell'AIRETT per l'esercizio dei diritti dell'interessato per i trattamenti di cui alla presente informativa è Giada Maurizzi raggiungibile al seguente indirizzo PEC: maurizzi.giada@pec.airett.it

Tra le responsabilità del Responsabile della protezione dei dati (RPD) figurano:

- Trattare i dati personali solo su istruzione documentata dei contitolari del trattamento;
- Implementare **misure tecniche e organizzative** adeguate per garantire un livello di sicurezza adeguato;
- Assistere i contitolari del trattamento nel garantire il rispetto degli **obblighi** in materia di protezione dei dati;
- **Notificare tempestivamente** ai titolari del trattamento qualsiasi violazione dei dati personali;
- Tenere un **registro delle attività** di trattamento svolte per conto dei titolari;

1.3 Ci sono standard applicabili al trattamento?

- **Regolamento Generale sulla Protezione dei Dati (GDPR)**: tutti i trattamenti dei dati personali devono rispettare i principi di **trasparenza**, **minimizzazione dei dati**, **sicurezza** dei dati, **diritti** dei partecipanti e **periodi di conservazione** dei dati;
- **ISO/IEC 27001**: è uno standard internazionale per la gestione della sicurezza delle informazioni;
- **Linee guida del Garante per la protezione dei dati personali**;
- **Certificazione ISO 27701** per la gestione delle informazioni sulla privacy;
- **Linee guida ICH-GCP** per la conduzione di sperimentazioni cliniche che assicurano la protezione dei diritti, della sicurezza e del benessere dei partecipanti.;
- **Dichiarazione di Helsinki** per principi etici nella ricerca medica;

1.4 Quali sono i dati trattati?

I dati personali raccolti includono:

- **Dati anagrafici**: nome, cognome, data di nascita, indirizzo e contatti.
- **Dati sanitari**: diagnosi di Sindrome di Rett, storia clinica.
- **Dati comportamentali**: osservazioni e registrazioni video delle sedute sperimentali.
- **Dati di contatto dei genitori/tutori**: nome, cognome, indirizzo e contatti.
- **Dati sperimentali**: informazioni sulle interazioni dei soggetti con i giochi sperimentali, comprese le risposte motorie e le interazioni sociali durante le sessioni di gioco.

1.5 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)¹?

Il ciclo di vita dei dati nel contesto della sperimentazione prevede una serie di fasi, ognuna delle quali è attentamente progettata per garantire la sicurezza, la qualità e la conformità alle normative vigenti.

1. Raccolta dei Dati: i dati vengono raccolti attraverso moduli di consenso informato, questionari, interviste, osservazioni dirette e registrazioni video delle interazioni dei partecipanti con i giochi interattivi, inclusa la documentazione medica.
2. Elaborazione dei Dati: i dati raccolti sono trascritti e annotati, archiviati in un database sicuro, con backup periodici e un rigoroso controllo di qualità per assicurare accuratezza e completezza.
3. Analisi dei Dati: I dati vengono pre-elaborati per rimuovere errori e standardizzare il formato, poi analizzati statisticamente per esaminare le risposte dei partecipanti, con i risultati documentati nei report di ricerca.
4. Conservazione dei Dati: i dati sono conservati per 36 mesi più 7 anni in un ambiente sicuro, sia su server interni che su piattaforme cloud, con accesso limitato al personale autorizzato.

¹ Vedi appendice A

5. Condivisione dei Dati: i dati possono essere condivisi con ricercatori e partner, pubblicati in riviste scientifiche con anonimizzazione, e trasferiti ad altre organizzazioni rispettando le normative di protezione dei dati.
6. Monitoraggio e Revisione: Audit regolari garantiranno la conformità con le normative sulla protezione dei dati e le politiche verranno aggiornate per riflettere nuove normative e best practice di sicurezza.
7. Gestione delle Violazioni dei Dati: In caso di violazioni dei dati, esistono piani di risposta che includono la notifica ai partecipanti e alle autorità competenti, con registrazione e analisi delle violazioni per migliorare le misure di sicurezza.
8. Cancellazione dei Dati: Al termine del periodo di conservazione di 7 anni, i dati personali saranno cancellati o anonimizzati in modo sicuro, con documentazione e verifica della cancellazione.

1.6 Quali sono le risorse di supporto ai dati?

Per garantire la sicurezza, l'integrità e l'efficacia del trattamento dei dati durante il progetto di ricerca, sono utilizzate diverse risorse di supporto, in particolare:

- Infrastruttura Tecnologica

Server e Sistemi di Archiviazione:

- Server interni: utilizzati per l'archiviazione sicura dei dati sensibili raccolti;
- Cloud Storage: piattaforme per la condivisione e la conservazione dei dati, con backup regolari e accesso controllato;

Software di Gestione dei Dati:

- Database Management Systems (DBMS): sistemi per la gestione e la manipolazione dei dati raccolti;
- Software di Analisi Statistica: strumenti come STATA, R o Python per l'analisi dei dati;

Software di Backup: soluzioni per il backup periodico e sicuro dei dati;

- Risorse Umane

- Data Protection Officer (DPO): responsabile della conformità alle normative sulla protezione dei dati e punto di contatto per qualsiasi questione relativa alla protezione dei dati personali;
- Ricercatori e Analisti: personale qualificato per la raccolta, l'elaborazione e l'analisi dei dati;
- Personale IT: tecnici specializzati nella gestione e sicurezza dell'infrastruttura IT;

- Strumenti di Monitoraggio e Audit

- Sistemi di Monitoraggio;
- Sistemi di Log Management: Per monitorare e registrare tutte le attività di accesso e modifica dei dati.
- Software di Audit: Strumenti per condurre audit regolari e garantire la conformità con le politiche di protezione dei dati e le normative.

PRINCIPI FONDAMENTALI

2.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono specifici, espliciti e legittimi. La ricerca mira a valutare l'efficacia dei giochi interattivi sviluppati dall'ISTC-CNR nel migliorare le competenze sensorie e sociali nei soggetti con Sindrome di Rett (RTT). La raccolta dei dati comportamentali e sociali tramite sedute video registrate è necessaria per raggiungere questi obiettivi scientifici. Inoltre, la conservazione dei dati per ulteriori ricerche scientifiche è una pratica conforme agli standard etici e legali vigenti, garantendo la protezione dei dati personali.

2.2. Quali sono le basi legali che rendono lecito il trattamento?

Nel contesto della sperimentazione clinica per soggetti con Sindrome di Rett, il trattamento dei dati personali deve avvenire in conformità con le basi legali previste dal Regolamento Generale sulla Protezione dei Dati (**Regolamento (UE) 2016/679 - GDPR**). In particolare, rendono lecito il trattamento dei dati personali:

- **Art. 6 (1)** GDPR;
- **Art. 9 (2) (a,i,j)** GDPR;
- **Art. 35** GDPR;
- **Considerando 45** GDPR;
- **Considerando 47** GDPR;
- **Art. 29 Working Party**, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679;
- Garante per la protezione dei dati personali, **provvedimento n. 467** dell'11 ottobre 2018;
- **D. lgs. 196/2003**, Codice in materia di protezione dei dati personali - Art. 110;

2.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti nel progetto sono adeguati, pertinenti e limitati alle specifiche necessità della ricerca. I dati anagrafici consentono un'identificazione univoca dei partecipanti e supportano il follow-up e le comunicazioni necessarie. I dati sanitari, come la diagnosi di Sindrome di Rett e la storia clinica, sono essenziali per confermare l'idoneità dei partecipanti e valutare l'efficacia del trattamento nel contesto clinico. Le osservazioni e le registrazioni video forniscono dati comportamentali dettagliati, utili per analizzare l'impatto dei trattamenti sperimentali. I dati di contatto dei genitori/tutori sono cruciali per garantire una comunicazione continua e il consenso informato. L'approccio include la minimizzazione dei dati, con valutazioni preventive, pseudonimizzazione/anonimizzazione e revisioni periodiche per mantenere la pertinenza e la sicurezza dei dati.

2.4 I dati sono esatti e aggiornati?

I dati raccolti sono mantenuti esatti e aggiornati attraverso la verifica iniziale accurata dei dati anagrafici e di contatto dei partecipanti. La conferma della diagnosi e la gestione della storia clinica dettagliata assicurano che i dati sanitari siano precisi e aggiornati, supportando una valutazione corretta dei partecipanti. Le osservazioni comportamentali, incluse le registrazioni video, sono gestite con protocolli standardizzati per garantire la documentazione dettagliata e obiettiva. Procedure chiare per la correzione e l'aggiornamento dei dati personali consentono agli interessati di segnalare e correggere errori, mentre la formazione continua del personale e il monitoraggio della qualità dei dati assicurano la precisione e l'integrità delle informazioni raccolte.

2.5 Qual è il periodo di conservazione dei dati?

In conformità alle *Linee Guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali (24 luglio 2008)* il periodo di conservazione dei dati durante la sperimentazione sulla sindrome di Rett comprende un arco temporale di 10 anni, di cui 36 mesi relativi alla sperimentazione e 7 anni di conservazione successiva.

2.6 Come sono informati del trattamento gli interessati?

Gli interessati sono informati dettagliatamente sul trattamento dei loro dati attraverso una varietà di strumenti. Questi includono informative scritte come brochure e lettere distribuite direttamente o online ai partecipanti e ai loro tutori legali. Inoltre, sono disponibili sezioni dedicate sui siti web dell'ISTC-CNR e dell'Associazione Italiana Sindrome di Rett, moduli di consenso informato che devono essere firmati per confermare l'accettazione delle condizioni del trattamento dati, sessioni informative condotte dai ricercatori per chiarire il progetto e rispondere a domande, e video esplicativi online per illustrare in dettaglio le finalità del trattamento dei dati.

2.7 Ove applicabile: come si ottiene il consenso degli interessati?

Per raccogliere il consenso degli interessati al trattamento dei dati personali per il progetto di ricerca congiunto tra l'ISTC-CNR e l'Associazione Italiana Sindrome di Rett viene utilizzato il Modulo di consenso informato presente in appendice all'Informativa per la privacy, contenente tutte le informazioni necessarie e raccolte in conformità con l'articolo 13 del GDPR. Il consenso viene raccolto in forma scritta, con la firma del modulo di consenso informato da parte dell'interessato o del tutore legale.

2.8 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo agli RDP. È possibile effettuare la richiesta tramite modulo online disponibile sui siti web ufficiali dell'ISTC-CNR e dell'Associazione Italiana Sindrome di Rett, inviando il modulo compilato via email o tramite una sezione dedicata sul sito. È anche possibile contattare telefonicamente i titolari del trattamento per avviare la procedura di accesso. I dati personali saranno forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico (ad esempio, CSV o JSON). Gli interessati possono richiedere che i

dati siano trasmessi direttamente a un altro titolare del trattamento indicato nella richiesta, previa presentazione della documentazione necessaria per dimostrare la loro autorità.

2.9 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo agli RDP. È possibile presentare una richiesta di rettifica dei dati personali indicando le informazioni corrette o aggiornate, tramite comunicazione scritta o online utilizzando i moduli predisposti. Il titolare del trattamento esaminerà la richiesta entro un mese, prorogabile di due mesi in casi complessi. È altresì possibile richiedere la cancellazione dei dati personali specificando i motivi e fornendo le informazioni necessarie per identificare i dati, con esclusione di casi specifici come obblighi legali o difese giudiziarie.

2.10 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo a [indirizzo email]. È possibile richiedere la limitazione del trattamento dei dati personali in determinate circostanze, come quando si contesta l'accuratezza dei dati o quando il trattamento è illecito ma l'interessato richiede la limitazione invece della cancellazione. È altresì possibile opporsi al trattamento dei dati personali, ad esempio per finalità di marketing diretto, inviando una comunicazione scritta o utilizzando i moduli predisposti.

2.11 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I Responsabili del trattamento sono stati nominati per gestire servizi in outsourcing che coinvolgono il trattamento di dati personali per conto del Titolare. Il contratto tra il Titolare e il Responsabile del trattamento, conforme all'articolo 28 del GDPR, specifica le istruzioni dettagliate per il trattamento dei dati personali fornite dal Titolare. Queste istruzioni sono formalizzate in un accordo giuridico vincolante e definiscono il tipo di dati trattati, le misure di sicurezza da implementare, la collaborazione necessaria per gestire le richieste degli interessati (come accesso e cancellazione) e altri compiti specifici come la notifica di violazioni dei dati o la valutazione dell'impatto sulla protezione dei dati (DPIA).

RISCHI

Individuazione delle misure di sicurezza esistenti o pianificate

Misure tecniche

Crittografia
Anonimizzazione
Partizionamento

Misure organizzative

Prevenzione delle fonti di rischio
Politica di tutela della privacy
Gestione delle politiche di tutela della privacy

Controllo degli accessi logici
Tracciabilità
Archiviazione
Sicurezza dei documenti cartacei
Minimizzazione dei dati
Sicurezza dei siti web
Backup
Sicurezza dei canali informatici
Sicurezza dell'hardware

Gestione dei rischi
Gestione del personale
Gestire gli incidenti di sicurezza
Gestire le violazioni dei dati personali

3.1 Rischio in caso di accesso illegittimo ai dati

- *Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?* Violazione della privacy, Furto d'identità, Discriminazione, Danno psicologico, Perdita di benefici futuri, Danno finanziario, Impatto sulla sicurezza personale, Compromissione della confidenzialità dei dati, Danno della reputazione personale

- *Quali sono le principali minacce che potrebbero concretizzare il rischio?* Accesso non autorizzato, Perdita o furto di dati, Perdita o furto di dispositivi, Vulnerabilità software, Errore umano, gestione inadeguata dei backup, Inadeguata formazione del personale

- *Quali sono le fonti di rischio?* Errore umano, attacco interno, fonte non umana, malware e ransomware, perdita o furto dispositivi, servizi di terze parti, disastri ambientali

- *Quali misure fra quelle individuate contribuiscono a mitigare il rischio?*

Controllo degli accessi logici, Backup, Gestione del personale, Prevenzione delle fonti di rischio, Sicurezza dell'hardware, Sicurezza dei siti web, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?



(Indefinito) Trascurabile Limitato Importante Massimo

Il rischio è limitato perchè gli impatti si possono evitare tramite le misure pianificate.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? ^



Il rischio è importante perchè le minacce e le fonti di rischio sono varie, rendendo più difficile il lavoro di individuazione delle misure.

3.2 Rischio in caso di modifiche indesiderate dei dati

- Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Danno della reputazione personale, Danno psicologico, Furto d'identità

- Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio? Accesso non autorizzato, Errore umano, Perdita o furto di dati, Inadeguata formazione del personale

- Quali sono le fonti di rischio? Perdita o furto dispositivi, disastri ambientali, malware e ransomware

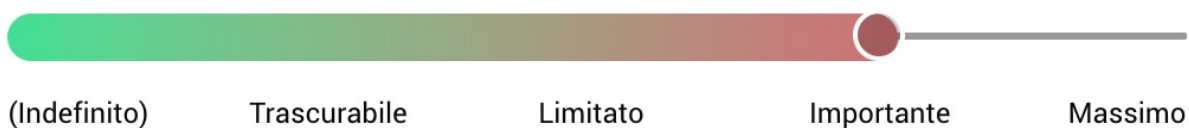
- Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Anonimizzazione, Sicurezza dei siti web, Sicurezza dei canali informatici, Crittografia, Prevenzione delle fonti di rischio

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate? ^



Il rischio è limitato perchè le misure vanno a ridurre gli impatti.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate? ^



Il rischio è importante perchè non tutte le minacce possono essere controllate

3.3 Rischio in caso di perdita di dati

- Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi? Compromissione della confidenzialità dei dati, Perdita di benefici futuri, Danno psicologico, Discriminazione

- Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio? Accesso non autorizzato, Errore umano, Perdita o furto di dati, Vulnerabilità software

- Quali sono le fonti di rischio?

attacco interno, disastri ambientali, errore umano, malware e ransomware, servizi di terze parti

- Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? Controllo degli accessi logici, Tracciabilità, Backup, Minimizzazione dei dati, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?



La perdita dei dati ha impatti importanti sugli individui.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?



La perdita dei dati potrebbe derivare da diverse minacce e fonti di rischio ma le misure sono tutte pianificate affinché ciò non si verifichi

