GDPR RISK ASSESSMENT TOOL

ALLEGATO TECNICO PER LA VALUTAZIONE DEI RISCHI

COMPRENDERE LA VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

Obiettivo di questo Allegato Tecnico è fornire uno strumento per la Valutazione dei rischi per i diritti e le libertà delle persone fisiche con riferimento all'Attività di trattamento oggetto di studio, **anche nel caso di Valutazione di impatto**.
Mediante questo strumento possono essere individuati i possibili rischi per i diritti e le libertà degli interessati, valutandone il livello in considerazione delle vulnerabilità, delle possibile minacce alle operazioni di trattamento e delle possibili conseguenze, ragionando in **termini di probabilità e gravità dell'impatto**, con riferimento alla ***natura*** , al ***contesto*** , alle ***finalità*** e all'***ambito di applicazione*** ; possono poi essere ponderati rispetto al livello di **rischio ritenuto accettabile**, e poi accettati ovvero rimessi alla consultazione dell'Autorità di controllo (nel caso ci si trovi nell'ambito della Valutazione di impatto).

COME FUNZIONA?

RISCHIO INERENTE

Mediante i pulsanti di navigazione nella parte superiore è possibile navigare agevolmente tra i diversi Fogli di questo Modello Excel; I primi 4 spiegano metodologia, criteri e metriche utilizzate; Ci sono poi i Fogli di ***impostazione iniziale :*** **Finalità, Natura, Ambito di Applicazione** nei quali mediante domande e risposte vengono poi forniti, nel Foglio **Rischio Accettabile**, preziose indicazioni e suggerimenti da considerare nella fase di Analisi, e viene determinato il ***Fattore di contesto*** che influisce il livello di probabilità e gravità dei rischi; sempre in questo Foglio, viene impostato il livello di ***rischio accettabile*** (medio o basso).
I Fogli **Impatto** e **Probabilità** sono i più laboriosi da compilare in quanto vanno determinati e giustificati i possibili livelli di gravità delle conseguenze, e il livello di probabilità di accadimento di eventi dannosi.
I Fogli **Vulnerabilità** e **Rischio Inerente** sono riepilogativi, utili a identificare le aree più sensibili da attenzionare e sulle quali programmare interventi.
Nei fogli **Misure** e **Governance** vanno invece specificate le misure organizzative e tecniche in essere, in termini di livello di adeguatezza, e il grado di gestione strutturata dei controlli sull'applicazione.
I Fogli **Efficacia** e **Rischio Residuo**, risultati dell'Analisi, mostrano i cruscotti finali, e il Foglio **Registro Rischi** consente di impostare le date di esecuzione per monitorare e gestire la valutazione nel tempo.

CONDIZIONI DI UTILIZZO - CREDITS

RINGRAZIAMENTI:
Si ringraziano tutti coloro che, appassionati della materia, in questi anni hanno contribuito a fornire spunti, critiche e osservazioni sull'evoluzione di questo strumento, la cui prima versione nasce nel 2018. In particolare ringrazio (l'ordine è irrilevante, spero di ricordarmi tutti e chiedo scusa per eventuali omissioni):
Cristina Cecere, Cesare Gallotti, Francesca Falbo, Giuseppe D'Acquisto, Fabio Fricano, Manuela Sforza, Salvatore Coppola, Gianmarco Cenci, Luisa Tucci, Angelica Alessi, Giovanni Battista Gallus, Gianni Lucatorto, Renato Fa, Diego Padovan, Paola Limatola, Sebastiano Plutino, Daniele Santucci.

Inoltre, devo ringraziare l'Autorità Garante per la protezione dati personali, tutte le Associazioni di cui faccio parte e gli Enti formativi per la grande qualità della formazione erogata:
Associazione Nazionale Protezione Dati, Istituto Italiano per la Privacy e la Valorizzazione dei dati, Federprivacy e TUV, InVeo, Osservatorio 679, Università Europea di Roma, Fondazione Basso.
Concludo con un sentito grazie per i docenti dei corsi specifici o momenti formativi e di confronto sul Risk assessment che ho seguito, in particolare:
Giuseppe D'Acquisto, Monica Perego, Manuela Sforza, Riccardo Giannetti.

GDPR RISK ASSESSMENT TOOL

COMPRENDERE LA VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

(Considerando 75 GDPR) I **rischi per i diritti e le libertà delle persone fisiche**, aventi probabilità e gravità diverse, possono derivare da **trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale**, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

(Considerando 76 GDPR) La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla **natura**, all'**ambito di applicazione**, al **contesto** e alle **finalità del trattamento**. *Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano* ***un rischio o un rischio elevato*** .

E' quindi importante definire livelli di rischio per gli interessati, e stabilirne probabilità e gravità per ogni singola attività di trattamento

In questo Tool per il livello di rischio viene utilizzata la seguente tassonomia:

Livello	RISCHIO PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI
Basso	Il rischio per gli interessati è accettabile dall'organizzazione mediante misure organizzative e tecniche idonee, ma deve continuare ad essere monitorato per controllare che cambiamenti non incrementino il livello di rischio
Medio	Il rischio medio per gli interessati potrebbe essere accettabile ma l'adozione delle misure tecnico-organizzative deve essere monitorata su basi regolari, e il trattamento può essere sottoposto a ulteriori considerazioni
Alto	Il rischio per le persone interessate al trattamento è ad un livello non accettabile e necessita un rafforzamento delle misure di mitigazione.
Elevato / Critico	Il rischio per gli interessati si presenta elevato o molto critico, mantenendo un livello non accettabile per l'organizzazione e necessitando l'aggiunta di ulteriori controlli a prevenzione/mitigazione dello stesso.

Se è il rischio è l'effetto dell'incertezza sugli obiettivi, quali sono gli obiettivi da raggiungere?

Evitare che gli effetti complessivi del trattamento possano generare conseguenze negative per le persone

Es. Limitazione dei Diritti
Diritto alla vita e alla integrità psico-fisica
Diritto alla dignità personale
Diritto al nome e all'immagine
Diritto alla sicurezza sociale e alla capacità giuridica
Diritto al rispetto della vita privata familiare
Diritto alla non discriminazione e al pari trattamento
Diritto all'istruzione e alla cultura
Diritto al lavoro
Diritto all'alloggio
Diritto alla tutela giurisdizionale
Diritto al rispetto del domicilio
Diritto al rispetto della corrispondenza

Es. Limitazione delle libertà
Libertà personale
Libertà e inviolabilità del domicilio
Libertà di manifestazione del pensiero
Libertà di religione
Libertà di riunione e associazione
Libertà di iniziativa economica
Libertà di matrimonio e procreazione
Libertà di insegnamento

Il DIRITTO ALLA PROTEZIONE DATI intende proteggere le persone da effetti negativi sui diritti e le libertà individuali con riferimento alle informazioni riferibili direttamente o indirettamente alle persone interessate

Quali sono i rischi che incombono sui trattamenti di dati personali? Sicuramente l'Art. 32 del GDPR ce ne indica alcuni al paragrafo 2; ma oltre ai rischi per la sicurezza, che mettono a repentaglio la riservatezza, l'integrità e la disponibilità delle informazioni, è necessario includere i rischi per le violazioni dei principi fondamentali, per la "safety" degli individui; ci viene dunque in soccorso la ISO/IEC 29134 per estendere il novero degli scenari di rischio da considerare, come sintetizzato di seguito.

Definizioni essenziali:

Ri **RISCHIO INERENTE:** è il rischio "intrinseco", "potenziale", la combinazione di probabilità di occorrenza di un evento minaccioso e della gravità dell'impatto in assenza di misure di mitigazione

Rr **RISCHIO RESIDUO** è il rischio dopo l'applicazione di misure di mitigazione con azioni e controlli organizzativi e tecnici

Ra **RISCHIO ACCETTABILE** è il rischio che l'Organizzazione decide di accettare per instaurare un certo processo o attività

Valutazione del rischio (risk assessment):

processo complessivo di identificazione, analisi e ponderazione del rischio.

Un metodo valido di valutazione del rischio dovrebbe avere le seguenti caratteristiche:

- ***completezza***: devono essere considerati, al giusto livello di sintesi, tutti gli asset, tutte le minacce e tutte le vulnerabilità;
- ***ripetibilità***: valutazioni condotte nello stesso contesto e nelle stesse condizioni devono dare gli stessi risultati;
- ***comparabilità***: valutazioni condotte in tempi diversi nello stesso contesto devono permettere di comprendere se il rischio è cambiato e come;
- ***coerenza***: a fronte di valori di asset, minacce e vulnerabilità più elevati di altri, il livello di rischio deve essere più elevato.

Scenari di rischio

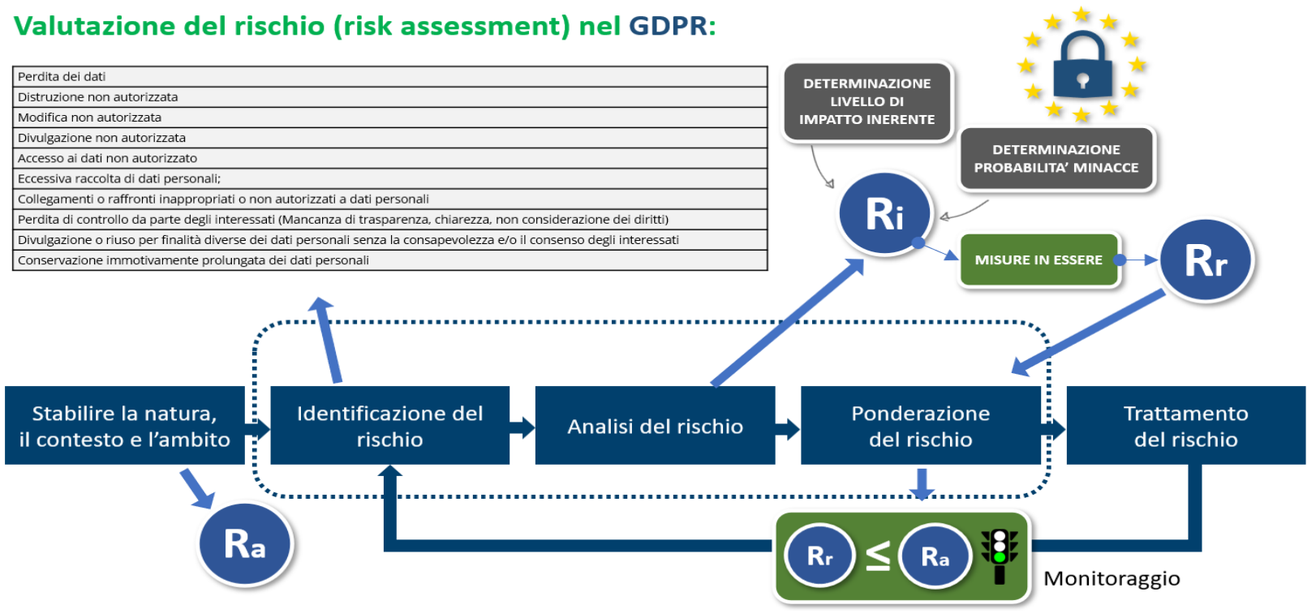
Perdita dei dati	Violazione DISPONIBILITA'
Distruzione non autorizzata	
Modifica indesiderata o non autorizzata	Violazione INTEGRITA' E ESATTEZZA
Divulgazione non autorizzata	Violazione RISERVATEZZA
Accesso ai dati non autorizzato o illegittimo	
Eccessiva raccolta di dati personali;	Violazione NECESSITA' E PROPORZIONALITA'
Collegamenti o raffronti inappropriati o non autorizzati di dati personali	
Perdita di controllo da parte degli interessati (mancanza di trasparenza, chiarezza, non considerazione dei diritti)	Violazione LICEITA'. TRASPARENZA E CORRETTEZZA
Divulgazione o riuso per finalità diverse dei dati personali senza la consapevolezza e/o il consenso degli interessati	
Conservazione immotivamente prolungata dei dati personali	Violazione LIMITAZIONE DELLA CONSERVAZIONE

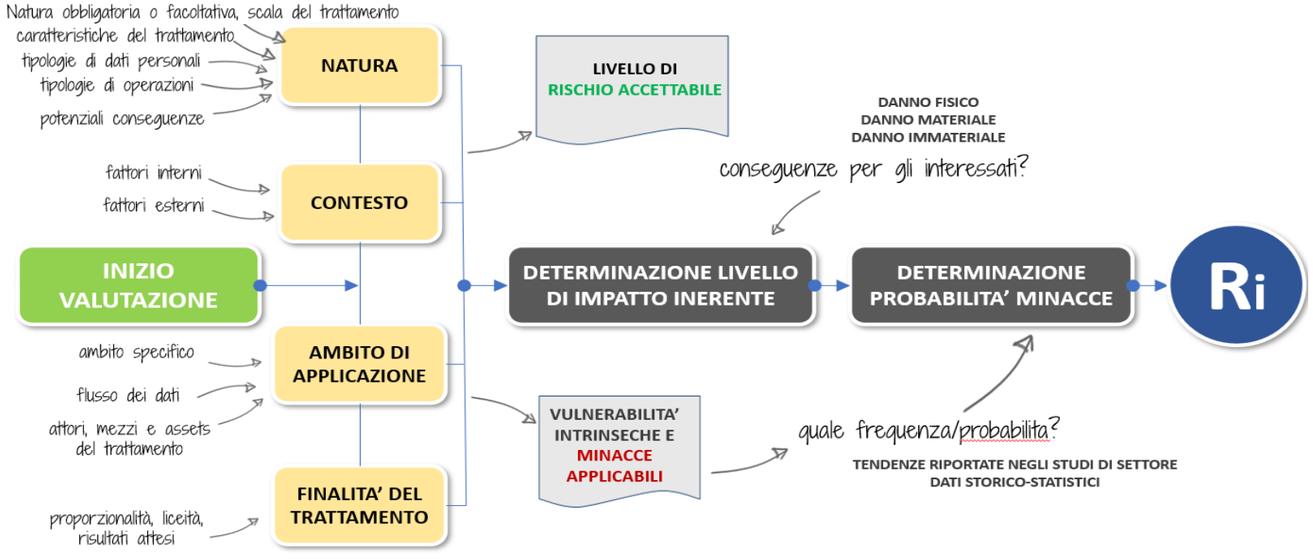
ISO/IEC 29134 - paragrafo 6.4.4.1 sull'identificazione dei rischi privacy, la norma invita a considerare altri aspetti

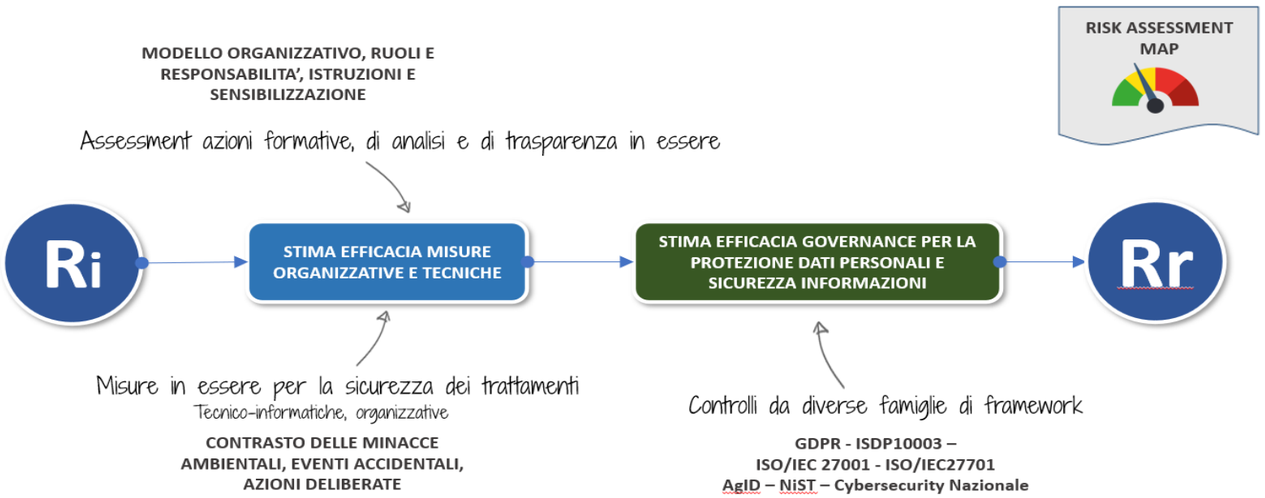
Anche il CNIL ne ravvisa la necessità: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

Valutazione del rischio (risk assessment) nel GDPR:

Perdita dei dati
Distruzione non autorizzata
Modifica non autorizzata
Divulgazione non autorizzata
Accesso ai dati non autorizzato
Eccessiva raccolta di dati personali;
Collegamenti o raffronti inappropriati o non autorizzati a dati personali
Perdita di controllo da parte degli interessati (Mancanza di trasparenza, chiarezza, non considerazione dei diritti)
Divulgazione o riuso per finalità diverse dei dati personali senza la consapevolezza e/o il consenso degli interessati
Conservazione immotivamente prolungata dei dati personali






MODELLO ORGANIZZATIVO, RUOLI E RESPONSABILITA', ISTRUZIONI E SENSIBILIZZAZIONE
Assessment azioni formative, di analisi e di trasparenza in essere
RISK ASSESSMENT MAP
Ri
STIMA EFFICACIA MISURE ORGANIZZATIVE E TECNICHE
STIMA EFFICACIA GOVERNANCE PER LA PROTEZIONE DATI PERSONALI E SICUREZZA INFORMAZIONI
Rr
Misure in essere per la sicurezza dei trattamenti
Tecnico-informatiche, organizzative
CONTRASTO DELLE MINACCE AMBIENTALI, EVENTI ACCIDENTALI, AZIONI DELIBERATE
Controlli da diverse famiglie di framework
GDPR - ISDP10003 –
ISO/IEC 27001 - ISO/IEC27701
AgID – NiST – Cybersecurity Nazionale

GDPR RISK ASSESSMENT TOOL

CRITERI UTILIZZATI NELLO STRUMENTO

NATURA DEL TRATTAMENTO Natura obbligatoria o facoltativa, scala del trattamento, operazioni , tipologie di dati personali trattati, effetti complessivi del trattamento

CONTESTO DEL TRATTAMENTO Analisi del contesto di riferimento, considerando i fattori interni ed esterni all'Organizzazione

AMBITO DI APPLICAZIONE Ambito specifico e modalità applicative con le quali avvengono i processi, attori dei processi, mezzi del trattamento

FINALITA' DEL TRATTAMENTO Finalità specifiche e legittime, per comprendere gli obiettivi del trattamento e, analizzando il flusso, individuare l'origine dei rischi

CRITERI DI CALCOLO:

PROBABILITA'

Stima della frequenza o possibilità di accadimento di un evento incerto che può deviare un processo dall'obiettivo di tutela delle persone

LIVELLO DI PROBABILITA'	DESCRIZIONE	SCORE
BASSO	Evento/Minaccia **poco probabile**/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore	1
MEDIO	Evento/Minaccia **possibile**; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore	2
ALTO	Evento/Minaccia **probabile**; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore	3

GRAVITA'

Stima del possibile impatto per le persone

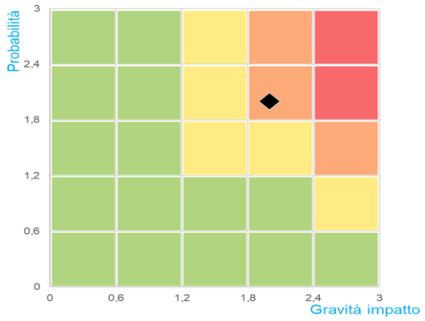
LIVELLO DI IMPATTO	CONSEGUENZE	DANNO FISICO	DANNO MATERIALE	DANNO IMMATERIALE	Score
BASSO	Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza troppi problemi	**Malessere** (es. mal di testa passeggero) o **ansia, preoccupazione** per mancanza di cura per una persona vulnerabile (es. minore)	**Fastidio - perdita di tempo** derivante dall'**impressione del riutilizzo dei propri dati** per pubblicità mirata o per ricezione di comunicazioni indesiderate (SPAM); perdita di tempo dovuto alla **necessità di ripetizione di azioni già svolte** (es. reinserimento dati per formalità, riconfigurazione, etc.)	Sensazione di **perdita di controllo dei propri dati** e del rispetto per la libertà di navigazione; **disagio per persone più vulnerabili** (es. lievi fastidi per minori o persone con necessità di tutori)	1
MEDIO	Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi	**Stress o disturbo minore psicologico o fisico** (es. malattia lieve a seguito del mancato rispetto di controindicazioni)	Eccessiva **difficoltà di accesso, o mancato accesso, a servizi pubblici o commerciali** (non vitali ma necessari); **danno materiale non ingente** derivante da un aspetto di vita privata che necessita riservatezza ; **perdita di opportunità di comfort** (es. cancellazioni di vacanze, cancellazione di account online, blocco account di servizi online, etc.); a**umenti di costi o conseguenze economiche non previste** (es. sanzioni, multe, interessi di mora, perdite di agevolazioni, etc.); Elaborazione di dati incorretti che provocano ad esempio **malfunzionamenti negli account bancari o di servizi previdenziali**; **pubblicità mirata online su aspetti confidenziali che si vogliono tenere nascosti** (es. gravidanza, trattamenti relativi a dipendenze, etc.); **profilazione inaccurata o inappropriata**	**Diffamazione, discredito, danni reputazionali** derivanti da comunicazioni mail indesiderate; **intimidazione sui social network**; **senso di violazione della privacy** senza danni irreparabili, **mancanza di riconoscimenti**, **problemi di relazioni** con gli altri, **discriminazione** sui social network, **danno di immagine**, etc.; **discriminazione in ambienti professionali o scolastici**, **opportunità perse** di avanzamento carriera	2
ALTO	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	**Disturbi fisici che provocano danni a lungo termine** (es. aggravamento dello stato di salute a seguito di mancato rispetto di controindicazioni, o cure non appropriate); **alterazione dell'integrità fisica** (es. incidenti o aggressioni); **grave disturbo psicologico** (depressione, fobie, fragilità dopo citazioni in giudizio, dopo estorsioni)	**Perdite economiche rilevanti** , divieto di tenuta o blocco di conti bancari, etc., difficoltà di **accesso a servizi pubblici importanti**, perdite di **opportunità / agevolazioni uniche** e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), **appropriazioni indebite** non compensate, **difficoltà economiche non temporanee** (es. necessità di prendere un prestito), divieto di **spostamenti all'estero, perdita di Clienti, dell'abitazione o del posto di lavoro**, esposizioni a **ricatti**, **perdite monetarie** a seguito di frodi o phishing, **danni alle proprietà** o perdite monetarie non indennizzate	Senso di **violazione della privacy** con danno irreparabile, **Separazione o divorzio**, **Cyber-bullismo**, discriminazione, **molestie psicologiche o sessuali**	3
CRITICO	Gli interessati possono avere conseguenze gravi, o addirittura irreversibili, che potrebbero non superare	**Rapimento**, **sequestro di persona**, disturbo psicologico **a lungo termine o permanente**, alterazione **permanente dell'integrità fisica**, **decesso**	**Impossibilità di lavorare** o **incapacità di ricollocazione**, impossibilità di citare in giudizio, **sanzioni penali**, cambio di stato amministrativo e/o **perdita dell'autonomia legale** (necessità di supervisione terza), smarrimento di **elementi di prova nell'ambito di un contenzioso**, rischio finanziario di **indebitamento ingente**, perdita di **accesso a infrastrutture vitali** (acqua, elettricità, ecc)	Allontanamento o **perdita di legami familiari**, perdita della **capacità di agire**	4

La formula utilizzata per il calcolo del rischio inerente è F(PxG) dove il Fattore di contesto F è calcolato come media tra i valori di incidenza dei fattori interni ed esterni.

Nel posizionamento del livello di rischio nei grafici (di Rischio inerente e Rischio Residuo), il valore della gravità dell'Impatto viene normalizzato sulla scala da 0 a 3; a tal fine, i valori di impatto indicati (1,2,3,4) vengono moltiplicati per 3 e divisi per 4.

La probabilità media di occorrenza delle minacce viene calcolata in base all'incidenza delle stesse sulla Conformità del trattamento, sulla Riservatezza, Integrità e Disponibilità dei dati

CRITERI DI RAPPRESENTAZIONE DEL LIVELLO DI RISCHIO



Stima	
Valori	**Valutazione**
	Critico
	Alto
	Medio
	Basso
◆	Posizionamento livello di rischio

ADEGUATEZZA MISURE ORGANIZZATIVE E TECNICHE

Stima	
Valori	**Valutazione**
Assenti o non attuate	Sebbene applicabili, le misure non sono implementate per contrastare le minacce specifiche
Presenti, ma inadeguate	Le misure sono state implementate in modo parziale o incompleto, e sono scarsamente efficaci
Presenti, migliorabili	Le misure poste in essere possono mitigare adeguatamente gli scenari di rischio, ma il monitoraggio o le verifiche non sono pienamente realizzati
Ben applicate	Le misure sono pienamente efficaci e costantemente verificate

ADEGUATEZZA MISURE DI GOVERNANCE

Stima	
Valori	**Valutazione**
Inadeguate	• La struttura organizzativa non è formalizzata e le responsabilità non sono formalmente definite e assegnate al personale; • assenza di procedure; • non vengono svolte attività di controllo; • il personale non possiede le competenze e il know-how necessari per svolgere le attività assegnate; • non viene svolta un'attività di monitoraggio del processo.
Deboli	La struttura organizzativa non è formalizzata e le responsabilità non sono adeguatamente assegnate al personale; • il processo è governato da procedure insufficienti e obsolete; • le attività di controllo sono carenti e non formalizzate; • mancanza di formazione del personale; • esiste una debole attività di monitoraggio del processo.
Adeguate	• la struttura organizzativa e le responsabilità assegnate al personale sono adeguatamente formalizzate; • il processo è disciplinato da procedure applicabili ma non ancora del tutto formalizzato; • le attività di controllo sono svolte ma non completamente documentate; • il personale sta rafforzando il proprio know-how ma richiede una formazione specifica; • esiste un'adeguata attività di monitoraggio del processo.
Verificate e ben applicate	• Esiste una struttura organizzativa formalizzata e ben progettata; • il processo è governato da politiche e procedure organizzative; • le attività di controllo e gli audit sono completamente documentati; • il personale possiede le competenze e il know-how necessari per svolgere le attività assegnate e la formazione specifica viene svolta e aggiornata; • esiste una forte attività di monitoraggio del processo.

GDPR RISK ASSESSMENT TOOL

METRICHE UTILIZZATE

NATURA DEL TRATTAMENTO

Circostanze delle operazioni

Natura obbligatoria = 1; Natura facoltativa = 1,5
Numerosità, quantità, identificabilità - Bassa = 0,5; Media = 1; Significativa = 1,5; Alta = 2

Potenziale impatto se la somma > 3; potenziale impatto significativo se la somma > 4,5; potenziale impatto elevato se la somma > 5,5

Potenziale conseguenza diretta/indiretta

Valori Si = 1; No = 0

Potenziale impatto se almeno 1 circostanza; potenziale impatto significativo se 2 circostanze; potenziale impatto elevato se > 2

Tipologie di operazioni

Valori Si = 1; No = 0

Potenziale impatto se almeno 1 circostanza; potenziale impatto significativo se 2 circostanze; potenziale impatto elevato se > 2

CONTESTO DEL TRATTAMENTO

Fattori di contesto

Valori: Poco significativa = 1; Mediamente significativa = 1,1; Molto significativa = 1,25

Media fra i valori e confronto fattori interni - fattori esterni => Fattore di contesto - moltiplicatore per la probabilità inerente
Se i fattori esterni sono maggiori di quelli interni, nella valutazione preliminare di rischiosità il fattore di contesto viene moltiplicato del 10% (*1,1)

AMBITO DI APPLICAZIONE

Assets

Valori: Nulla=0; Poco significativa = 1; Mediamente significativa = 1,1; Molto significativa = 1,25

Valorizzazione dell'incidenza sui parametri Conformità del trattamento, sulla Riservatezza, Integrità e Disponibilità dei dati
Assegnazione macrocategorizzazione in Persone/processi/Dati - Sistemi - Tecnoogie

RISCHIO ACCETTABILE

Valori MEDIO o BASSO da giustificare; impostare tenendo in considerazione le risultanze dell'analisi di NATURA; CONTESTO, AMBITO APPLICAZIONE

Nel foglio viene proposta una valutazione preliminare di rischiosità ottenuta nel seguente modo:
Un potenziale impatto viene fuori dal valore max riscontrato nella NATURA del trattamento;
Il Fattore di contesto (eventualmente aumentato del 10% in base ai fattori esterni prevalenti su quelli interni) viene sommato con il valore 1 o 2
a seconda che l'incidenza media degli Assets (Persone e processi, Reti e sistemi, Tecnologie) sia minore di 1,1 (il valore medio assoluto di incidenza);
Moltiplicando questo valore (una potenziale "probabilità") per l'impatto, sia un valore da 1 a 9; dove rischio basso è da 1 a 3, medio da 4 a 6, elevato da 7 a 9

PROBABILITA' MINACCE

Conteggio minacce applicabili, medie per categoria, max probabilità per Conformità, riservatezza, disponibilità, Integrità

LIVELLO DI RISCHIO INERENTE

Per i diversi rischi: il valore impatto (1,2,3,4) viene normalizzato per essere rappresentato sulla matrice 3X3;
Le probabilità (per parametri C,R,I,D - conformità - riservatezza - disponibilità integrità) vengono moltiplicate per il fattore di contesto
Si ottengono dunque valori di impatto inerente e probabilità inerente dei diversi rischi, che vengono posizionati nella matrice e moltiplicati per il livello nel grafico a barre

MISURE IN ESSERE

Grado di applicazione:

Assente o non attuata	-1
Presente ma inadeguata	1,25
Presente, migliorabile	2
Ben applicata	4

Ponderazione con Importanza della MISURA (Peso)

Medio-bassa	0,5
Significativa	0,75
Alta	1

MISURE GOVERNANCE

Grado di applicazione:

Inadeguata	1
Parzialmente adeguata	2
Adeguata	3
Verificata e ben applicata	4

Ponderazione con Importanza della MISURA (Peso)

Medio-bassa	0,5
Significativa	0,75
Alta	1

EFFICACIA

Efficacia mitigazione:
Inadeguata < 10%
Debole fra 10% e 25%
Adeguata fra 25% e 50%
Forte > 50%
Se l'efficacia è ad esempio del 60% - la vulnerabilità dei controlli è del 40% - ossia il livello di rischio viene ridotto del 40%. Per vulnerabilità massima (100%) il rischio rimane invariato.

RISCHIO RESIDUO

I valori di impatto inerente e probabilità inerenti vengono moltiplicati per il valore di vulnerabilità media dei controlli, ottenuta con media fra l'efficacia delle misure specifiche e l'efficacia delle misure di governance

GDPR RISK ASSESSMENT TOOL

FINALITA' E DESCRIZIONE DEL TRATTAMENTO

Obiettivo: Descrivere il trattamento, l'origine dei possibili rischi e se possibile il flusso, allegando un flowchart, uno schema, o utilizzando il modello di flowchart proposto

Descrizione dell'attività di trattamento	Studio clinico osservazionale "A REAl-life study on short-term Dual Antiplatelet treatment in Patients with ischemic stroke or Transient ischemic attack (READAPT)"
Finalità determinate, esplicite e legittime	Finalità di ricerca scientifica: Perseguimento di interesse pubblico rilevante da parte dell'Università degli studi dell'Aquila in qualità di soggetto istituzionale promotore
Origine dei rischi	L'origine dei rischi non è da ricercarsi tanto nella complessità di processi o tecnologie che afferiscono alle operazioni di trattamento, quanto alla natura particolare dei dati trattati relativi allo stato di salute, che possono avere effetti sulle persone in quanto si tratta di uno studio clinico

FLUSSO DEL TRATTAMENTO

input	OPERAZIONE TRATTAMENTO	output	INTERESSATI	TITOLARE	RESPONSABILE	ALTRO RESPONSABILE	DESTINATARI
	Idonea base giuridica per il trattamento			NO			
	Annullamento operazione		END		CRO		
Mappatura attività di trattamento	**Informazione agli interessati**	Informativa	Pazienti dei CRO	UNIVAQ			
Attività di cura	**Raccolta**	*Raccolta parametri stato di salute dei pazienti che prestano il consenso per la finalità di ricerca*	Pazienti dei CRO	CRO			
Parametri dello stato di salute	**Registrazione**	*Inserimento nel Sistema informativo REDCAP dell'Ateneo*		UNIVAQ	CRO		
Form web dei questionari	**Organizzazione**	*Database strutturato dello Studio osservazionale*		UNIVAQ			
Database	**Strutturazione**	*Campi parametro per le elaborazioni statische aggregate*		UNIVAQ			
Informative e consensi UNIVAQ conservati a cura del CRO per conto dell'Ateneo - Tabelle di pseudonimizzazione a cura del CRO - Dati nel database a cura dell'Ateneo	**Conservazione**	*Dati pseudonimizzati nel database; dati di reidentificazione ad uso esclusivo del CRO*		UNIVAQ	CRO		
Eventuale correzione parametri	**Adattamento o Modifica**	*Aggiornamento record possibile soltanto al personale di coordinamento dell'Ateneo*		UNIVAQ	CRO		
Dati nel database	**Estrazione**	*Statistiche aggregate*		UNIVAQ			
Dati nel database	**Consultazione**	*Report*		UNIVAQ			
Dati nel database	**Uso**	*Elaborazione e conteggi*		UNIVAQ			
Dati nel database	**Elaborazione automatizzata**	*?*		UNIVAQ			

NO	**[Elaborazione decisionale interamente automatizzata]**	*NO*					
Dati nel database	**Profilazione**	*Osservazioni parametri*		UNIVAQ			
Risultati Studio	**Comunicazione mediante trasmissione**	*Report e Pubblicazioni*		UNIVAQ			Comunità scientifica
Risultati Studio	**Diffusione**	*Report e Pubblicazioni*		UNIVAQ			Comunità scientifica
Risultati Studio	**Raffronto o interconnessione**	*Eventuali comparazioni*		UNIVAQ			
NO	**Limitazione**	*NO*					
Dopo 5 anni	**Cancellazione**	*Dati nel database ripuliti - Consensi distrutti*		UNIVAQ	CRO		
Dopo 5 anni	**Distruzione**	*Dati nel database ripuliti - Consensi distrutti*		UNIVAQ	CRO		
Dati nel database	**Copia protetta / Backup**	*Supporti Backup dell'Ateneo*		UNIVAQ			
Supporti Backup dell'Ateneo	**Ripristino**	*Recupero dati in caso di necessità*		UNIVAQ			

GDPR RISK ASSESSMENT TOOL

ANALISI DELLA NATURA DEL TRATTAMENTO

Obiettivo: Analizzando la "natura" in termini di caratteristiche generali, possibili effetti complessivi (Cons. 75) e Natura dei dati trattati e tipologie delle operazioni (Cons. 75), si ottengono degli "alert" che forniscono indicazioni su quali possibili impatti vanno determinati per il trattamento in esame

NATURA DEL TRATTAMENTO Natura obbligatoria o facoltativa, scala del trattamento, operazioni , effetti e tipologie di dati personali trattati

Principali caratteristiche:

Circostanze delle operazioni	Valore	NOTE
Natura obbligatoria (norma o regolamento a supporto) o iniziativa volontaria	Volontaria	Progetto di ricerca no profit su iniziativa del DISCAB dell'UNIVAQ
Numerosità degli interessati (scala del trattamento)	Media	Lo studio ha l'obiettivo di coinvolgere circa 106 centri e 350 pazienti
Quantità delle informazioni trattate	Significativa	Parametri clinici e abitudini correlate allo stato di salute
Identificabilità degli interessati	Bassa	Pseudonimizzazione - solo le Aziende sanitarie hanno la possibilità di reidentificare il paziente

POTENZIALE IMPATTO

Specificare la presenza di possibili effetti complessivi del trattamento (Cons. 75 GDPR)

Potenziale conseguenza diretta o indiretta	Sì/No	NOTE
Discriminazione	No	
Furto o usurpazione di identità	No	
Perdite finanziarie	No	
Pregiudizio alla reputazione	No	
Perdita di riservatezza dei dati personali protetti da segreto professionale	No	
Decifratura non autorizzata della pseudonimizzazione	Sì	una decifratura non autorizzata consentirebbe di reidentificare il paziente
Danno economico o sociale significativo	No	
Privazione di diritti e libertà	Sì	Il diritto alla riservatezza dei pazienti potrebbe essere violato
Impedimento dell'esercizio del controllo sui dati personali	No	

ATTENZIONE - POTENZIALE IMPATTO SIGNIFICATIVO PER GLI INTERESSATI

Indicare la presenza di tipologie di dati personali / operazioni (Cons. 75 GDPR):

Tipologia di operazioni	Sì/No	NOTE
Trattamento di dati personali che rivelano l'origine razziale o etnica	No	
Trattamento di opinioni politiche, convinzioni religiose o filosofiche	No	
Trattamento di dati che rivelano l'appartenenza sindacale	No	
Trattamento di dati genetici, biometrici o relativi alla salute	Sì	Lo Studio osservazionale riguarda dati clinici
Trattamento di dati relativi alla vita sessuale	No	
Trattamento di dati relativi a condanne penali e a reati o alle relative misure di sicurezza	No	

Valutazione di aspetti personali riguardanti il rendimento professionale	No	
Valutazione di aspetti personali riguardanti la situazione economica	No	
Valutazione di aspetti personali riguardanti la salute	Sì	**Lo Studio osservazionale riguarda dati clinici e abitudini correlate allo stato di salute**
Valutazione di aspetti personali riguardanti le preferenze o gli interessi personali	No	
Valutazione di aspetti personali riguardanti l'affidabilità o il comportamento	No	
Valutazione di aspetti personali riguardanti l'ubicazione o gli spostamenti per creare o utilizzare profili personali	No	
Trattamento di dati personali di soggetti vulnerabili, in particolare minori	No	
Trattamento di una notevole quantità di dati personali e un vasto numero di interessati	No	

ATTENZIONE - POTENZIALE IMPATTO SIGNIFICATIVO PER GLI INTERESSATI

GDPR RISK ASSESSMENT TOOL

ANALISI DEL CONTESTO

Obiettivo: Analizzare i fattori di contesto interni ed esterni per determinare l'incidenza nel trattamento, e considerarli nell'accettabilità del rischio e nella analisi

CONTESTO NEL QUALE VA CONSIDERATA L'ATTIVITA' Considerazioni circa i fattori interni ed esterni all'Organizzazione

Specificare il livello di incidenza dei fattori esterni e interni rispetto ai trattamenti di dati personali

Fattori di contesto **ESTERNI**	Incidenza	Motivazione / Note
Aspetti geopolitici	POCO SIGNIFICATIVA	non influente
Contesto sociale	POCO SIGNIFICATIVA	contesto sanitario - non correlato al contesto sociale
Attenzione mediatica / Appetibilità del Settore / Mercato di riferimento	MOLTO SIGNIFICATIVA	dati particolarmente appetibili
Dipendenza dalla reputazione - Aspettative delle parti interessate (Utenti / Clienti / Associati, etc.)	POCO SIGNIFICATIVA	non particolarmente influente
Dipendenza da Fornitori	POCO SIGNIFICATIVA	non particolarmente influente
Correlazione delle attività all'evoluzione tecnologica	POCO SIGNIFICATIVA	non particolarmente influente
Fattori ambientali nel territorio di riferimento, eventi naturali	MEDIAMENTE SIGNIFICATIVA	I server di Ateneo sono in una regione in Zona 1
Aspetti regolatori	MEDIAMENTE SIGNIFICATIVA	Norme e vincoli del Comitato etico mediamente influenti
Potenziali atti illeciti dall'esterno	MEDIAMENTE SIGNIFICATIVA	Tendenze ad attacchi cyber nel periodo 2020 - 2021 in aumento nelle aziende sanitarie ma i dati sono in Ateneo

Fattori di contesto **INTERNI**	Incidenza	Motivazione / Note
Strategie dell'Organizzazione	MEDIAMENTE SIGNIFICATIVA	Attività istituzionale di ricerca - nella norma
Complessità dell'Organizzazione	MOLTO SIGNIFICATIVA	Studio con soggetto Promotore e numerosi partecipanti
Processi (numerosità e complessità)	POCO SIGNIFICATIVA	Processo particolarmente semplice
Personale (numerosità e varietà di mansioni)	POCO SIGNIFICATIVA	Partecipano solo sperimentatori
Infrastrutture (numerosità e complessità)	MEDIAMENTE SIGNIFICATIVA	Server di Ateneo con 1 istanza software ad hoc per la sicurezza dei database e files -
Sistemi informativi	MEDIAMENTE SIGNIFICATIVA	incidenza sistemi nella norma
Attività pubblicistiche, Reputazione	MEDIAMENTE SIGNIFICATIVA	nella norma
Compliance	MEDIAMENTE SIGNIFICATIVA	Parere Comitato Etico e Comitati Etici CRO - norme protezione dati personali
Potenziali disordini e agitazioni interne	POCO SIGNIFICATIVA	poco rilevante
Situazione finanziaria	MEDIAMENTE SIGNIFICATIVA	Studio no profit - può incidere nell'attenzione al progetto
Resilienza al cambiamento	MEDIAMENTE SIGNIFICATIVA	nella norma, Atenei e CRO sono adaptive alle metodologie di ricerca
Continuità operativa	POCO SIGNIFICATIVA	Entità del numero dei parametri bassa

FATTORI INTERNI PIU' RILEVANTI DI QUELLI ESTERNI

FATTORI DI CONTESTO MEDIAMENTE SIGNIFICATIVI

GDPR RISK ASSESSMENT TOOL

ANALISI DELL'AMBITO DI APPLICAZIONE

Obiettivo:	Comprendere come viene effettuato il trattamento, individuando gli asset coinvolti (persone e processi, strumenti, sistemi, tecnologie) e attribuire l'incidenza di ciascuna categoria per l'applicabilità delle possibili minacce che possono incombere sulle operazioni di trattamento

AMBITO DI APPLICAZIONE DEL TRATTAMENTO: Modalità con le quali avvengono i processi, attori dei processi, mezzi del trattamento

Descrizione dell'ambito relativo al trattamento	Il processo prevede l'inserimento dati pseudonimizzati da parte dei CRO nel sistema REDCAP dell'Ateneo e le successive elaborazioni - aggragazioni da parte del Coordinamento di progetto del DISCAB (Dipartimento di Scienze Cliniche Applicate e Biotecnologiche) dell'Università degli Studi dell'Aquila.

Specificare il livello di incidenza degli ASSETS nei processi di trattamento di dati personali

ASSETS	Incidenza	Motivazione / Note
Risorse umane (persone impegnate nel trattamento)	MEDIAMENTE SIGNIFICATIVA	ci sono diversi autorizzati coinvolti nelle attività di trattamento (gli sperimentatori dei CRO)
Dati e informazioni in archivi cartacei	POCO SIGNIFICATIVA	il trattamento avviene prevalentemente con modaità elettroniche - soltanto i consensi al trattamento sono in forma cartacea
Dati e informazioni in formato digitale	MOLTO SIGNIFICATIVA	I dati sono organizzati e strutturati in un database
Processi e Unità organizzative	POCO SIGNIFICATIVA	Processo di raccolta e inserimento dati relativamente semplice
Attività in capo a soggetti esterni (Fornitori e processors, Providers, destinatari, etc.)	NULLA	In relazione allo Studio di ricerca, UNIVAQ e CRO sono autonomi titolari e non ci sono responsabili
Sedi e Uffici, locali fisici del Titolare e dei Responsabili	MEDIAMENTE SIGNIFICATIVA	nella norma - i CRO devono cmq conservare schede e consensi in modo sicuro
Data Center - Centri elaborazioni dati del Titolare e dei Responsabili	MOLTO SIGNIFICATIVA	Il Server di Ateneo con il software REDCAP è particolarmente importante pe ril progetto
Servers	MOLTO SIGNIFICATIVA	Il Server di Ateneo con il software REDCAP è particolarmente importante pe ril progetto
Software e applicazioni, APP	MOLTO SIGNIFICATIVA	L'Applicazione REDCAP è rilevante per la gestione dello Studio
Servizi online (Web, Cloud, Cloud storage, SaaS, etc)	POCO SIGNIFICATIVA	L'applicativo è fruibile via web ma non ci sono altri servizi esterni necessari
Database e DBMS	MEDIAMENTE SIGNIFICATIVA	Dati nel DB - importante ma nella norma
Postazioni utente, Computer fissi	POCO SIGNIFICATIVA	postazioni utili solo all'inserimento dati pseudonimizzati
Dispositivi mobili (Laptop, Tablet, Smartphones, etc.)	POCO SIGNIFICATIVA	postazioni utili solo all'inserimento dati pseudonimizzati
Posta elettronica e messaggistica	MEDIAMENTE SIGNIFICATIVA	usata solo per comunicazioni di servizio e link di accesso
Dispositivi portatili e removibili [USB pendrive, memorie flash, hard disk esterni]	POCO SIGNIFICATIVA	non necessari
Rete intranet [LAN] e apparati [switch – router -Firewall]	POCO SIGNIFICATIVA	poco rilevante
Connettività Internet - Linee di comunicazione - VPN	POCO SIGNIFICATIVA	poco rilevante
Dispositivi e strumentazione medico-scientifica	MEDIAMENTE SIGNIFICATIVA	necessari per l'acquisizione dei parametri
Sistemi e supporti di registrazione audiovisiva	NULLA	-
Sistemi di elaborazione dati biometrici, riconoscimento facciale, etc.	NULLA	-
Dispositivi IoT, wearable devices, assistenti vocali e domotica	NULLA	-
Videosorveglianza, strumenti "intelligenti" di monitoraggio connessi (es. geolocalizzazione, scatole nere, droni, etc.)	NULLA	-
Algoritmi di Intelligenza Artificiale e Machine Learning	NULLA	-
Blockchain Technology	NULLA	-

GDPR RISK ASSESSMENT TOOL

LIVELLO DI RISCHIO ACCETTABILE

In base alle considerazioni registrate e ai potenziali risultati:

DESCRIZIONE E FINALITA' DEL TRATTAMENTO

DESCRIZIONE	Studio clinico osservazionale "A REAl-life study on short-term Dual Antiplatelet treatment in Patients with ischemic stroke or Transient ischemic attack (READAPT)"
FINALITA'	Finalità di ricerca scientifica: Perseguimento di interesse pubblico rilevante da parte dell'Università degli studi dell'Aquila in qualità di soggetto istituzionale promotore

NATURA DEL TRATTAMENTO

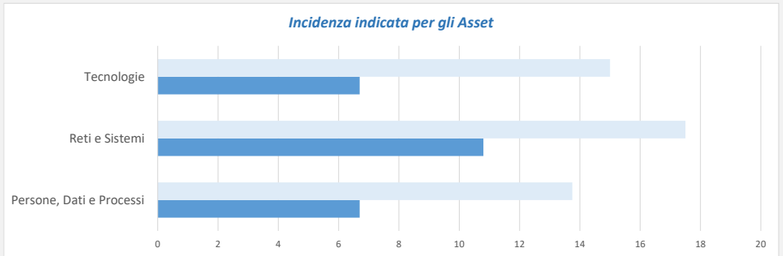
Obbligatorietà, Scala, Numerosità, Identificabilità:	POTENZIALE IMPATTO
Possibili effetti complessivi del trattamento	ATTENZIONE - POTENZIALE IMPATTO SIGNIFICATIVO PER GLI INTERESSATI
Tipologie di dati / operazioni:	ATTENZIONE - POTENZIALE IMPATTO SIGNIFICATIVO PER GLI INTERESSATI

CONTESTO DEL TRATTAMENTO

Bilanciamento Fattori interni - Fattori esterni:	FATTORI INTERNI PIU' RILEVANTI DI QUELLI ESTERNI
Rilevanza Fattori interni ed esterni	FATTORI DI CONTESTO MEDIAMENTE SIGNIFICATIVI

AMBITO DI APPLICAZIONE DEL TRATTAMENTO

Ambito relativo al trattamento	Il processo prevede l'inserimento dati pseudonimizzati da parte dei CRO nel sistema REDCAP dell'Ateneo e le successive elaborazioni - aggragazioni da parte del Coordinamento di progetto del DISCAB (Dipartimento di Scienze Cliniche Applicate e



Fattore di Contesto 1,07 POTENZIALE RISCHIO MEDIO

In considerazione della natura, del contesto, dell'ambito di applicazione e delle finalità perseguite nei trattamenti di dati personali, come da valutazione complessiva, si stabilisce in questa sezione il livello di rischio accettabile:.

Livello rischio accettabile: MEDIO

Motivazione:	L'Ateneo ritiene importante lo Studio clinico in oggetto e si è comunque disposti ad accettarne la fattibilità a fronte di un livello di rischio medio per le persone

GDPR RISK ASSESSMENT TOOL

DETERMINAZIONE DEI LIVELLI DI GRAVITA' DI IMPATTO (conseguenze per gli interessati)

Rispondere alla domanda: quali sono le possibili conseguenze per gli interessati in caso di:

SCENARIO DI RISCHIO	PROPRIETA' A RISCHIO	IMPATTO	Motivazione / Note	CONSEGUENZE	DANNO FISICO	DANNO MATERIALE	DANNO IMMATERIALE	Score
PERDITA DI DATI	*Disponibilità, Riservatezza*	MEDIO	**I parametri dei pazienti possono essere recuperati dagli sperimentatori**	Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi	Stress o disturbo minore psicologico o fisico (es. malattia lieve a seguito del mancato rispetto di controindicazioni)	Eccessiva difficoltà di accesso, o mancato accesso, a servizi pubblici o commerciali (non vitali ma necessari); danno materiale non ingente derivante da un aspetto di vita privata che necessita riservatezza ; perdita di opportunità di comfort (es. cancellazioni di vacanze, cancellazione di account online, blocco account di servizi online, etc.); aumenti di costi o conseguenze economiche non previste (es. sanzioni, multe, interessi di mora, perdite di agevolazioni, etc.); Elaborazione di dati incorretti che provocano ad esempio malfunzionamenti negli account bancari o di servizi previdenziali; pubblicità mirata online su aspetti confidenziali che si vogliono tenere nascosti (es. gravidanza, trattamenti relativi a dipendenze, etc.); profilazione inaccurata o inappropriata	Diffamazione, discredito, danni reputazionali derivanti da comunicazioni mail indesiderate; intimidazione sui social network; senso di violazione della privacy senza danni irreparabili, mancanza di riconoscimenti, problemi di relazioni con gli altri, discriminazione sui social network, danno di immagine, etc.; discriminazione in ambienti professionali o scolastici, opportunità perse di avanzamento carriera	2
DISTRUZIONE NON AUTORIZZATA DI DATI	*Disponibilità, Integrità*	ALTO	**Lo Studio osservazionale è utile per certe patologie e la distruzione dei dati comprometterebbe la possibile utilità per le persone fisiche beneficiarie (in questo caso nullo è l'impatto per i pazienti)**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	Disturbi fisici che provocano danni a lungo termine (es. aggravamento dello stato di salute a seguito di mancato rispetto di controindicazioni, o cure non appropriate); alterazione dell'integrità fisica (es. incidenti o aggressioni); grave disturbo psicologico (depressione, fobie, fragilità dopo citazioni in giudizio, dopo estorsioni)	Perdite economiche rilevanti , divieto di tenuta o blocco di conti bancari, etc., difficoltà di accesso a servizi pubblici importanti, perdite di opportunità / agevolazioni uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), appropriazioni indebite non compensate, difficoltà economiche non temporanee (es. necessità di prendere un prestito), divieto di spostamenti all'estero, perdita di Clienti, dell'abitazione o del posto di lavoro, esposizioni a ricatti, perdite monetarie a seguito di frodi o phishing, danni alle proprietà o perdite monetarie non indennizzate	Senso di violazione della privacy con danno irreparabile, Separazione o divorzio, Cyber-bullismo, discriminazione, molestie psicologiche o sessuali	3
MODIFICHE INDESIDERATE O NON AUTORIZZATE AI DATI	*Integrità*	ALTO	**Lo Studio osservazionale è utile per certe patologie e la distruzione dei dati comprometterebbe la possibile utilità per le persone fisiche beneficiarie (in questo caso nullo è l'impatto per i pazienti)**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	Disturbi fisici che provocano danni a lungo termine (es. aggravamento dello stato di salute a seguito di mancato rispetto di controindicazioni, o cure non appropriate); alterazione dell'integrità fisica (es. incidenti o aggressioni); grave disturbo psicologico (depressione, fobie, fragilità dopo citazioni in giudizio, dopo estorsioni)	Perdite economiche rilevanti , divieto di tenuta o blocco di conti bancari, etc., difficoltà di accesso a servizi pubblici importanti, perdite di opportunità / agevolazioni uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), appropriazioni indebite non compensate, difficoltà economiche non temporanee (es. necessità di prendere un prestito), divieto di spostamenti all'estero, perdita di Clienti, dell'abitazione o del posto di lavoro, esposizioni a ricatti, perdite monetarie a seguito di frodi o phishing, danni alle proprietà o perdite monetarie non indennizzate	Senso di violazione della privacy con danno irreparabile, Separazione o divorzio, Cyber-bullismo, discriminazione, molestie psicologiche o sessuali	3
DIVULGAZIONE NON AUTORIZZATA DI DATI PERSONALI	*Riservatezza*	ALTO	**La violazione di riservatezza circa le abitudini relative allo stato di salute o di parametri clinici e cure ricevute può avere effetti complessivi anche gravi per i pazienti e in generale per tutte le persone (studio clinico a livello nazionale)**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	Disturbi fisici che provocano danni a lungo termine (es. aggravamento dello stato di salute a seguito di mancato rispetto di controindicazioni, o cure non appropriate); alterazione dell'integrità fisica (es. incidenti o aggressioni); grave disturbo psicologico (depressione, fobie, fragilità dopo citazioni in giudizio, dopo estorsioni)	Perdite economiche rilevanti , divieto di tenuta o blocco di conti bancari, etc., difficoltà di accesso a servizi pubblici importanti, perdite di opportunità / agevolazioni uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), appropriazioni indebite non compensate, difficoltà economiche non temporanee (es. necessità di prendere un prestito), divieto di spostamenti all'estero, perdita di Clienti, dell'abitazione o del posto di lavoro, esposizioni a ricatti, perdite monetarie a seguito di frodi o phishing, danni alle proprietà o perdite monetarie non indennizzate	Senso di violazione della privacy con danno irreparabile, Separazione o divorzio, Cyber-bullismo, discriminazione, molestie psicologiche o sessuali	3
ACCESSO ILLEGITTIMO O NON AUTORIZZATO AI DATI	*Riservatezza, Integrità, Disponibilità*	ALTO	**La violazione di riservatezza circa i dati sullo stato di salute può avere effetti complessivi anche gravi per i pazienti; inoltre, l'eventuale compromissione dell'integrità dei dati dello Studio ha effetti su tutte le persone potenzialmente beneficiarie**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	Disturbi fisici che provocano danni a lungo termine (es. aggravamento dello stato di salute a seguito di mancato rispetto di controindicazioni, o cure non appropriate); alterazione dell'integrità fisica (es. incidenti o aggressioni); grave disturbo psicologico (depressione, fobie, fragilità dopo citazioni in giudizio, dopo estorsioni)	Perdite economiche rilevanti , divieto di tenuta o blocco di conti bancari, etc., difficoltà di accesso a servizi pubblici importanti, perdite di opportunità / agevolazioni uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), appropriazioni indebite non compensate, difficoltà economiche non temporanee (es. necessità di prendere un prestito), divieto di spostamenti all'estero, perdita di Clienti, dell'abitazione o del posto di lavoro, esposizioni a ricatti, perdite monetarie a seguito di frodi o phishing, danni alle proprietà o perdite monetarie non indennizzate	Senso di violazione della privacy con danno irreparabile, Separazione o divorzio, Cyber-bullismo, discriminazione, molestie psicologiche o sessuali	3
ECCESSIVA RACCOLTA DI DATI PERSONALI	*Adeguatezza, pertinenza, limitata finalità*	MEDIO	**I questionari clinici non possono esulare dalle finalità di ricerca clinica specifica anche per motivi etici**	Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi	Stress o disturbo minore psicologico o fisico (es. malattia lieve a seguito del mancato rispetto di controindicazioni)	Eccessiva difficoltà di accesso, o mancato accesso, a servizi pubblici o commerciali (non vitali ma necessari); danno materiale non ingente derivante da un aspetto di vita privata che necessita riservatezza ; perdita di opportunità di comfort (es. cancellazioni di vacanze, cancellazione di account online, blocco account di servizi online, etc.); aumenti di costi o conseguenze economiche non previste (es. sanzioni, multe, interessi di mora, perdite di agevolazioni, etc.); Elaborazione di dati incorretti che provocano ad esempio malfunzionamenti negli account bancari o di servizi previdenziali; pubblicità mirata online su aspetti confidenziali che si vogliono tenere nascosti (es. gravidanza, trattamenti relativi a dipendenze, etc.); profilazione inaccurata o inappropriata	Diffamazione, discredito, danni reputazionali derivanti da comunicazioni mail indesiderate; intimidazione sui social network; senso di violazione della privacy senza danni irreparabili, mancanza di riconoscimenti, problemi di relazioni con gli altri, discriminazione sui social network, danno di immagine, etc.; discriminazione in ambienti professionali o scolastici, opportunità perse di avanzamento carriera	2
COLLEGAMENTI O RAFFRONTI INAPPROPRIATI O NON AUTORIZZATI DI DATI PERSONALI	*Adeguatezza, pertinenza, limitata finalità*	ALTO	**raffronti non pertinenti possono condurre a supposizioni o azioni con conseguenze gravi per i pazienti**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	Disturbi fisici che provocano danni a lungo termine (es. aggravamento dello stato di salute a seguito di mancato rispetto di controindicazioni, o cure non appropriate); alterazione dell'integrità fisica (es. incidenti o aggressioni); grave disturbo psicologico (depressione, fobie, fragilità dopo citazioni in giudizio, dopo estorsioni)	Perdite economiche rilevanti , divieto di tenuta o blocco di conti bancari, etc., difficoltà di accesso a servizi pubblici importanti, perdite di opportunità / agevolazioni uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), appropriazioni indebite non compensate, difficoltà economiche non temporanee (es. necessità di prendere un prestito), divieto di spostamenti all'estero, perdita di Clienti, dell'abitazione o del posto di lavoro, esposizioni a ricatti, perdite monetarie a seguito di frodi o phishing, danni alle proprietà o perdite monetarie non indennizzate	Senso di violazione della privacy con danno irreparabile, Separazione o divorzio, Cyber-bullismo, discriminazione, molestie psicologiche o sessuali	3

PERDITA DI CONTROLLO DA PARTE DEGLI INTERESSATI (MANCANZA DI TRASPARENZA, CHIAREZZA, NON CONSIDERAZIONE DEI DIRITTI)	*Liceità, correttezza, trasparenza*	MEDIO	**le finalità di ricerca sono comunque nell'ambito dell'interesse pubblico rilevante e la perdita di controllo da parte degli interessati non ha comunque conseguenze gravi**	Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi	Stress o disturbo minore psicologico o fisico (es. malattia lieve a seguito del mancato rispetto di controindicazioni)	Eccessiva difficoltà di accesso, o mancato accesso, a servizi pubblici o commerciali (non vitali ma necessari); danno materiale non ingente derivante da un aspetto di vita privata che necessita riservatezza ; perdita di opportunità di comfort (es. cancellazioni di vacanze, cancellazione di account online, blocco account di servizi online, etc.); aumenti di costi o conseguenze economiche non previste (es. sanzioni, multe, interessi di mora, perdite di agevolazioni, etc.); Elaborazione di dati incorretti che provocano ad esempio malfunzionamenti negli account bancari o di servizi previdenziali; pubblicità mirata online su aspetti confidenziali che si vogliono tenere nascosti (es. gravidanza, trattamenti relativi a dipendenze, etc.); profilazione inaccurata o inappropriata	Diffamazione, discredito, danni reputazionali derivanti da comunicazioni mail indesiderate; intimidazione sui social network; senso di violazione della privacy senza danni irreparabili, mancanza di riconoscimenti, problemi di relazioni con gli altri, discriminazione sui social network, danno di immagine, etc.; discriminazione in ambienti professionali o scolastici, opportunità perse di avanzamento carriera	2
DIVULGAZIONE O RIUSO PER FINALITÀ DIVERSE DEI DATI PERSONALI SENZA LA CONSAPEVOLEZZA E/O IL CONSENSO DEGLI INTERESSATI	*Liceità, correttezza e trasparenza; Adeguatezza, pertinenza, limitata finalità*	MEDIO	**le finalità di ricerca sono comunque nell'ambito dell'interesse pubblico rilevante e l'utilizzo dei dati per ulteriore finalità senza la piena consapevolezza da parte degli interessati non avrebbe comunque conseguenze gravi**	Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi	Stress o disturbo minore psicologico o fisico (es. malattia lieve a seguito del mancato rispetto di controindicazioni)	Eccessiva difficoltà di accesso, o mancato accesso, a servizi pubblici o commerciali (non vitali ma necessari); danno materiale non ingente derivante da un aspetto di vita privata che necessita riservatezza ; perdita di opportunità di comfort (es. cancellazioni di vacanze, cancellazione di account online, blocco account di servizi online, etc.); aumenti di costi o conseguenze economiche non previste (es. sanzioni, multe, interessi di mora, perdite di agevolazioni, etc.); Elaborazione di dati incorretti che provocano ad esempio malfunzionamenti negli account bancari o di servizi previdenziali; pubblicità mirata online su aspetti confidenziali che si vogliono tenere nascosti (es. gravidanza, trattamenti relativi a dipendenze, etc.); profilazione inaccurata o inappropriata	Diffamazione, discredito, danni reputazionali derivanti da comunicazioni mail indesiderate; intimidazione sui social network; senso di violazione della privacy senza danni irreparabili, mancanza di riconoscimenti, problemi di relazioni con gli altri, discriminazione sui social network, danno di immagine, etc.; discriminazione in ambienti professionali o scolastici, opportunità perse di avanzamento carriera	2
CONSERVAZIONE IMMOTIVAMENTE PROLUNGATA DEI DATI PERSONALI	*Limitazione della conservazione*	MEDIO	**Una conservazione eccessiva dei dati potrebbe portare a supposizioni retrospettive non pertinenti, che comunque non hanno effetti particolarmente gravi per le persone**	Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi	Stress o disturbo minore psicologico o fisico (es. malattia lieve a seguito del mancato rispetto di controindicazioni)	Eccessiva difficoltà di accesso, o mancato accesso, a servizi pubblici o commerciali (non vitali ma necessari); danno materiale non ingente derivante da un aspetto di vita privata che necessita riservatezza ; perdita di opportunità di comfort (es. cancellazioni di vacanze, cancellazione di account online, blocco account di servizi online, etc.); aumenti di costi o conseguenze economiche non previste (es. sanzioni, multe, interessi di mora, perdite di agevolazioni, etc.); Elaborazione di dati incorretti che provocano ad esempio malfunzionamenti negli account bancari o di servizi previdenziali; pubblicità mirata online su aspetti confidenziali che si vogliono tenere nascosti (es. gravidanza, trattamenti relativi a dipendenze, etc.); profilazione inaccurata o inappropriata	Diffamazione, discredito, danni reputazionali derivanti da comunicazioni mail indesiderate; intimidazione sui social network; senso di violazione della privacy senza danni irreparabili, mancanza di riconoscimenti, problemi di relazioni con gli altri, discriminazione sui social network, danno di immagine, etc.; discriminazione in ambienti professionali o scolastici, opportunità perse di avanzamento carriera	2

GDPR RISK ASSESSMENT TOOL

DETERMINAZIONE DELLA PROBABILITA' DEL VERIFICARSI DI EVENTI MINACCIOSI

In questa sezione vengono impostate le probabilità di occorrenza delle potenziali minacce al trattamento, così categorizzate:

Minacce alla ***conformità*** del trattamento;
Eventi con ***danni fisici/materiali*** ;
Eventi ***naturali*** ;
Indisponibilità di servizi essenziali;
Compromissione di dati e informazioni per ***azioni deliberate*** ;
Problemi tecnici ;
Compromissione di dati o servizi per ***azioni involontarie***

TIPOLOGIA DI MINACCIA	CAUSA CHE PROVOCA L'EVENTO	Principi compromessi Parametri RID	Principali Target della minaccia	APPLICABILE?	Livello P (inerente)		CRITERI / RIFERIMENTI PER MOTIVARE IL VALORE
Minacce alla conformità del trattamento	**Scarsa cultura in materia di privacy e dei diritti degli interessati, inconsapevolezza o disinteresse nell'applicazione delle istruzioni e regolamenti per i trattamenti di dati personali**	liceità, correttezza, necessità, esattezza e trasparenza, minimizzazione, limitazione della conservazione	*Persone impegnate nel trattamento, Processi del trattamento, Fornitori*	Si	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	C'e la possibilità che sperimentatori di Centri non siano abbastanza consapevoli e formati sui temi della data protection
	Inadeguata conoscenza dei vincoli di protezione dati nei rapporti, regolamentazioni e contratti	necessità, minimizzazione, limitazione della conservazione	*Persone impegnate nel trattamento, Processi del trattamento, Fornitori e Destinatari*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Gli sperimentatori conoscono i vincoli correlati ai contratti di ricerca, ruolo dei comitati etici, del DPO, etc.
	Confusione nei ruoli rispetto ai trattamenti di dati personali, per elevata job rotation o frequenti modifiche organizzative, numerosità del personale e dei processi, etc.	liceità, correttezza e trasparenza	*Persone impegnate nel trattamento, Processi del trattamento, Fornitori e Destinatari*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Sperimentatori nell'ambito specifico conosciuti e identificati, c'eè scarsa possibilità di utilizzo di persone diverse
	Disattenzione o non adeguata considerazione delle necessità di fiducia e delle esigenze di controllo dei dati da parte degli interessati (scarsa conoscenza dei principi fondamentali)	liceità, correttezza e trasparenza, necessità, esattezza	*Persone impegnate nel trattamento, Processi del trattamento, applicazioni software e sistemi intelligenti*	Si	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	C'e la possibilità che sperimentatori non siano abbastanza consapevoli e formati sui temi della data protection
	Carenza di capacità comunicativa idonea alla preparazione di informazioni adeguate nei confronti degli interessati, non conoscenza degli attuali trend di Legal Design	necessità, minimizzazione, limitazione della conservazione	*Persone impegnate nel trattamento, Processi del trattamento, applicazioni software e sistemi intelligenti*	Si	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	C'e la possibilità che sperimentatori non siano abbastanza consapevoli e formati sui temi della data protection
	Utilizzo di prassi, tecniche o sistemi non progettati e/o impostati per la protezione dei dati personali	necessità, minimizzazione, limitazione della conservazione, esattezza	*Persone impegnate nel trattamento, Processi del trattamento, applicazioni software e sistemi intelligenti*	Si	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Possibile approccio non corretto al rischio
	Utilizzo di grandi quantità di dati personali e di molteplici fonti per incroci - raffronti - integrazioni - filtri e analisi	necessità, minimizzazione, limitazione della conservazione, esattezza	*Persone impegnate nel trattamento, Processi del trattamento, applicazioni software e sistemi intelligenti*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Rara possibilità nello Studio in questione
	Inconsapevolezza delle possibili conseguenze derivanti dalle elaborazioni elettroniche, superficialità e/o scarsa dimestichezza con l'uso delle tecnologie	liceità, correttezza e trasparenza, necessità, minimizzazione, limitazione della conservazione, esattezza	*Persone impegnate nel trattamento, Processi del trattamento, Fornitori, Applicazioni software e sistemi intelligenti*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Scolarizzazione adeguata e dimestichezza del personale ok

Eventi con danni fisici/materiali	**Incendio**	D	*Sedi titolare e responsabili, Data Centers, Uffici, Locali con postazioni e supporti di memorizzazione, Archivi Cartacei, Servers, Apparati di rete, Linee di comunicazione*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Evento possibile
	Allagamento	D	*Sedi titolare e responsabili, Data Centers, Uffici, Locali con postazioni e supporti di memorizzazione, Archivi Cartacei, Servers, Apparati di rete, Linee di comunicazione*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Storicamente mai successo
	Polvere, corrosione, deterioramento, congelamento.	D	*Data Centers, Uffici, Locali con postazioni e supporti di memorizzazione, Archivi Cartacei, Servers, Workstations, Devices portatili, Apparati di rete*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Ambienti salubri e clima nella norma
	Distruzione di documenti cartacei o strumentazione e/o supporti con dati da parte di malintenzionati (vandalica) o per errore (disattenzione)	D	*Persone impegnate nel trattamento, Archivi cartacei o assets tecnologici*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Atti di Guerra/Azioni Militari/Atti terroristici	D	*Sedi titolare e responsabili, Data Centers, Uffici, Locali con postazioni e supporti di memorizzazione, Archivi Cartacei, Servers, Apparati di rete, Linee di comunicazione*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
Eventi Naturali	**Fenomeni climatici (Uragani, Cicloni, Nevicate, Grandine)**	D	*Sedi titolare e responsabili, Data Centers, Uffici, Locali con postazioni e supporti di memorizzazione, Archivi Cartacei, Servers, Apparati di rete, Linee di comunicazione*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Terremoti, eruzioni vulcaniche	D	*Sedi titolare e responsabili, Data Centers, Uffici, Locali con postazioni e supporti di memorizzazione, Archivi Cartacei, Servers, Apparati di rete, Linee di comunicazione*	Sì	ALTO	*Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore*	Evento probabile in Abruzzo - Zona 1
	Fulmini e scariche atmosferiche	D	*Sedi titolare e responsabili, Data Centers, Uffici, Locali con postazioni e supporti di memorizzazione, Archivi Cartacei, Servers, Apparati di rete, Linee di comunicazione*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
Indisponibilità di Servizi essenziali	**Guasto aria condizionata o sistemi di raffreddamento nei locali C.e.d.**	D	*Data Centers, Servers*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Perdita di energia (o sbalzi di tensione)	D	*Sistemi di elaborazione Servers e Client, Dispositivi elettronici*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Malfunzionamento nei componenti di rete e/o Errori di trasmissione - errori di instradamento (misrouting)	ID	*Sistemi di rete e Linee di comunicazione del Titolare e dei Responsabili, Applicazioni e Sistemi interconnessi*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	bassa storicità
	Interruzione nei collegamenti internet, e della connettività di rete fra sedi e con i providers (inclusi danni alle linee di telecomunicazioni)	D	*Sistemi di rete e Linee di comunicazione del Titolare e dei Responsabili*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile

	Interruzione di servizi erogati da fornitori esterni inclusi ISP, CSP, Siti Disaster Recovery, supporto tecnico specialistico o attività esternalizzate a fornitori (ad esempio per fallimento, chiusura attività, incidenti informatici e non)	D	*Persone impegnate nel trattamento, Processi del trattamento, Sedi e Data Centers dei Responsabili, Servers e Linee di comunicazione, Ambienti online*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	bassa storicità
	Interruzione di servizi per indisponibilità di personale (scioperi, malattie, etc.)	D	*Persone impegnate nel trattamento, Processi del trattamento*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	bassa storicità
Compromissione di dati e informazioni per azioni deliberate	**Denial of Service per attacco deliberato di terzi**	D	*Strumenti e Sistemi utilizzati per il trattamento, tecnologiee processi*	Si	ALTO	*Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore*	Tendenze attuali riportate da rapporti Clusit e Studi di settore
	Denial of Service per azione intenzionale da parte di personale interno	D	*Strumenti e Sistemi utilizzati per il trattamento, tecnologiee processi*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Web application Cyber attacks	RID	*Sistemi, ambienti e dispositivi raggiungibili online*	Si	ALTO	*Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore*	Tendenze attuali riportate da rapporti Clusit e Studi di settore
	Intercettazione (sia umana, sbirciando o origliando, sia tecnologica inclusa analisi del traffico di rete, cablata o wireless)	R	*Persone impegnate nel trattamento, Apparati di rete, Postazioni Client e dispositivi, sistemi di messaggistica e posta elettronica*	Si	ALTO	*Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore*	Tendenze attuali riportate da rapporti Clusit e Studi di settore
	Furto di documenti o strumentazione, dispositivi e/o supporti di memorizzazione	RD	*Persone impegnate nel trattamento, documenti o strumenti e/o supporti di memorizzazione*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Infiltrazione nelle comunicazioni o lettura /copia non autorizzata di documenti cartacei o archivi informatici, password, dati, ricezione messaggi da origini non affidabili o attacchi da utenti interni o esterni (cyber attacks)	RID	*Persone impegnate nel trattamento, Apparati di rete, Postazioni Client e dispositivi, sistemi di messaggistica e posta elettronica*	Si	ALTO	*Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore*	Tendenze attuali riportate da rapporti Clusit e Studi di settore
	Furto o mascheramento di identità da parte di personale interno	RID	*Persone impegnate nel trattamento, Sistemi e Dispositivi*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Furto o mascheramento di identità da parte di esterni (es. fornitori)	RID	*Persone impegnate nel trattamento, Sistemi e Dispositivi*	No			Non ci sono fornitori esterni nel processo
	Azioni di "raggiro" a danno degli operatori mediante tecniche di Social Engineering: Phishing - Whaling - Pretexting, Tailgating, Doxing	RID	*Persone impegnate nel trattamento, Sistemi e Dispositivi che prevedono scambi di comunicazioni*	Si	ALTO	*Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore*	Tendenze attuali riportate da rapporti Clusit e Studi di settore
	Uso dei servizi e sistemi da parte di persone non autorizzate o elevamento di privilegi nei profili autorizzativi	RID	*Persone impegnate nel trattamento, Processi del trattamento*	Si	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità

	Modifica deliberata e non autorizzata di dati residenti su archivi informatici	RID	*Files e database utilizzati nel trattamento*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Accesso fisico non autorizzato ai locali o agli archivi fisici	RID	*Sedi titolare e responsabili, Data Centers, Uffici con postazioni e supporti di memorizzazione, Servers, Apparati di rete*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Uso non autorizzato o negligente della strumentazione, accessi a reti e sistemi non autorizzati	RID	*Persone impegnate nel trattamento, Processi del trattamento, Strumenti e dispositivi, Sistemi informativi e Reti*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Alterazione volontaria e non autorizzata di dati	I	*Files e database utilizzati nel trattamento, Sistemi Informativi, dispositivi*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Rivelazione di informazioni (da parte del personale o fornitori) es. trasmissione di dati o messaggi a destinatari errati, pubblicazione o diffusione di dati personali	R	*Persone impegnate nel trattamento, Postazioni e dispositivi Client, sistemi di messaggistica e posta elettronica*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
Problemi tecnici	**Fault o malfunzionamento degli strumenti e apparati IT**	ID	*Sistemi di elaborazione Servers / NAS/ Apparati di rete e Client (Postazioni, dispositivi mobili, supporti di memorizzazione)*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Malfunzionamenti hardware (disco pieno, alimentazione elettrica dei sistemi, componenti essenziali dei sistemi, degrado dei media)	RID	*Software gestionali (sistemi informativi online / accessibili agli utenti - nell'ambito del trattamento)*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Malfunzionamenti software applicativi	ID	*DBMS (Database management Systems)*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Malfunzionamenti nei database (dimensioni, configurazione, aggiornamenti, etc.)	RID	*Sistemi di elaborazione Servers e Client (Postazioni, dispositivi mobili, supporti di memorizzazione)*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Azione MALWARE: virus informatici, ransomware, codici malevoli	RID	*Software gestionali (sistemi informativi online / interni - utilizzati dalle persone impegnate nel trattamento)*	Sì	ALTO	*Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore*	Tendenze attuali riportate da rapporti Clusit e Studi di settore
	Malfunzionamento di apparati di rete	ID	*Amministratori di sistema*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Denial of Service per inadeguatezza del sistema (banda, obsolescenza sistemi, sovraccarico, etc.)	D	*Apparati Networking, Cabling, Antenne*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile

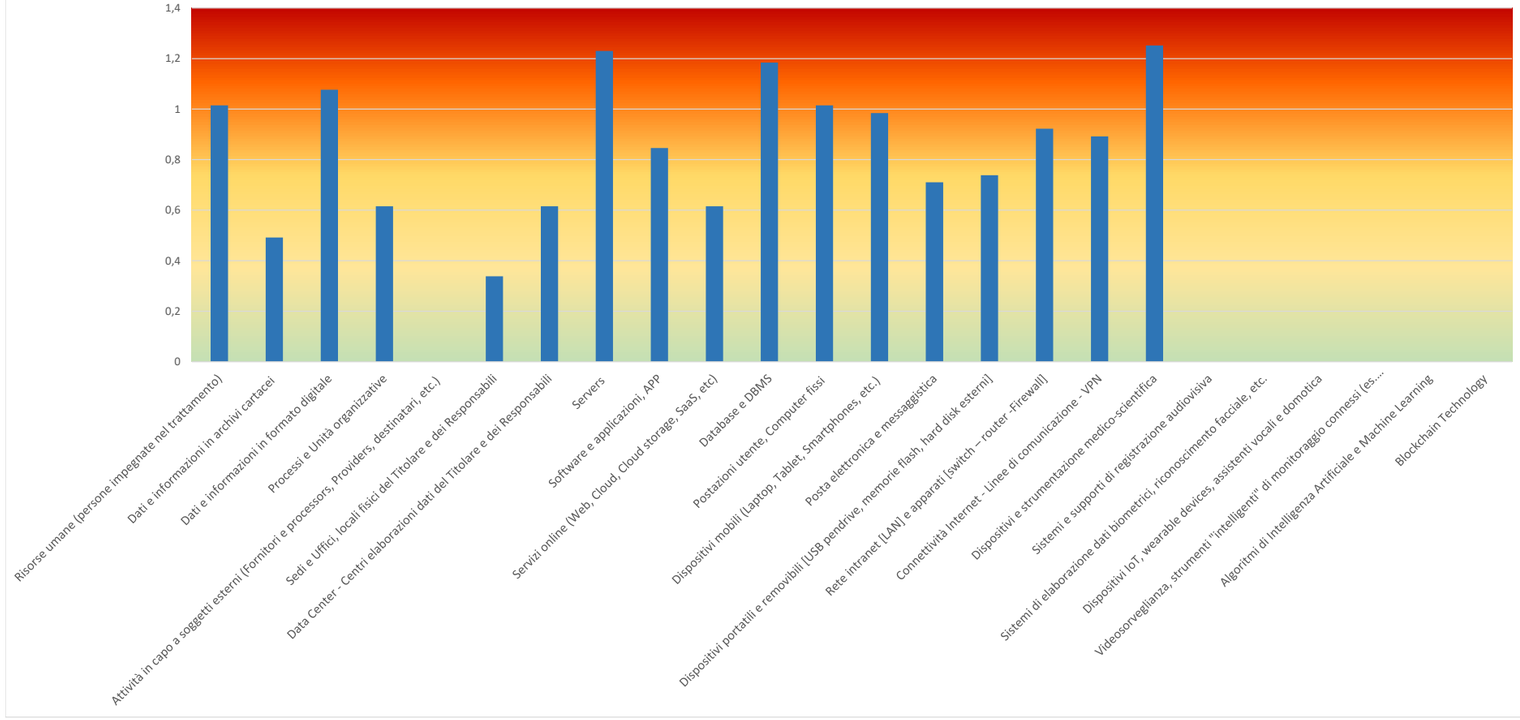
	Disturbi elettromagnetici	ID	*Ambienti WEB*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
Compromissione di dati o servizi per azioni involontarie	**Errori degli utenti nell'uso dei sistemi informativi, inclusa posta elettronica**	ID	*Sistemi di elaborazione Servers e Client*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Abuso o cattivo utilizzo di risorse di sistema	ID	*Sistemi e componenti IT (Servers, Postazioni Client, Apparati Networking, supporti memorizzazione digitali*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Errori di manutenzione hardware e software di base	ID	*Amministratori di Sistema, Servers, PC, Dispositivi, Apparati Networking, Cabling, Antenne Linee comunicazione*	Sì	MEDIO	*Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità ma evento possibile
	Smarrimento di documenti, dispositivi, apparati o memorie di massa	RD	*Sistemi di elaborazione Servers e Client, dispositivi, Apparati Networking*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Recupero di informazioni da documentazione cartacea abbandonata o da supporti o media dismessi (principalmente memorie di massa).	R	*documenti o strumenti e/o supporti di memorizzazione*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità
	Ripudio dei messaggi	I	*Persone impegnate nel trattamento, Comunicazioni ai destinatari*	Sì	BASSO	*Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia avvenga in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore*	Bassa storicità

GDPR RISK ASSESSMENT TOOL

PRINCIPALI FATTORI DI RISCHIO E ESPOSIZIONE MEDIA

CATEGORIE DI MINACCE	Livello MAX Prob.
Minacce alla conformità del trattamento	MEDIO
Eventi con danni fisici/materiali	MEDIO
Eventi Naturali	ALTO
Indisponibilità di Servizi essenziali	MEDIO
Compromissione di dati e informazioni per azioni deliberate	ALTO
Problemi tecnici	ALTO
Compromissione di dati o servizi per azioni involontarie	MEDIO

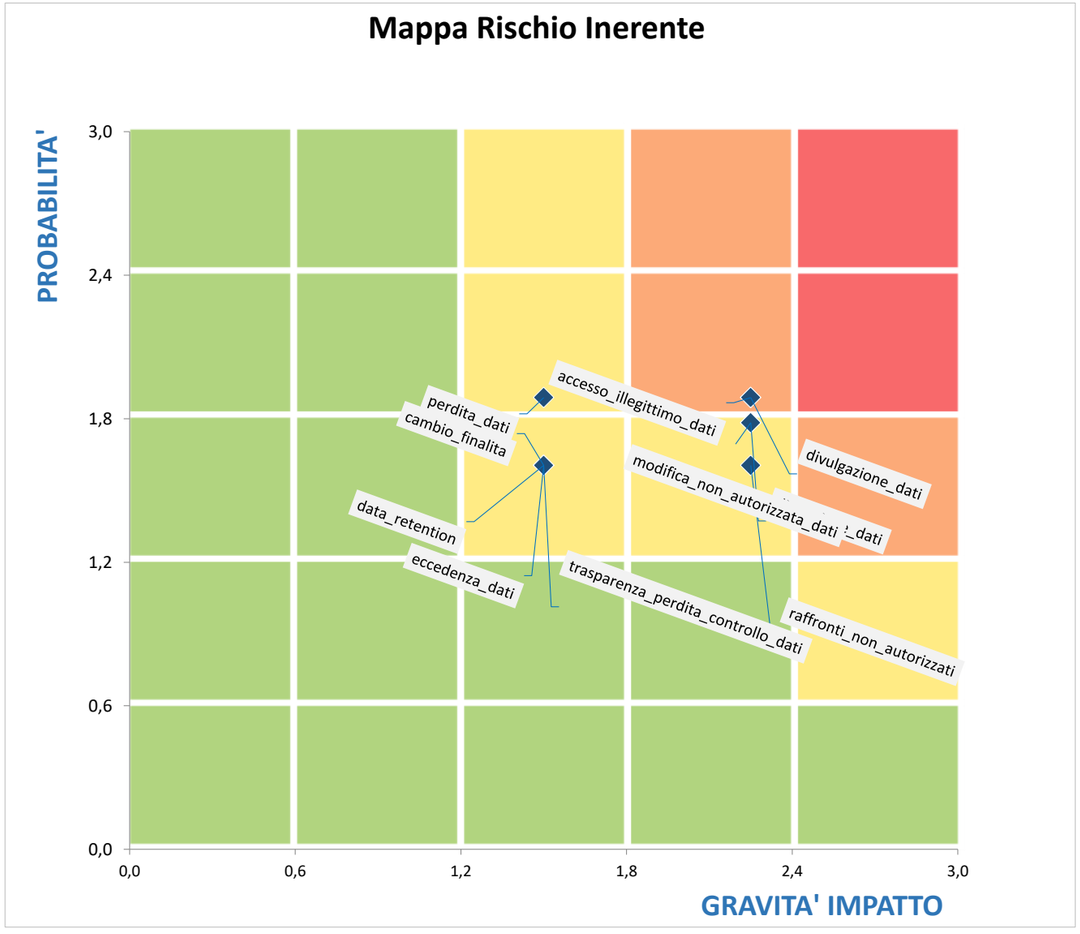
CATEGORIE DI ASSET E RELATIVE POTENZIALI VULNERABILITA' PONDERATE IN BASE ALL'AMBITO DI APPLICAZIONE

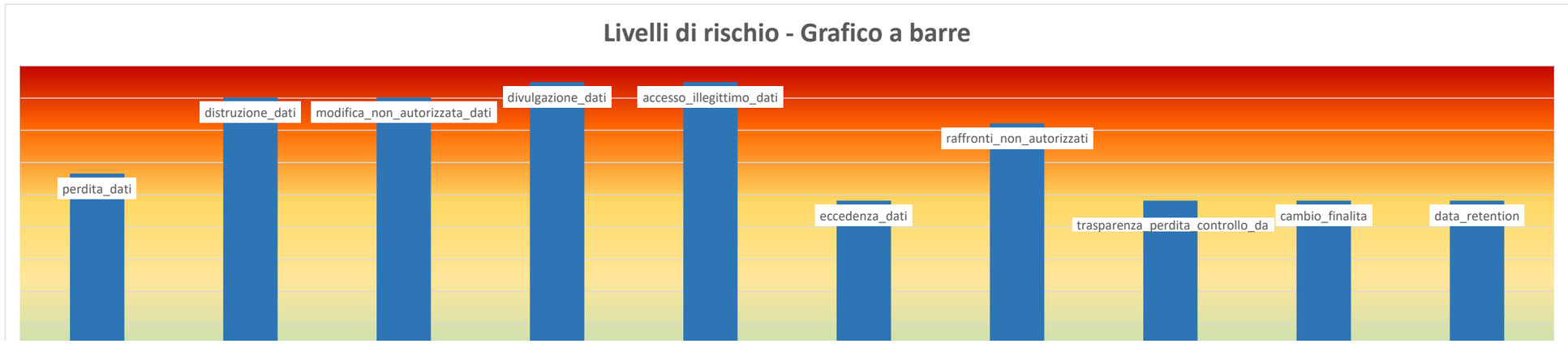


GDPR RISK ASSESSMENT TOOL

RISCHIO INERENTE

Risk ID	Rischio	Grav. Impatto(i)	Prob.(i)	Livello RISCHIO
perdita_dati	**PERDITA DI DATI**	MEDIO	PROBABILE	MEDIO
distruzione_dati	**DISTRUZIONE NON AUTORIZZATA DI DATI**	ELEVATO	POSSIBILE	MEDIO
modifica_non_autorizzata_dati	**MODIFICHE INDESIDERATE O NON AUTORIZZATE AI DATI**	ELEVATO	POSSIBILE	MEDIO
divulgazione_dati	**DIVULGAZIONE NON AUTORIZZATA DI DATI PERSONALI**	ELEVATO	PROBABILE	ALTO
accesso_illegittimo_dati	**ACCESSO ILLEGITTIMO O NON AUTORIZZATO AI DATI**	ELEVATO	PROBABILE	ALTO
eccedenza_dati	**ECCESSIVA RACCOLTA DI DATI PERSONALI**	MEDIO	POSSIBILE	MEDIO
raffronti_non_autorizzati	**COLLEGAMENTI O RAFFRONTI INAPPROPRIATI O NON AUTORIZZATI DI DATI PERSONALI**	ELEVATO	POSSIBILE	MEDIO
trasparenza_perdita_controllo_dati	**PERDITA DI CONTROLLO DA PARTE DEGLI INTERESSATI (MANCANZA DI TRASPARENZA, CHIAREZZA, NON CONSIDERAZIONE DEI DIRITTI)**	MEDIO	POSSIBILE	MEDIO
cambio_finalita	**DIVULGAZIONE O RIUSO PER FINALITÀ DIVERSE DEI DATI PERSONALI SENZA LA CONSAPEVOLEZZA E/O IL CONSENSO DEGLI INTERESSATI**	MEDIO	POSSIBILE	MEDIO
data_retention	**CONSERVAZIONE IMMOTIVAMENTE PROLUNGATA DEI DATI PERSONALI**	MEDIO	POSSIBILE	MEDIO





GDPR RISK ASSESSMENT TOOL

DETERMINAZIONE EFFICACIA DELLE MISURE DI SICUREZZA IN ESSERE

In questa sezione viene impostata l'applicazione delle misure organizzative e tecniche in essere

EVENTO MINACCIOSO		CONTROMISURE	Applicabile	Applicazione	Importanza	Criteri e motivazioni per applicabilità e rilevanza
Minacce alla conformità del trattamento	*Misure organizzative*	Sensibilizzazione e formazione del personale sulla cultura della protezione dati e sui principi fondamentali di liceità correttezza e trasparenza, limitazione finalità, minimizzazione, limitazione della conservazione	Sì	Ben applicata	Significativa	Lo study manager e lo statistical data manager hanno effettuato l'aggiornamento dei corsi di "Good Clinical Pratice-GCP" di cui dispongono certificazione.
	Misure organizzative	Privacy by design e by default e minimizzazione nei processi di trattamento	Sì	Ben applicata	Alta	La scheda di raccolta è stata disegnata per minimizzare il numero di dati personali richiesti. I solo dato anagrafico trattenuto è la data di nascita dell'interessato data la rilevanza statistica. Il paziente viene identificato attraverso un codice univoco ad esclusiva conoscenza dei centri partecipanti.
	Misure generali di sicurezza dei sistemi	Privacy by design e by default inserita nelle tecnologie del trattamento	Sì	Ben applicata	Alta	REDCAP non supporta la conservazione di dati codificati "at rest". Tuttavia, la trasmissione di dati durante la compilazione del questionario è effettuata con il protocollo https.
	Misure organizzative	Comunicazione e informazioni trasparenti, efficaci (es. granulari e stratificate, comprensibili e snelle) agli interessati	Sì	Ben applicata	Alta	Tutte le comunicazioni tra gli interessati avvengono per iscritto o per mezzo elettronico, di cui si dispone tracciabilità e trasparenza. Il linguaggio è semplice, chiaro e conciso.
	Misure organizzative	Definizione puntuale di ruoli, compiti e responsabilità nelle operazioni di trattamento di dati personali	Sì	Ben applicata	Alta	Ogni figura coinvolta, dai responsabili di funzione agli operatori esecutivi, è formalmente identificata e dotata di un mansionario aggiornato che specifichi le attività consentite, i limiti di autonomia, e gli obblighi di controllo.
	Misure organizzative	Attuazione di un modello organizzativo efficace (con procedure, istruzioni, gestione degli incidenti e registrazioni delle non conformità, etc.) e verificato con AUDIT	Sì	Ben applicata	Alta	Sono adottate procedure documentate e la gestione del rischio legato a ogni fase del trattamento. L'efficacia del modello è misurata secondo indicatori di performance (KPI) e verificata periodicamente attraverso audit strutturati secondo standard riconosciuti
	Misure organizzative	Instaurazione e pubblicizzazione di canali di comunicazione e/o punti di contatto per l'esercizio dei diritti degli interessati, richieste di chiarimento, etc.	Sì	Ben applicata	Alta	Ciacun interessato dispone dei contatti degli investigatori principali della sede cui fa riferimento e dello staff del centro Promotore. I contatti sono presenti nel modulo di consenso e nell'informativa Privacy.
Eventi con danni fisici/materiali (Agenti fisici quali incendio, allagamento, attacchi esterni, etc.)	*Misure organizzative*	Progettazione e costruzione in zone distanti da impianti esplosivi, boschi e foreste, fiumi e dighe	Sì	Presente, migliorabile	Alta	Arisist
	Misure organizzative	Separazione impianti e compartimentazione antincendio, Allarmi temperatura e sistemi di rilevazione e auto-spegnimento incendi, gas inerte e interruzione automatica alimentazione	Sì	Presente, migliorabile	Alta	Arisist
	Misure organizzative	Allarmi antiumidità e antiallagamento sotto pavimento flottante	Sì	Presente, migliorabile	Alta	Arisist
	Misure organizzative	Allarmi antintrusione, Locali blindati, Controllo accessi e Videosorveglianza	Sì	Presente, migliorabile	Alta	Arisist
	Misure organizzative	Filtri antipolvere e altri sistemi di pulizia	Sì	Presente, migliorabile	Alta	Arisist
	Misure organizzative	Impianti di condizionamento e ventilazione	Sì	Presente, migliorabile	Alta	Arisist
	Misure organizzative	Personale di Vigilanza	Sì	Presente, migliorabile	Alta	Direzione Generale
Eventi naturali (Terremoti, fenomeni climatici, eruzioni, etc.)	*Misure organizzative*	Progettazione e costruzione/installazione delle infrastrutture in zone non particolarmente soggette a fenomeni naturali disastrosi	Sì	Ben applicata	Alta	Arisist
	Misure organizzative	Sedi / Locali costruiti con tecniche antisismiche	Sì	Ben applicata	Alta	Arisist
	Misure organizzative	Strutture di protezione contro uragani e tempeste	Sì	Presente, migliorabile	Medio-bassa	Arisist
	Misure generali di sicurezza dei sistemi	Utilizzo di Sistemi/supporti di elaborazione e conservazione dati trasportabili in caso di evacuazione	Sì	Presente, migliorabile	Medio-bassa	Arisist
	Misure generali di sicurezza dei sistemi	Sistemi di Continuità operativa (BC) e di Disaster Recovery	Sì	Presente ma inadeguata	Medio-bassa	Arisist
Indisponibilità di Servizi essenziali (interruzioni collegamenti, guasti, sbalzi tensione e/o mancanza di energia, servizi esterni di fornitori, providers etc.)	*Misure generali di sicurezza dei sistemi*	Progettazione impianti e sistemi secondo certificazioni vigenti (es. quadro e sistema distribuzione elettrica, etc.)	Sì	Ben applicata	Alta	Apred
	Misure generali di sicurezza dei sistemi	Gruppo di continuità / UPS / Stabilizzatori	Sì	Presente, migliorabile	Alta	Apred
	Misure generali di sicurezza dei sistemi	Hardware monitoring (con allarmi per surriscaldamenti, guasti componenti, etc.)	Sì	Presente, migliorabile	Alta	Arisist
	Misure generali di sicurezza dei sistemi	Sistemi di elaborazione dati ridondati - Business Continuity	Sì	Presente, migliorabile	Medio-bassa	Arisist
	Misure generali di sicurezza dei sistemi	Linee di comunicazione - connettività Internet ridondate con gestori diversi - Strumenti di bilanciamento del carico	Sì	Presente, migliorabile	Significativa	Aridata
	Misure organizzative	Contratti attivi di manutenzione e assistenza dei Sistemi, Applicazioni, Reti, Tecnologie	Sì	Presente, migliorabile	Alta	Aridata, Arisist
	Misure organizzative	Verifiche garanzie affidabilità dei Fornitori di Servizi (qualificazione fornitori a priori, due diligence di monitoraggio, audit, etc.) e predisposizione contratti con Service Level Agreement idonei	Sì	Presente ma inadeguata	Medio-bassa	Aridata, Arisist
	Misure organizzative	Policy per gestione situazioni emergenza dei servizi affidati all'esterno scoperti (es. anche con preaccordi con fornitori ulteriori)	Sì	Presente, migliorabile	Medio-bassa	Aridata, Arisist
	Misure generali di sicurezza dei sistemi	Vulnerability Assessment periodici	Sì	Presente, migliorabile	Significativa	Aridata

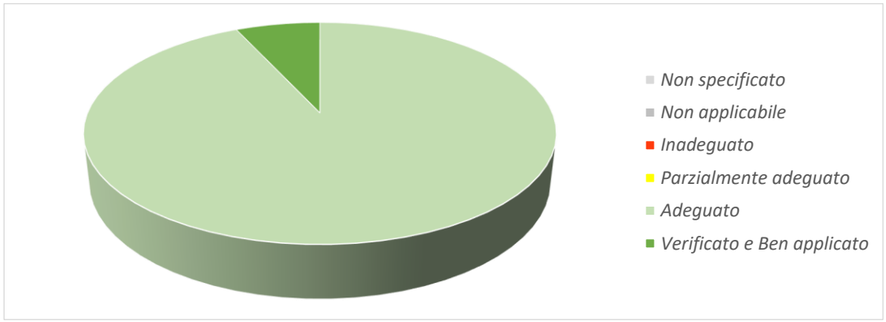
Compromissione di dati e informazioni per azioni deliberate (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	***Misure generali di sicurezza dei sistemi***	Penetration Tests periodici	Sì	**Presente, migliorabile**	**Significativa**	Aridata
	Misure generali di sicurezza dei sistemi	Sistema di crittografia applicato alle comunicazioni	Sì	**Presente, migliorabile**	**Alta**	Aridata
	Misure generali di sicurezza dei sistemi	Crittografia end-to-end nell'uso del Cloud	Sì	**Presente, migliorabile**	**Medio-bassa**	Non applicabile
	Misure applicate ai dati	Crittografia applicata ai database e files di lavoro residenti	Sì	**Assente o non attuata**	**Significativa**	Aridata
	Misure generali di sicurezza dei sistemi	Sistemi di Threat Intelligence - SIEM (security information and event management) - Intrusion Detection Systems e Intrusion Prevention Systems - SOC esterni	Sì	**Presente ma inadeguata**	**Alta**	Aridata
	Misure organizzative	NDA (Non disclosure agreements) - Clausole riservatezza e penali con Fornitori	Sì	**Presente ma inadeguata**	**Medio-bassa**	Aridata, Arisist
	Misure organizzative	Formazione del personale sulle minacce CYBER (Cybersecurity awareness)	Sì	**Presente, migliorabile**	**Alta**	
	Misure generali di sicurezza dei sistemi	Profili di autorizzazione idonei e Segregazione dei ruoli, gestione degli accessi privilegiati	Sì	**Presente ma inadeguata**	**Alta**	Aridata, Arisist, Prof. Sacco
	Misure applicate ai dati	Separazione ambienti dati "critici" da applicazioni e dati non personali	Sì	**Ben applicata**	**Alta**	I dati critici o personali non vengono inseriti nella piattaforma elettronica di raccolta dati (REDCap) cui ha accesso esclusivo lo staff del centro promotore. I centri partecipanti hanno accesso ai dati "critici" dei rispettivi interessati.
	Misure organizzative	Policy per il riutilizzo sicuro e la dismissione di dispositivi elettronici e supporti	Sì	**Presente, migliorabile**	**Medio-bassa**	Non applicabile
	Misure applicate ai dati	Archiviazione sicura della Documentazione cartacea (Cassaforte, Armadi chiusi, Locali chiusi)	Sì	**Presente, migliorabile**	**Medio-bassa**	Aridata, Arisist
	Misure organizzative	Controllo accessi fisico (Portineria, Procedure per gestione chiavi/antifurto/allarme, etc.)	Sì	**Presente, migliorabile**	**Significativa**	Arisist
	Misure applicate ai dati	Utilizzo di Crittografia sui supporti removibili (USB Sticks, Hard disk USB, SD, etc.)	Sì	**Presente, migliorabile**	**Medio-bassa**	Non applicabile
	Misure generali di sicurezza dei sistemi	Gestione sicura dei siti web e delle applicazioni online (Protezione da SQL Injection, CS scripting, Broken Auth e Session Management, Privilege Escalation, Deserialization or Direct Object Reference, XML Entities, CSRF, Broken Access Control, etc)	Sì	**Presente, migliorabile**	**Significativa**	Aridata
	Misure generali di sicurezza dei sistemi	Auditing / Logging sulle postazioni utente e sui sistemi operativi Servers e Client	Sì	**Presente, migliorabile**	**Significativa**	Arisist
	Misure generali di sicurezza dei sistemi	Auditing / Logging sulle applicazioni	Sì	**Presente, migliorabile**	**Significativa**	Aridata
	Misure generali di sicurezza dei sistemi	Sistemi di protezione della Rete (es. MAC Address Binding per rete cablata e wireless)	Sì	**Presente, migliorabile**	**Significativa**	Aridata
	Misure generali di sicurezza dei sistemi	Wifi con protezione crittografica e registrazione e logging utenti	Sì	**Ben applicata**	**Medio-bassa**	Aridata
	Misure generali di sicurezza dei sistemi	Firewall di rete e Appliance con content filtering	Sì	**Presente, migliorabile**	**Alta**	Aridata
	Misure generali di sicurezza dei sistemi	Gestione Patching e Updates sugli apparati (Routers, Firewalls, switches, etc.)	Sì	**Presente, migliorabile**	**Alta**	Aridata
	Misure generali di sicurezza dei sistemi	Verifiche ispettive interne ed esterne (a Fornitori) sul campo e controllo periodico delle policy di Data retention	Sì	**Presente ma inadeguata**	**Medio-bassa**	non applicabile
	Misure applicate ai dati	Salvataggi su supporti diversificati / alternati (evitano la crittazione dei supporti agganciati in caso di cryptolocker)	Sì	**Presente, migliorabile**	**Alta**	Arisist
	Misure generali di sicurezza dei sistemi	Antivirus e anti Malware su workstation - devices - servers	Sì	**Presente, migliorabile**	**Alta**	Arisist
Problemi tecnici (malfunzionamenti software o hardware, guasti e anomalie dei componenti IT)	***Misure organizzative***	Gestion asset inventory organizzata e sistema di allarmistica degli eventi di malfunzionamento	Sì	**Presente, migliorabile**	**Alta**	Arisist
	Misure generali di sicurezza dei sistemi	Test e collaudo dei Software applicativi interni e prodotti esterni prima dell'acquisto	Sì	**Presente, migliorabile**	**Alta**	Aridata
	Misure generali di sicurezza dei sistemi	Manutenzione interna periodica di Sistemi e di reti (Backup configurazioni, verifica firmware, prestazioni hardware, capienza dischi, utilizzo risorse, etc.)	Sì	**Presente, migliorabile**	**Alta**	Aridata, Arisist
	Misure organizzative	Contratti di di manutenzione e assistenza hardware attivi e con Service Level Agreement idonei	Sì	**Presente, migliorabile**	**Alta**	Aridata, Arisist
	Misure organizzative	Contratti di di manutenzione e assistenza software attivi e con Service Level Agreement idonei	Sì	**Presente, migliorabile**	**Alta**	Aridata, Arisist
	Misure applicate ai dati	Sistemi Fault Tolerance (RAID Dischi, Spare parts di ricambio, etc.)	Sì	**Presente, migliorabile**	**Alta**	Arisist
	Misure organizzative	Formazione degli operatori e Amministratori di Sistema	Sì	**Ben applicata**	**Significativa**	Aridata, Arisist
Compromissione di dati o servizi per azioni involontarie (Errori involontari, che possono esporre i dati e i sistemi a virus e malware, uso non autorizzato di strumentazione, accessi non autorizzati a locali fisici, rete, sistemi o banche dati, etc.)	***Misure organizzative***	Formazione e sensibilizzazione del personale interno ed esterno sulla sicurezza dei trattamenti	Sì	**Presente, migliorabile**	**Alta**	Aridata, Arisist
	Misure applicate ai dati	Controllo accessi logici (Profili utente e diritti e privilegi di accesso gestiti e documentati)	Sì	**Ben applicata**	**Alta**	La creazione degli account REDCap con i relativi privilegi è a capo del personale dell'area tecnica-scientifica del Dipartimento di Scienze Cliniche Applicate dell'università. Solo lo study manager e lo statistical data manager dispongono di
	Misure applicate ai dati	Gestione account, autorizzazioni e privilegi organizzata (Es. Identity Management)	Sì	**Ben applicata**	**Alta**	Lo study manager e lo statistical data manager, in quanto parte dello staff del centro promotore, sono le uniche due figure in possesso di profili utente per il sistema REDCap con credenziali separate.
	Misure applicate ai dati	Logging delle operazioni sui dati (creazione, lettura, estrazione, modifica, cancellazione)	Sì	**Ben applicata**	**Medio-bassa**	Il logging delle operazioni sui dati è implementato nel sistema REDCap. Utenti con specifico privilegio di accesso possono ottenere la lista completa delle operazioni sui dati (creazione, lettura, estrazione, modifica e cancellazione) e degli utenti che le hanno effettuate.
	Misure generali di sicurezza dei sistemi	Gestione organizzata dello sviluppo di software e algoritmi	Sì	**Assente o non attuata**	**Medio-bassa**	Non applicabile-non vengono sviluppati software o algoritmi.
	Misure applicate ai dati	Gestione salvataggi dati con snapshot incrementali per recovery errori utente	Sì	**Presente, migliorabile**	**Alta**	Arisist
	Misure organizzative	Formazione specifica e audit al personale sulle vulnerabilità informatiche (ripudio, furti identità, phishing, doxing, pretexting, keylogging, dirottamento browser, etc.)	Sì	**Presente, migliorabile**	**Significativa**	UOSF
	Misure organizzative	Gestione del personale (turnazioni, carichi di lavoro, competenze, knowledge management)	Sì	**Presente, migliorabile**	**Significativa**	Aridata, Arisist

CATEGORIE DI MINACCE	Prob.(iner.)	Efficacia Misure
Minacce alla conformità del trattamento	MEDIO	71,43%
Eventi con danni fisici/materiali	MEDIO	25,00%
Eventi Naturali	ALTO	28,75%
Indisponibilità di Servizi essenziali	MEDIO	19,53%
Compromissione di dati e informazioni per azioni deliberate	ALTO	10,16%
Problemi tecnici	ALTO	28,57%
Compromissione di dati o servizi per azioni involontarie	MEDIO	26,56%

VULNERABILITA' MEDIA DOPO MISURE DI SICUREZZA
70,00%

SELF ASSESSMENT PRESIDIO CONTROLLI SULLE MISURE TECNICO ORGANIZZATIVE

Oltre alle contromisure specifiche per le diverse tipologie di minacce, un modello organizzativo per la Data Protection impone un self assessment del **livello di PRESIDIO** delle misure tecnico-organizzative adottate, con il quale è possibile valutare l'efficacia dei controlli già in essere.



ISTRUZIONI:

Per ogni famiglia di misure organizzative e tecniche va specificato, dopo aver analizzato il contesto, lo **STATO DI ADEGUATEZZA** utilizzando i valori come da Legenda. Il livello di rischio "inerente" valutato in precedenza, sarà di conseguenza ponderato in base ai controlli già in essere, la cui efficacia è funzionale a mitigare gli effetti delle minacce, e in base all'efficacia dei processi per garantire la costante applicazione delle misure per la prevenzione delle minacce (ossia

1- Inadeguato	*Il controllo non è previsto o è assente nella pratica.*
2- Parzialmente adeguato	*Il controllo è applicato sporadicamente o in modo inadeguato, non garantendone quindi l'efficacia.*
3- Adeguato	*Il controllo è applicato ma si rilevano mancanze, soprattutto formali (per esempio, inesattezze nelle procedure).*
4- Verificato e Ben applicato	*Il controllo è sistematicamente applicato e non sono state rilevate inadeguatezze al controllo.*
NA	*Il controllo NON è applicabile (attenzione nell'ottica della governance dovrebbero applicarsi quasi tutti questi macrocontrolli)*

Controllo (Famiglie ISO/IEC 27001 - 29151 - 27701 e ISDP10003:2020)	Valutazione controllo	Rilevanza controllo	NOTE, MOTIVAZIONI E GIUSTIFICAZIONI
Art. 37 38 39 GDPR / ISDP10003 A.2.4 / Designazione, Ruolo e Compiti del **Responsabile della protezione dati**	3	Significativa	*è stato designato l'RPD e sono documentate le scelte compiute per l'individuazione della necessità e i criteri di valutazione e selezione; sono altresì formalizzati i compiti e gli ambiti di operatività, e risultano evidenze dell'operato dell'RPD*
27001 A.10 / 29151 A.10 / Art. 32 GDPR / ISDP10003 A.5.4 / Misure di sicurezza - **pseudonimizzazione e/o cifratura** dei dati personali	3	Alta	*Verificare la concreta applicazione*
27001 A.9 - A.10 - A.11 - A.12 - A.15 - A.17 / 29151 A.9 - A.10 - A.11 - A.12 - A.15 - A.17 / Art. 32 GDPR / ISDP10003 A.5.3 / 27701 A.7.4 - A.7.2.6 - A.7.2.5 / Misure di sicurezza - generale capacità di **assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**	3	Alta	*Verificare la concreta applicazione*
29151-A.6 - A.7 / 27701 - A.7.4.1 e A.7.4.2 / ISDP10003 A.3.1.7 / Art. 5 GDPR **Limitazione della raccolta dati e minimizzazione**	3	Significativa	*Verificare la concreta applicazione*
29151-A.4.1 - A.4.2 / 27701 A.7.2.1. - A.7.2.2 - A.7.3.1 / ISDP10003 A.3.2 e A.3.1.1. / Art. 5 GDPR Applicazione della **Legittimità e Specifica delle finalità**	4	Alta	*Approfondita liceità dello Studio e acquisito parere del Comitato Etico*
29151-A.9.1 - A.9.2 / 27701 - A.7.3.2 - A.7.3.3 / ISDP10003 A.3.3 / Art. 12-14 GDPR **Informative trasparenti e comprensibili - Trasparenza**	3	Alta	*Predisposta informativa ad hoc*
29151 A.3.1 - A.3.2 / 27701 A.7.3.4 / ISDP10003 A.3.2.2 - A.3.2.8 / Art. 7-8 GDPR **Raccolta e gestione dei consensi**	3	Alta	*Affidato al CRO - da verificare efficacia*
29151 A.7.1 / 27701 A.7.4.4 - A.7.4.5 - A.7.4.6 - A.7.4.7 - A.7.4.8 - A.7.4.9 / ISDP10003 A.3.5 / Art. 5 GDPR **Limitazione dell'uso, conservazione e divulgazione**	4	Alta	*Analisi svolta dei dati necessari e data retention impostata*
29151 A.10 / 27701 A.7.3 / ISDP10003 A.3.4 / Artt.15-22 GDPR **Gestione dell'esercizio dei diritti degli interessati**	3	Alta	*Viene proposta specifica informativa e chiesto il consenso per lo Studio ad hoc*
29151 A.8 / 27701 A.7.4.3 / ISDP10003 A.3.1.4 / Art. 5 GDPR **Accuratezza e Qualità dei dati personali**	3	Alta	*I dati registrati vengono rianalizzati per qualità dal coordinamento di Ateneo*
27001 A.05 - A.18 / 29151 A.2 - A.5 / Art. 32 GDPR / 27701 A.7.2 - A.7.4 / ISDP10003 A.1.1 - A.4.1. A.5.1. A.5.3 / **Politica e Procedure per la sicurezza** delle informazioni (Istruzioni documentate per la sicurezza e la protezione dati), inclusa una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**	3	Alta	*Procedure di Ateneo in essere, da rivedere le effettive applicazioni*

27001 A.06 - A.15 / 29151 A.06 - A.11 - A.15 / ISDP10003 A.2 / **Ruoli e responsabilità** per la sicurezza delle informazioni (Organigramma, Istruzioni e policy specifiche per la protezione dei dati personali, Vincoli di riservatezza, separazione dei compiti per evitare conflitti di interesse, Autorizzazioni ai dati personali)	3	Significativa	*Importante in Ateneo, modello impostato ma da verificare e rivedere*
27001 A.08 / 29151. A.8 / ISDP10003 A.5.1 **Gestione del registro delle attività di trattamento e Gestione degli asset** (Censimento, manutenzione, aggiornamenti e monitoraggio dei sistemi di elaborazione - servers - workstations - dispositivi mobile)	3	Alta	*Presente ma da verificare*
27001 A.9 - A.12 / 29151 A.12.1 A.13 / ISDP10003 A.4 / **Procedure operative e responsabilità del personale IT** - Procedure documentate per la gestione delle responsabilità dei Sistemi, e per gestire le attività di sviluppo, test e cambiamenti	3	Alta	*Presenti ma da verificare*
27001 A.15 / 29151-A.11.3-ADD / ISDP10003 A.2.3 - A.7.2 / **Relazione con i fornitori** (clausole contrattuali con processors e subprocessors, diritti di audit, diritto ad acquisire documenti ed evidenze a garanzia dei trattamenti affidati)	3	Alta	*Presenti ma da verificare*
27001 A.16 / 29151-A.7.3 / ISDP10003 A.5.2 / 27701 Section 6 PIMS-specific guidance related to ISO/IEC 27002 / **Gestione degli incidenti relativi alla sicurezza** delle informazioni (Procedure per la gestione degli incidenti e data breach conosciute da autorizzati e processors, distribuzione moduli e/o strumenti per la segnalazione e Registro Incidenti)	3	Alta	*Presenti ma da verificare*
27001 A.17 / 29151 A.17 / ISDP10003 A.5.4 / Art. 32 GDPR / Aspetti relativi alla sicurezza delle informazioni nella gestione della **continuità operativa** (Business continuity Plan, Politica per i livelli di servizio e assegnazione dei compiti in caso di interruzione o indisponibilità, eventuale sito di disaster recovery) o altre misure per dimostrare la **capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**	3	Alta	*Presenti ma da verificare*
27001 A.7 / 29151 A.11.1 / ISDP10003 A.5.4 / Art. 28-29 GDPR / **Sicurezza delle risorse umane** (Vincoli di riservatezza e autorizzazioni documentate, Istruzioni e verifica del rispetto delle procedure)	3	Alta	*Presenti ma da verificare*
27001 A.07.02.02 / 291591 A.11.5 / ISDP10003 A.5.3 / Art. 28-29 GDPR **Consapevolezza, istruzione, formazione e addestramento** sulla sicurezza delle informazioni (sensibilizzazione continua di dipendenti e collaboratori, formazione e informazione, verifica della comprensione delle istruzioni ricevute)	3	Alta	*Presenti ma da verificare*
27001 A.09 / 29151 A.12 / ISDP10003 A.5.2 - A.5.3 - A.5.4 / **Controllo degli accessi ai sistemi per il trattamento dati** (Gestione delle credenziali di accesso univoche, politica di password complesse e dove necessario autenticazione a due fattori, profili di autorizzazione ai soli dati di pertinenza (Applicazione del principio del need to know e segregation of duty, (indispensabilità e necessità, separazione))	3	Alta	*Presenti ma da verificare*
27001 A.12.04 / ISDP10003 A.5.2 - / **Raccolta dei log e monitoraggio** (files di registro attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali (visualizzazione, modifica, cancellazione) sia per gli operatori che per gli amministratori di reti, database e sistemi	3	Alta	*Presenti ma da verificare*
27001 A.12 / ISDP10003 A.5.2 - A.5.3 - A.5.4 / **Sicurezza delle attività operative** (tecniche di crittografia per supporti di memorizzazione (Postazioni e supporti esterni, pseudonimizzazione, query sicure sul db)	3	Alta	*Presenti ma da verificare*
27001 A.14.01 / ISDP10003 A.5.2 - A.5.4 / **Requisiti di sicurezza dei sistemi informativi** (gestione privilegi sulle workstation, antivirus e aggiornamenti di sicurezza, vincoli sui supporti removibili, auditing dei trasferimenti di dati)	3	Alta	*Presenti ma da verificare*
27001 A.13 / ISDP10003 A.5.2 - A.5.4 / **Sicurezza delle comunicazioni** (Navigazione Internet controllata, Firewall, protocolli SSL/TSL, Wireless protette, accessi VPN idoneamente protetti e controllati periodicamente)	3	Alta	*Presenti ma da verificare*
27001 A.12.03 / ISDP10003 A.5.2 - A.5.4 / **Backup** (Politiche e procedure documentate, Salvataggi Registri dei backup e dei test di ripristino, dati backup crittografati e conservati in luogo diverso)	3	Alta	*Presenti ma da verificare*
27001 A.06.02 / **Dispositivi portatili e telelavoro** (Politica mobile devices, BYOD, ruoli e responsabilità definiti e documentati, crittografia per devices che accedono a sistemi IT)	3	Alta	*Presenti ma da verificare*

27001 A.12.6 / **Gestione delle vulnerabilità tecniche** 27001 A.14.2 / **Sicurezza nei processi di sviluppo e supporto** (gestione del ciclo di vita dello sviluppo e dei sistemi, valutazione vulnerabilità e aggiornamenti, patch, verifica sistemi aperti al web, penetration test)	3	Alta	*Presenti ma da verificare*
27001 A.08.03.02 / **Dismissione dei supporti** 27001 A.11.02.07 / **Dismissione sicura o riutilizzo delle apparecchiature** (Procedura documentata per la distruzione controllata e sicura dei documenti cartacei e per la cancellazione sicura dei dati con smagnetizzazione o altre tecniche; affidamento a responsabile esterno con attività supervisionate e certificate)	3	Alta	*Presenti ma da verificare*
27001 A.11 / / ISDP10003 A.5.2 - A.5.3 / **Sicurezza fisica e ambientale** (Le aree ed i locali sono controllati per l'accesso sia al personale che per gli esterni, e protetti con sistemi anti-intrusione, e i criteri di sicurezza e di controllo accessi vengono periodicamente revisionati)	3	Alta	*Presenti ma da verificare*

GDPR RISK ASSESSMENT TOOL

EFFICACIA MISURE ORGANIZZATIVE E TECNICHE E GOVERNANCE

CATEGORIE DI MINACCE	Livello Probabilità iner.	Efficacia Misure	
Minacce alla conformità del trattamento	MEDIO	71,43%	Forte
Eventi con danni fisici/materiali	MEDIO	25,00%	Adeguato
Eventi Naturali	ALTO	28,75%	Adeguato
Indisponibilità di Servizi essenziali	MEDIO	19,53%	Debole
Compromissione di dati e informazioni per azioni deliberate	ALTO	10,16%	Debole
Problemi tecnici	ALTO	28,57%	Adeguato
Compromissione di dati o servizi per azioni involontarie	MEDIO	26,56%	Adeguato

EFFICACIA MEDIA MISURE ORGANIZZATIVE E TECNICHE	
30,00%	Adeguato

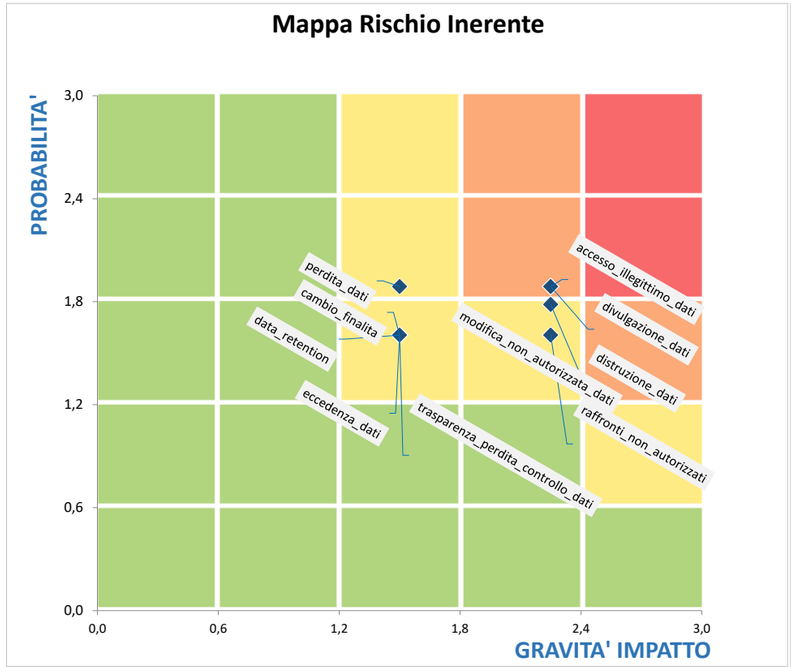
EFFICACIA GOVERNANCE	VULNERABILITA' MEDIA A SEGUITO DELLE MISURE APPLICATE E DEI PRESIDI DI GOVERNANCE NEL CONTESTO DI RIFERIMENTO
74,78%	60,11%

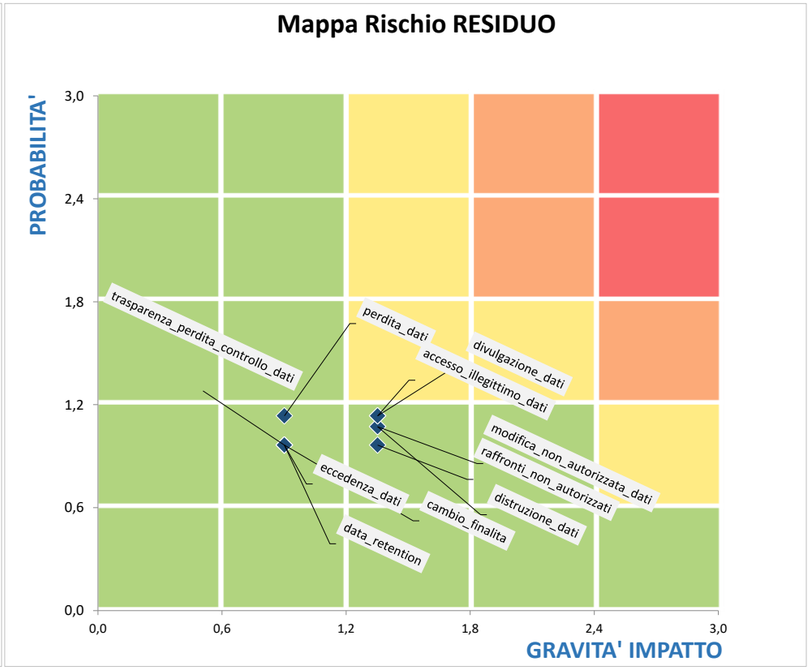
LIVELLO MITIGAZIONE COMPLESSIVO		
	39,89%	Adeguato

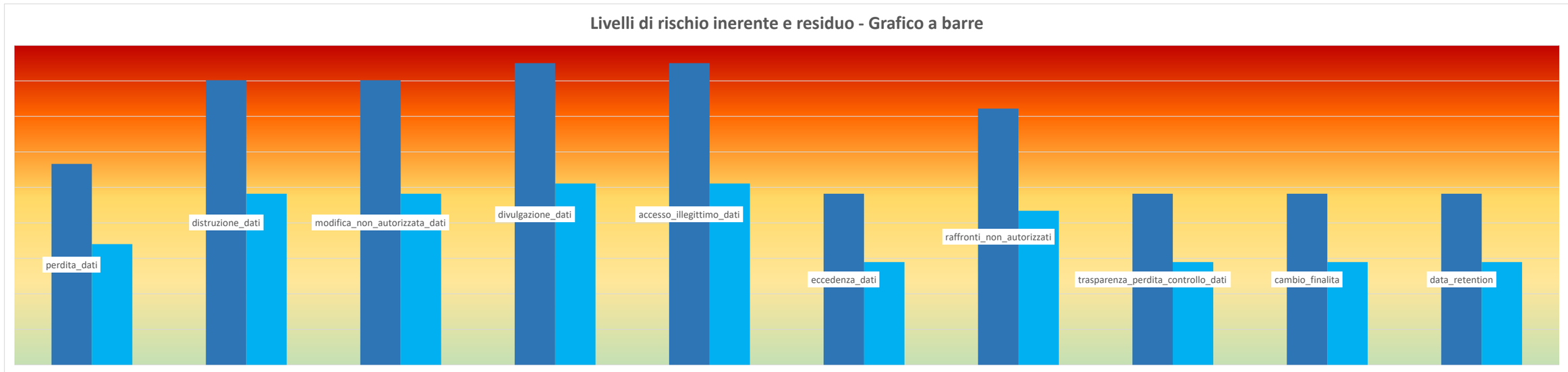
GDPR RISK ASSESSMENT TOOL

MITIGAZIONE DEL RISCHIO (scorrere in basso per i grafici)

Risk ID	Rischio	Impatto (inerente)	Probabilità (inerente)	RISCHIO INERENTE		Impatto (residuo)	Probabilità (residua)	RISCHIO RESIDUO	ACCETTABILITA'
perdita_dati	**PERDITA DI DATI**	MEDIO	PROBABILE	MEDIO	→	BASSO	POCO PROBABILE	**BASSO**	Sì
distruzione_dati	**DISTRUZIONE NON AUTORIZZATA DI DATI**	ELEVATO	POSSIBILE	MEDIO	→	MEDIO	POCO PROBABILE	**BASSO**	Sì
modifica_non_autorizzata_dati	**MODIFICHE INDESIDERATE O NON AUTORIZZATE AI DATI**	ELEVATO	POSSIBILE	MEDIO	→	MEDIO	POCO PROBABILE	**BASSO**	Sì
divulgazione_dati	**DIVULGAZIONE NON AUTORIZZATA DI DATI PERSONALI**	ELEVATO	PROBABILE	ALTO	→	MEDIO	POCO PROBABILE	**BASSO**	Sì
accesso_illegittimo_dati	**ACCESSO ILLEGITTIMO O NON AUTORIZZATO AI DATI**	ELEVATO	PROBABILE	ALTO	→	MEDIO	POCO PROBABILE	**BASSO**	Sì
eccedenza_dati	**ECCESSIVA RACCOLTA DI DATI PERSONALI**	MEDIO	POSSIBILE	MEDIO	→	BASSO	POCO PROBABILE	**BASSO**	Sì
raffronti_non_autorizzati	**COLLEGAMENTI O RAFFRONTI INAPPROPRIATI O NON AUTORIZZATI DI DATI PERSONALI**	ELEVATO	POSSIBILE	MEDIO	→	MEDIO	POCO PROBABILE	**BASSO**	Sì
trasparenza_perdita_controllo_dati	**PERDITA DI CONTROLLO DA PARTE DEGLI INTERESSATI (MANCANZA DI TRASPARENZA, CHIAREZZA, NON CONSIDERAZIONE DEI DIRITTI)**	MEDIO	POSSIBILE	MEDIO	→	BASSO	POCO PROBABILE	**BASSO**	Sì
cambio_finalita	**DIVULGAZIONE O RIUSO PER FINALITÀ DIVERSE DEI DATI PERSONALI SENZA LA CONSAPEVOLEZZA E/O IL CONSENSO DEGLI INTERESSATI**	MEDIO	POSSIBILE	MEDIO	→	BASSO	POCO PROBABILE	**BASSO**	Sì
data_retention	**CONSERVAZIONE IMMOTIVAMENTE PROLUNGATA DEI DATI PERSONALI**	MEDIO	POSSIBILE	MEDIO	→	BASSO	POCO PROBABILE	**BASSO**	Sì






Livelli di rischio inerente e residuo - Grafico a barre
perdita_dati
distruzione_dati
modifica_non_autorizzata_dati
divulgazione_dati
accesso_illegittimo_dati
eccedenza_dati
raffronti_non_autorizzati
trasparenza_perdita_controllo_dati
cambio_finalita
data_retention