DPIA :

Società Ospedale San Raffaele S.r.l.

Panoramica del trattamento

Quale è il trattamento in considerazione?

Processo Ricerca Scientifica

Fase Ricerca clinica

Attività Esecuzione di attività di ricerca scientifica

Descrizione Questo è uno studio osservazionale multicentrico nazionale retrospettivo e prospettico di coorte in cui verranno arruolati i pazienti che verranno sottoposti a chirurgica colorettale. La prima parte dello studio è retrospettiva e la raccolta dei dati inizierà dal 01 gennaio 2022 al 30 giugno 2023. I pazienti arruolati saranno divisi in tre gruppi (FT: fumatori di tabacco; NRT: terapia sostitutiva della nicotina; NF: non fumatori) e i dati verranno confrontati tra i gruppi per valutare se ci sono differenze statisticamente significative riguardo alle complicanze postoperatorie. Il gruppo NF sarà a sua volta suddiviso in pazienti che non hanno mai fumato e in pazienti che hanno smesso di fumare. Una ulteriore analisi di pazienti ex-fumatori sarà eseguita per valutare se l'incidenza di complicanze si discosta da quella osservata nei pazienti che non hanno mai fumato. La seconda parte dello studio sarà prospettica e durerà un anno. Anche in questo studio i pazienti arruolati saranno divisi in tre gruppi (gruppo NF, gruppo FT, e gruppo NRT) e dati ottenuti da tutte le variabili registrate saranno confrontati tra i gruppi. I dati ottenuti i modo retrospettivo e prospettico saranno analizzati insieme per ogni gruppo. L'ipotesi dello studio è che il fumo di tabacco abbia un ruolo rilevante nella comparsa di complicanze postoperatorie. In particolar modo si ipotizza che il gruppo di pazienti che assume NRT (definito come gruppo di pazienti NRT) abbia una incidenza di complicanze postoperatorie dopo chirurgia colorettale superiore a quanto osservato nel gruppo di controllo dei pazienti non fumatori (NF) o ex fumatori ed inferiore al gruppo dei pazienti fumatori di tabacco (FT).

Unità Organizzativa Chirurgia Generale - Chirurgia Colonrettale

Categoria di Interessato	Numerosità degli interessati	Soggetti Vulnerabili	Finalità	Termini di conservazione	Criteri
Pazienti	Migliaia	Soggetti arruolati in studi clinici	Finalità di ricerca scientifica in campo medico, biomedico o epidemiologico	5 anni	

Ruolo dalla Società Titolare del Trattamento

Il trattamento è effettuato in contitolarità? (art. 26 GDPR) No

Il trattamento è effettuato per conto del titolare? (art. 28 GDPR) No

È prevista una comunicazione ad altri Titolari? (art. 2.4 ter a) CP) No

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Categorie di Dati Personali	Subcategoria di Dati Personali
Dati Comuni	Anagrafica e/o dati di contatto
Dati Particolari	Dati relativi alla salute

I dati sono pubblicamente disponibili? No

È prevista diffusione dati a terzi indeterminati? (art. 2.4 ter b) CP) No

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

Note

1. Raccolta dei dati

- I dati vengono raccolti sia **retrospettivamente** (dal 1° gennaio 2022 al 30 giugno 2023) sia **prospetticamente** (per un anno successivo).
- Vengono acquisiti da **pazienti sottoposti a chirurgia colorettale**, raccolti durante il ricovero, nel corso della preparazione all'intervento e fino a 30 giorni dopo l'intervento.
- La raccolta avviene tramite **piattaforma REDCap**, accessibile solo allo staff dello studio

2. Registrazione e pseudonimizzazione

- A ciascun paziente viene assegnato un **codice identificativo**.
- I dati sono **pseudonimizzati**: solo il medico dello studio può associare il codice al nominativo.
- La raccolta avviene in **CRF (Case Report Form)** elettronici, in modo accurato e leggibile, come da documentazione clinica originale.

3. Gestione e protezione

- I dati sono **protetti da accessi non autorizzati** e custoditi nel **Trial Master File**.
- Solo lo **Sperimentatore Principale** e i delegati del centro promotore possono accedere ai dati complessivi.

4. Analisi

- I dati vengono analizzati in forma aggregata.
- Le variabili vengono trattate con **analisi statistica** (test di Mann-Whitney, t-test, regressione logistica ecc.), utilizzando **SPSS 22.0**.

5. Pubblicazione e diffusione

- I risultati saranno **pubblicati in forma anonima** in riviste scientifiche e congressi.
- I dati **non identificabili** saranno comunicati ai ricercatori coinvolti e resteranno di **proprietà dell'IRCCS Ospedale San Raffaele**.

6. Conservazione e aspetti etici

- Lo studio è conforme alla normativa privacy (D.L. 196/2003 e Regolamento UE 679/2016).
- Tutti i pazienti firmano un **consenso informato**, incluso l'uso dei loro dati.

Modalità di raccolta Dati raccolti presso interessato

Quali sono le risorse di supporto ai dati?

Il trattamento è effettuato in modalità cartacea? Si

Il trattamento è effettuato in modalità automatizzata? Si

Asset	Asset Proposto
Secure Web Application (RedCap)	Secure Web Application (RedCap)

Principi Fondamentali

Proporzionalità e necessità

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

Spiegare perché le finalità del trattamento sono specifiche, esplicite e legittime.

Specifici

Il trattamento dei dati è finalizzato a:

- **Valutare l'incidenza e la severità delle complicanze post-operatorie** fino a 30 giorni dall'intervento di chirurgia colorettale in relazione all'abitudine tabagica.
- Confrontare i gruppi di pazienti: **non fumatori (NF), fumatori di tabacco (FT)** e pazienti in **terapia sostitutiva della nicotina (NRT)**.
- Analizzare eventuali differenze anche tra **ex-fumatori e mai fumatori**

Espliciti

- Gli scopi sono chiaramente **definiti nel protocollo di studio** (capitoli 2 e 3).
- Sono descritti nel **consenso informato** che ogni paziente deve firmare prima della partecipazione, inclusa l'autorizzazione all'utilizzo dei dati personali.

Legittimi

- Lo studio ha ottenuto (o otterrà) **approvazione da un Comitato Etico**.
- È svolto **nel rispetto della normativa sulla privacy** (Reg. UE 679/2016 – GDPR e D.Lgs. 196/2003), con misure adeguate per garantire l'anonimizzazione e la sicurezza dei dati.
- Lo studio è **osservazionale, no profit e non commerciale**; quindi non ci sono finalità di lucro legate al trattamento.

Quali sono le basi legali che rendono lecito il trattamento?

Dati Comuni
Consenso dell'interessato, ai sensi dell'art. 6, par. 1 lett. a) del GDPR

Categorie particolari di dati
Consenso dell'interessato, ai sensi dell'art. 9, par. 2 lett. a) del GDPR

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

Spiegare perché ogni dato raccolto è necessario per le finalità del trattamento.

Sì, i dati raccolti nel protocollo PASSAGE sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità dello studio, in conformità con il principio di minimizzazione dei dati sancito dall'articolo 5, paragrafo 1, lettera c) del GDPR .

Adeguatezza e pertinenza

Lo studio raccoglie dati strettamente necessari per valutare l'incidenza e la severità delle complicanze post-operatorie in relazione all'abitudine tabagica nei pazienti sottoposti a chirurgia colorettale. Questi dati includono informazioni cliniche, abitudini tabagiche e terapie sostitutive della nicotina, pertinenti e adeguati per le finalità dichiarate dello studio.

Limitazione dei dati

Il protocollo prevede la raccolta di dati pseudonimizzati, accessibili solo al personale autorizzato, e la conservazione dei dati per un periodo limitato al raggiungimento delle finalità dello studio. Inoltre, lo studio è conforme alle normative sulla privacy, garantendo che i dati siano trattati in modo lecito, corretto e trasparente.

Pertanto, il trattamento dei dati nel protocollo PASSAGE rispetta il principio di minimizzazione dei dati, assicurando che siano raccolti e trattati solo i dati necessari per le finalità specifiche dello studio.

I dati sono esatti e aggiornati? Sì

Descrivere le misure previste per garantire la qualità dei dati.

Nel **Protocollo PASSAGE**, l'aderenza al principio di **esattezza e aggiornamento dei dati** (art. 5, par. 1, lett. d del GDPR) è rispettata **nei limiti del disegno dello studio**, che prevede due fasi:

Dati retrospettivi

- Raccolti **ex post** da documentazione clinica già presente (cartelle, referti, etc.).
- Non essendo "attuali", non possono essere aggiornati nel senso classico del termine.
- Tuttavia, si fa affidamento sull'**accuratezza della documentazione medica originale**.

Il protocollo prevede che i dati retrospettivi siano riportati in CRF "**in modo accurato, completo e leggibile, esattamente come registrati nei documenti originali**"

Dati prospettici

- Raccolti **in tempo reale** durante il ricovero e fino a 30 giorni post-intervento.
- Consentono maggiore **controllo sull'aggiornamento** e verifica dell'esattezza.

È responsabilità dello **staff dello studio**, sotto supervisione dello Sperimentatore Principale, garantire che i dati siano **inseriti correttamente e aggiornati se necessario**.

Strumenti a supporto

- Utilizzo della piattaforma **REDCap** garantisce tracciabilità, controllo degli accessi e possibilità di revisione/miglioramento dei dati.
- Il sistema consente la **modifica dei dati inseriti** da parte degli operatori autorizzati, secondo i criteri delle Good Clinical Practice (GCP).

Qual è il periodo di conservazione dei dati?

Dati comuni 5 anni

Categorie particolari di dati 5 anni

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Per partecipare allo studio ogni paziente dovrà accettare e sottoscrivere il consenso informato, che verrà raccolto retrospettivamente per i pazienti già operati nel periodo di interesse o durante il ricovero relativo all'intervento chirurgico per i pazienti arruolati in modo prospettico. Verrà richiesta l'autorizzazione all'utilizzo dei dati personali

Ove applicabile: come si ottiene il consenso degli interessati?

Tramite sottoscrizione dell'informativa e del relativo consenso specifico

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

Avanzando la richiesta ai contatti indicati all'interno dell'informativa

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

Avanzando la richiesta ai contatti indicati all'interno dell'informativa

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

Avanzando la richiesta ai contatti indicati all'interno dell'informativa

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

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Non sono previsti trasferimenti extra UE

Misure esistenti o pianificate

Misure di Sicurezza

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application (RedCap)	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Application (RedCap)				ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure di Sicurezza in Corso

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.
	Secure Web Application	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
	Secure Web Application (RedCap)	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

Misure di Sicurezza Aziendali

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
			Formazione						Basso		Trasversale			
A.1	A - Security Policy e Procedure Protezione PII	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.2	A - Security Policy e Procedure Protezione PII	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.3	A - Security Policy e Procedure Protezione PII	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.4	A - Security Policy e Procedure Protezione	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	PII	la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.												
A.5	A - Security Policy e Procedure Protezione PII	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.6	A - Security Policy e Procedure Protezione PII	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	"
B.1	B - Ruoli e Responsabilità	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
B.2	B - Ruoli e Responsabilità	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.												
B.3	B - Ruoli e Responsabilità	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
B.4	B - Ruoli e Responsabilità	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
B.5	B - Ruoli e Responsabilità	Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
C.1	C- Access Control Polic	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	y	(coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.												
C.2	C-Access Control Policy	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali.				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Non Conforme	
C.3	C-Access Control Policy	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
C.4	C-Access Control Policy	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
D.1	D-Reso	L'organizzazione dovrebbe disporre				S	S	S	Bass	S	Trasversal	Verti	Conf	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	urce and asset management	di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).				ì	ì	ì	o	ì	e	cale	orme	
D.2	D-Resource and asset management	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.				Sì	Sì	Sì	Basso		Trasversale	Trasversale	Conforme	
D.3	D-Resource and asset management	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
D.4	D-Resource and asset management	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Non Applicabile	
E.1	E - Change	L'organizzazione deve assicurarsi che tutte le				Sì	Sì	Sì	Bass	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	Management	modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.							o					
E.2	E - Change Management	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
E.3	E - Change Management	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.												
F.1	F - Data Processor (responsabile esterno)	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
F.2	F - Data Processor (responsa	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	bile esterno)	informa il titolare del trattamento senza indebiti ritardi.												
F.3	F - Data Processor (responsabile esterno)	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
F.4	F - Data Processor (responsabile esterno)	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
F.5	F - Data Processor (responsabile ester	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi				Sì	No	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	no)	documentati di riservatezza / non divulgazione.												
G.1	G - Gestione Incidenti/ Personal Data breaches	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
G.2	G - Gestione Incidenti/ Personal Data breaches	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	
G.3	G - Gestione Incidenti/ Personal Data breaches	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Non Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
G.4	G - Gestione Incidenti/ Personal Data breaches	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
H.1	H - Business Continuity	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).				No	No	Sì	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
H.2	H - Business Continuity	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	
H.3	H - Business Continuity	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		personali.												
H.4	H - Business Continuity	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.				No	No	Sì	Alto	Sì	Trasversale	Verticale	Non Conforme	
H.5	H - Business Continuity	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.				No	No	Sì	Alto	Sì	Trasversale	Verticale	Conforme	
I.1	I - Riservatezza del personale	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
I.2	I - Riservatez	Prima di assumere i propri compiti, i dipendenti,				Sì	No	No	Med	Sì	Trasversal	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	za del personale	lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.							io		e			
I.3	I - Riservatezza del personale	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	
J.1	J - Training	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.												
J.2	J - Training	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
J.3	J - Training	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
K.1	K - Controllo Accessi e autenticazione	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.2	K - Controllo Accessi e autenticazione	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.												
K.3	K - Controllo Accessi e autenticazione	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.4	K - Controllo Accessi e autenticazione	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	
K.5	K - Controllo Accessi e autenticazione	Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
K.6	K - Controllo Accessi e autenticazione	Le password degli utenti devono essere memorizzate in una forma "hash".				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
K.7	K - Controllo Accessi e autenticazione	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
K.8	K - Controllo Accessi e autenticazione	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
L.1	L - Logging e Monitoraggio	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica,				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		cancellazione).												
L.2	L - Logging e Monitoraggio	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
L.3	L - Logging e Monitoraggio	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
L.4	L - Logging e Monitoraggio	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
L.5	L - Logging e Monitoraggio	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
M.1	M - Server/Dat	I server ove risiedono database e				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	abase security - crittografia	applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.											Conforme	
M.2	M - Server/Database security - crittografia	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
M.3	M - Server/Database security - crittografia	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.4	M - Server/Database security - crittografia	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.5	M - Server/Database security - crittografia	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		senza ulteriori informazioni.												
M.6	M - Server/Database security - crittografia	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
N.1	N - Workstation security	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
N.2	N - Workstation security	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.3	N - Workstation security	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.4	N - Workstation security	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.5	N - Workstation secur	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ity	devono essere installati regolarmente.												
N.6	N - Workstation security	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
N.7	N - Workstation security	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.8	N - Workstation security	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.				Sì	Sì	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.9	N - Workstation security	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.1	O - Sicurezza del network e	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	delle comunicazioni	crittografata tramite protocolli crittografici (TLS / SSL).												
O.2	O - Sicurezza del network e delle comunicazioni	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	
O.3	O - Sicurezza del network e delle comunicazioni	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	
O.4	O - Sicurezza del network e delle comunicazioni	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
O.5	O - Sicurezza del network e delle comu	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Non Applicabile	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	nicazioni	dei dati personali.												
O.6	O - Sicurezza del network e delle comunicazioni	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.7	O - Sicurezza del network e delle comunicazioni	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
P.1	P - Back up dati	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.				No	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
P.2	P - Back up dati	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	
P.3	P - Back up dati	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
P.4	P - Back up dati	I backup completi devono essere eseguiti regolarmente.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
P.5	P - Back up	I supporti di backup dovrebbero essere				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	dati	testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.												
P.6	P - Back up dati	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.7	P - Back up dati	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.8	P - Back up dati	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare del trattamento.				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Non Applicabile	
P.9	P - Back up dati	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.				Sì	Sì	Sì	Alto	Sì	Verticale	Verticale	Conforme	
Q.1	Q - Mobile/Portable Devices	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
Q.2	Q - Mobile/Portable Devic	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	es	pre-registrati e pre-autorizzati.												
Q.3	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
Q.4	Q - Mobile/Portable Devices	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
Q.5	Q - Mobile/Portable Devices	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.6	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.7	Q - Mobile/Portable Devices	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.				Sì	No	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.8	Q - Mobile/Po	Per l'accesso ai dispositivi mobili è necessario				Sì	Sì	No	Alto	Sì	Trasversal	Verticale	Non Conf	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	rtable Devices	prendere in considerazione l'autenticazione a due fattori (autenticazione forte).									e		orme	
Q.9	Q - Mobile/Portable Devices	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
R.1	R - Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.2	R - Sicurezza del ciclo di vita delle applicazioni	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.3	R - Sicurezza del ciclo di vita delle applicazioni	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.4	R -	Dovrebbero				S	S	S	Ba	S	Verti	Verti	Conf	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	Sicurezza del ciclo di vita delle applicazioni	essere seguiti standard e pratiche di codifica sicure.				ì	ì	ì	sso	ì	cale	cale	orme	
R.5	R - Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.6	R - Sicurezza del ciclo di vita delle applicazioni	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.7	R - Sicurezza del ciclo di vita delle applicazioni	Devono essere eseguiti test periodici di penetrazione.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.8	R - Sicur	Si dovrebbero ottenere				S	S	S	Med	S	Verti	Verti	Conf	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ezza del ciclo di vita delle applicazioni	informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.				ì	ì	ì	io	ì	cale	cale	orme	
R.9	R - Sicurezza del ciclo di vita delle applicazioni	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
S.1	S - Cancellazione/ Eliminazione dei Dati	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	
S.2	S - Cancellazione/ Eliminazione dei Dati	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.				Sì	No	No	Basso		Trasversale	Verticale	Non Applicabile	
S.3	S - Cancellazione/ Eliminazione dei Dati	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Non Applicabile	
S.4	S - Canc	Se i servizi di terzi sono utilizzati per				Sì	No	No	Med	Sì	Trasversal	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ellazione/ Eliminazione dei Dati	disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.							io		e			
S.5	S - Cancellazione/ Eliminazione dei Dati	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	
S.6	S - Cancellazione/ Eliminazione dei Dati	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Non Applicabile	
T.1	T - Sicurezza Fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	
T.2	T - Sicurezza Fisica	Meccanismi di identificazione tramite mezzi appropriati, ad es. i badge				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.												
T.3	T - Sicurezza Fisica	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.4	T - Sicurezza Fisica	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.5	T - Sicurezza Fisica	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.6	T - Sicurezza Fisica	Le aree protette vuote dovrebbero essere bloccate fisicamente e controllate periodicamente.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.7	T - Sicurezza Fisica	Ddovrebbero essere attivati nella sala server un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di				No	No	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		continuità (UPS).												
T.8	T - Sicurezza Fisica	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Misure Non Utilizzate

Misure Non Utilizzate

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
			Formazione						Basso		Trasversale			
A.1	A - Security Policy e Procedure Protezione PII	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.2	A - Security Policy e Procedure Protezione PII	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.3	A - Security Policy e Procedure Protezione	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	PII	policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate.												
A.4	A - Security Policy e Procedure Protezione PII	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.5	A - Security Policy e Procedure Protezione PII	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.6	A - Security Policy e Procedure Protezione PII	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	"
B.1	B - Ruoli e Responsa	Ruoli e responsabilità relative al trattamento dei dati personali				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	bilità	sono chiaramente definite e allocate in accordo con la security policy aziendale												
B.2	B - Ruoli e Responsabilità	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
B.3	B - Ruoli e Responsabilità	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
B.4	B - Ruoli e Responsabilità	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
B.5	B - Ruoli e	Compiti e responsabilità in conflitto, ad				Sì	Sì	Sì	Alto	Sì	Trasversal	Trasversal	Parzialme nte	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	Responsabilità	esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.									e	e	Conforme	
C.1	C-Access Control Policy	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
C.2	C-Access Control Policy	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali.				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Non Conforme	
C.3	C-Access	Dovrebbe essere chiaramente definita e				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	Control Policy	documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).											Conforme	
C.4	C-Access Control Policy	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
D.1	D-Resource and asset management	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
D.2	D-Resource and asset manageme	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.				Sì	Sì	Sì	Basso		Trasversale	Trasversale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	nt													
D.3	D-Resource and asset management	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
D.4	D-Resource and asset management	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Non Applicabile	
E.1	E - Change Management	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
E.2	E - Change Management	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		(non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.												
E.3	E - Change Management	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
F.1	F - Data Processor (responsabile esterno)	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione e del Titolare del trattamento.												
F.2	F - Data Processor (responsabile esterno)	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
F.3	F - Data Processor (responsabile esterno)	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
F.4	F - Data Processor (responsa	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	bile esterno)	controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.												
F.5	F - Data Processor (responsabile esterno)	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.				Sì	No	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
G.1	G - Gestione Incidenti/ Personal Data breaches	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
G.2	G - Gestione Incidenti/ Personal Data breaches	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.												
G.3	G - Gestione Incidenti/ Personal Data breaches	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Non Conforme	
G.4	G - Gestione Incidenti/ Personal Data breaches	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
H.1	H - Business Continuity	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).				No	No	Sì	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
H.2	H - Business Continuity	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		(seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.												
H.3	H - Business Continuity	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	
H.4	H - Business Continuity	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.				No	No	Sì	Alto	Sì	Trasversale	Verticale	Non Conforme	
H.5	H - Business Continuity	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.				No	No	Sì	Alto	Sì	Trasversale	Verticale	Conforme	
I.1	I - Riservatezza del personale	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.												
I.2	I - Riservatezza del personale	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Conforme	
I.3	I - Riservatezza del personale	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	
J.1	J - Training	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.												
J.2	J - Training	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
J.3	J - Training	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
K.1	K - Controllo Accessi e	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	autenticazione	a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.												
K.2	K - Controllo Accessi e autenticazione	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.3	K - Controllo Accessi e autenticazione	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.4	K - Controllo Accessi e auten	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ticazione	l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).												
K.5	K - Controllo Accessi e autenticazione	Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
K.6	K - Controllo Accessi e autenticazione	Le password degli utenti devono essere memorizzate in una forma "hash".				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
K.7	K - Controllo Accessi e autenticazione	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
K.8	K - Controllo Accessi e autenticazi	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	one	trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.												
L.1	L - Logging e Monitoraggio	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
L.2	L - Logging e Monitoraggio	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
L.3	L - Logging e Monitoraggio	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
L.4	L - Logging e Monitorag	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	gio	di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.												
L.5	L - Logging e Monitoraggio	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
M.1	M - Server/Database security - crittografia	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
M.2	M - Server/Database security - crittografia	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
M.3	M - Server/Database security - critto	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	grafia	hardware.												
M.4	M - Server/Database security - crittografia	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.5	M - Server/Database security - crittografia	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.6	M - Server/Database security - crittografia	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
N.1	N - Workstation security	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
N.2	N - Workstation security	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
N.3	N - Workstation security	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.4	N - Workstation security	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.5	N - Workstation security	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.6	N - Workstation security	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
N.7	N - Workstation security	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.8	N - Workstation security	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per				Sì	Sì	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Azienda le	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.												
N.9	N - Workstation security	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.1	O - Sicurezza del network e delle comunicazioni	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.2	O - Sicurezza del network e delle comunicazioni	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	
O.3	O - Sicurezza del network e delle comunicazioni	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza)				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		attraverso dispositivi predefiniti.												
O.4	O - Sicurezza del network e delle comunicazioni	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
O.5	O - Sicurezza del network e delle comunicazioni	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Non Applicabile	
O.6	O - Sicurezza del network e delle comunicazioni	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.7	O - Sicurezza del network e delle comunicazioni	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
P.1	P - Back up dati	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.				No	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
P.2	P - Back up dati	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	
P.3	P - Back up dati	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
P.4	P - Back up dati	I backup completi devono essere eseguiti regolarmente.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
P.5	P - Back up dati	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.6	P - Back up dati	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.7	P - Back up dati	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.8	P - Back up dati	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare del trattamento.				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Non Applicabile	
P.9	P - Back	Le copie dei backup				S	S	S	Alt	S	Verti	Verti	Conf	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	up dati	dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.				ì	ì	ì	o	ì	cale	cale	orme	
Q.1	Q - Mobile/Portable Devices	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
Q.2	Q - Mobile/Portable Devices	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	
Q.3	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
Q.4	Q - Mobile/Portable Devices	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
Q.5	Q - Mobile/Portable Devices	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile				Sì	No	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		che è stato compromesso.												
Q.6	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.7	Q - Mobile/Portable Devices	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.				Sì	No	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.8	Q - Mobile/Portable Devices	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).				Sì	Sì	No	Alto	Sì	Trasversale	Verticale	Non Conforme	
Q.9	Q - Mobile/Portable Devices	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
R.1	R - Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.2	R - Sicurezza del ciclo di	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	vita delle applicazioni	sviluppo.												
R.3	R - Sicurezza del ciclo di vita delle applicazioni	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.4	R - Sicurezza del ciclo di vita delle applicazioni	Dovrebbero essere seguiti standard e pratiche di codifica sicure.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.5	R - Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.6	R - Sicurezza del ciclo di vita delle applicazio	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ni	operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.												
R.7	R - Sicurezza del ciclo di vita delle applicazioni	Devono essere eseguiti test periodici di penetrazione.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.8	R - Sicurezza del ciclo di vita delle applicazioni	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.9	R - Sicurezza del ciclo di vita delle applicazioni	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
S.1	S - Cancellazione/ Eliminazione dei Dati	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		distruzione fisica.												
S.2	S - Cancellazione/ Eliminazione dei Dati	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.				Sì	No	No	Basso		Trasversale	Verticale	Non Applicabile	
S.3	S - Cancellazione/ Eliminazione dei Dati	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Non Applicabile	
S.4	S - Cancellazione/ Eliminazione dei Dati	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Conforme	
S.5	S - Cancellazione/ Eliminazione dei Dati	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	
S.6	S - Cancellazione/ Eliminazione	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file				Sì	No	No	Alto	Sì	Trasversale	Verticale	Non Applicabile	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	dei Dati	cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali.												
T.1	T - Sicurezza Fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	
T.2	T - Sicurezza Fisica	Meccanismi di identificazione tramite mezzi appropriati, ad es. i badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.3	T - Sicurezza Fisica	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.4	T - Sicurezza Fisica	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.5	T - Sicur	Se del caso, dovrebbero essere				Sì	Sì	Sì	Med	Sì	Trasversal	Trasversal	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ezza Fisica	costruite barriere fisiche per impedire l'accesso fisico non autorizzato.							io		e	e		
T.6	T - Sicurezza Fisica	Le aree protette vuote dovrebbero essere bloccate fisicamente e controllate periodicamente.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.7	T - Sicurezza Fisica	Ddovrebbero essere attivati nella sala server un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS).				No	No	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.8	T - Sicurezza Fisica	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali
Utilizzo da parte di terzi di dati dell'interessato
Perdita di controllo dei propri dati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia
Comportamenti sleali/fraudolenti
Attacco informatico (es. social engineering, man in the middel, denial of ervice, brute force, etc.)
Furto e/o perdita di dispositivi, supporti di memorizzazione, documenti

Quali sono le fonti di rischio?

Fonte
Fonti umane esterne (es. criminali informatici, fornitori, utenti)
Fonti umane interne accidentali (es. collaboratori negligenti)

Misure Applicate

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application (RedCap)	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure da Applicare

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.
	Secure Web Application (RedCap)	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
	Secure Web Application (RedCap)	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

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

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

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali
Dati non esatti e/o non aggiornati

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Minaccia
Errore operativo

Quali sono le fonti di rischio?

Fonte
Fonti umane interne accidentali (es. collaboratori negligenti)

Misure Applicate

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
					come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application (RedCap)	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
					persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure da Applicare

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				senza ulteriori informazioni.
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.
	Secure Web Application (RedCap)	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
	Secure Web Application	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

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

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

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Impatti Potenziali
Costi aggiuntivi

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Minaccia
Errore operativo

Quali sono le fonti di rischio?

Fonte
Eventi tecnologici (es. guasti, malfunzionamenti, etc.)
Fonti umane interne accidentali (es. collaboratori negligenti)

Misure Applicate

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
					al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure da Applicare

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.

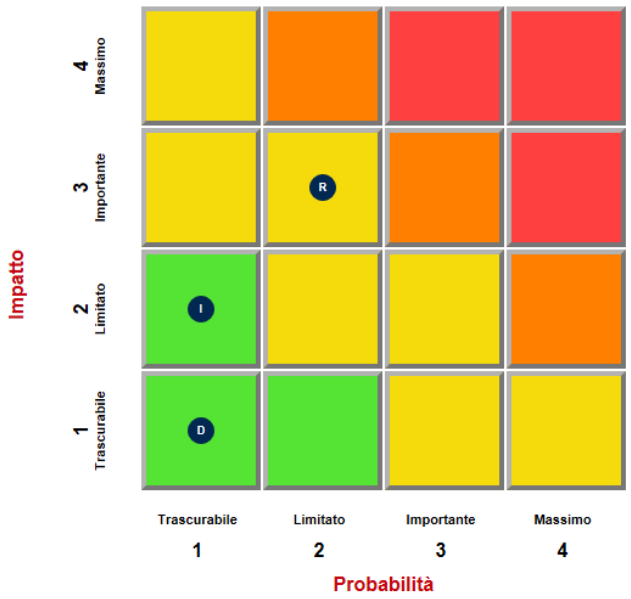
Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.
	Secure Web Application (RedCap)	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
	Secure Web Application (RedCap)	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	(RedCap)				utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

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

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

Mappatura del rischio



		Probabilità	Impatto
R	Riservatezza	Limitato	Importante
I	Integrità	Trascurabile	Limitato
D	Disponibilità	Trascurabile	Trascurabile

Il rischio del trattamento è dunque Limitato

Pareri DPO/RDP e interessati

Nome/i DPO/RDP	Giorgio Presepio
Tenuto conto di quanto segue	Il trattamento può essere implementato
Specifichi le motivazioni della sua scelta	Il trattamento è necessario per lo svolgimento di uno studio osservazionale scientifico volto a valutare l'associazione tra abitudine tabagica e incidenza di complicanze post-operatorie in pazienti sottoposti a chirurgia colorettale. Lo studio è condotto in conformità con i principi etici della Dichiarazione di Helsinki, le Good Clinical Practice (GCP) e la normativa vigente in materia di protezione dei dati personali, in particolare il Regolamento UE 2016/679 (GDPR) e il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018. Il trattamento dei dati personali e particolari (categorie particolari di dati, art. 9 GDPR) è fondato sulle seguenti basi giuridiche: • Consenso esplicito dell'interessato, ottenuto tramite modulo informativo e firmato, conforme agli artt. 6, par. 1, lett. a) e 9, par. 2, lett. a) del GDPR; • Finalità di ricerca scientifica, nel rispetto delle garanzie previste dall'art. 89 del GDPR, con misure tecniche e organizzative adeguate per la protezione dei diritti e delle libertà degli interessati. Il trattamento è inoltre: • Limitato ai dati strettamente necessari per il raggiungimento delle finalità scientifiche indicate nel protocollo; • Pseudonimizzato, tramite l'utilizzo di codici identificativi non direttamente riconducibili all'identità del paziente; • Sottoposto a controlli di accesso, audit e protezioni logiche su piattaforma REDCap, nel rispetto del principio di accountability e di sicurezza dei dati. La base giuridica, le finalità specifiche, i soggetti autorizzati al trattamento e le misure di sicurezza sono descritti nel protocollo approvato dal Comitato Etico dell'IRCCS Ospedale San Raffaele, promotore dello studio.
Parere degli Interessati	Non è stato chiesto il parere degli interessati
Scheda Completata	No