Valutazione d’impatto sulla protezione dei dati

DPIA REMARKER

13/07/2026

Indice

1. Introduzione

Il presente documento “DPIA REMARKER” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “Studio REMARKER”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

2. Informazioni essenziali

Data di creazione dell’analisi	12/06/2026
Data generazione documento	13/07/2026
Data del prossimo controllo	30/06/2027
Stato	Definitivo
Reporter	ALBERTO LONTANO

3. Stima del rischio e pre-assessment

Pre-Assessment

Tipologia del trattamento	Risposta
Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti dell’interessato.	No
Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).	No

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

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

Stima del rischio

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

4. Informazioni sul trattamento

Codice identificativo	Nome	Data di creazione	Data dell'ultima modifica
626	Studio REMARKER	12/06/2026	13/07/2026

Descrizione

La tomografia a coerenza ottica (OCT) permette la visualizzazione degli strati retinici, sede di danno in molteplici patologie (degenerazione maculare senile [AMD], pucker maculare, distacco di retina regmatogeno, patologie vascolari come la retinopatia diabetica e l'occlusione venosa). Individuare biomarcatori associati a progressione di malattia per le malattie croniche, come l'AMD, o al recupero post-chirurgico nelle patologie acute, come il distacco di retina, permetterebbe, nel primo caso, di adottare corrette tempistiche di monitoraggio e trattamento della patologia, e, nel secondo, di individuare i fattori preoperatori associati a maggior recupero visivo in dipendenza dell'intervento ricevuto, con conseguente standardizzazione dell'approccio chirurgico.

Obiettivi dello studio sono:

1. Valutare i biomarcatori OCT associati a evoluzione a AMD neovascolare o atrofica;

2. valutare i biomarcatori OCT associati a miglior recupero visivo in pazienti affetti da distacco di retina regmatogeno primario;

3. valutare i biomarcatori OCT associati a minor presenza di metamorfopsie in pazienti sottoposti a intervento chirurgico per foro maculare o pucker maculare.

Lo studio prevede la raccolta di dati retrospettivi e di dati prospettici.

Rispetto al trattamento dei dati dei pazienti, AOU "Maggiore della Carità" di Novara, ASST Ovest Milanese, Ospedale di Circolo e Fondazione Macchi di Varese - ASST dei Sette Laghi si configurano come Titolari autonomi.

Engineering (cartella clinica elettronica ambulatoriale) e Mrdoc (software Ophthal) si configurano come Responsabili del trattamento dati.

I dati saranno pseudonimizzati, con una chiave di pseudonimizzazione conservata presso le rispettive Direzioni Sanitarie.

Finalità del trattamento

Ricerca scientifica	
Basi giuridiche	
Articolo 6 a) - L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità - consenso acquisito in modalità cartacea	
Articolo 9 a) – l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche	
Articolo 9 j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.	
Basi giuridiche	
artt. 6, par. 1, lett. a), 9, par. 2, lett. a) e lett j), del Regolamento (UE) 2016/679 e art. 110 del D.lgs. 196/2003 e ss.mm.ii., Mentre per la coorte prospettica (1000 pazienti) agli interessati vengono sottoposti informative e consensi alla partecipazione allo studio e al trattamento dati, per la coorte retrospettiva non è possibile informare singolarmente gli interessati e ottenerne il relativo consenso a causa della sussistenza delle seguenti ragioni organizzative ed etiche:, - elevato numero complessivo dei soggetti da arruolare nello studio (3000 pazienti)	
Origine dei dati	
Raccolti presso l'interessato	
Dati già raccolti	
Modalità del trattamento	
Informatizzato	
Categorie di dati	
Categorie particolari di dati personali	
Sanitari	Stato di salute attuale del paziente
	Stato di salute pregresso del paziente
Biometrici	biometrici
Dati personali comuni	
Anagrafici ordinari	Data di Nascita
Foto e video	

Categorie di interessati	
Assistiti dal SSN	
Titolare	AOU Maggiore della Carità di Novara
Responsabile della protezione dei dati	SLALOM srl ; Alessandra Gaetano
Diffusione dei dati	Non viene effettuata la diffusione dei dati.
Trasferimenti e comunicazioni dei dati	
Il trattamento prevede il trasferimento o la comunicazione di dati	
Periodo di conservazione dei dati personali	
Durata attività/procedimento	
Descrizione del periodo di conservazione dei dati	
In conformità al principio di limitazione della conservazione i dati saranno conservati per 7 anni a partire dalla conclusione dello studio.	
Applicativi	ELLIPSE AMB
Note	
I dati raccolti deriveranno dall'analisi retrospettiva e prospettica delle cartelle cliniche elettroniche e delle immagini OCT. I dati demografici e clinici (diagnosi, età, sesso, acuità visiva, presenza di metamorfopsie, esame del fundus, condizione del cristallino, lunghezza assiale, profondità della camera anteriore, farmaci, trattamenti parachirurgici e chirurgici effettuati) saranno estrapolati dalle cartelle cliniche elettroniche ambulatoriali. I dati OCT saranno scaricati come raw files dall'archivio dello strumento OCT Spectralis (Heidelberg Engineering, Heidelberg, Germany) e Swept-Source DRI OCT Triton Plus (Topcon Medical Systems Europe, Milan, Italy). Le immagini a colori del fondo oculare saranno scaricate come raw files dall'archivio dello strumento iCare Eidon TrueColor Confocal fundus imaging system. È prevista l'analisi dei dati OCT ricavati dall'OCT Spectralis (Heidelberg Engineering, Heidelberg, Germany) tramite software Ophthal	

Descrizione sistematica delle componenti del trattamento

Descrizione delle diverse componenti tecnologiche, fisiche ed organizzative che partecipano dell'attività di trattamento valutata.

Componenti organizzative

Componente	Descrizione
Soggetti Interni	**Descrizione sintetica (es. soggetti facenti parte o meno del personale tecnico informatico, descrizione delle attività svolte in relazione ai trattamenti in esame, formazione ricevuta, procedure che ne disciplinano le mansioni, relazioni con altre componenti**
	Dirigente Medico della Direzione Medica dei Presidi Ospedalieri, Sperimentatore Principale, co-sperimentatori, data manager coinvolti nello studio clinico che accedono ai dati per l'elaborazione scientifica. Tutti i soggetti operano nel rispetto delle procedure aziendali di sicurezza informatica e protezione dei dati personali (es. regolamento interno, policy di accesso ai sistemi). Il personale coinvolto ha ricevuto formazione specifica in materia di protezione dei dati personali (Reg. UE 2016/679 – GDPR).
Soggetti Esterni	**Descrizione sintetica (es. caratteristiche del servizio erogato o del titolo che giustifica il coinvolgimento di tale soggetto, presenza di un accordo sul trattamento di dati, relazioni con altre componenti)**
	Engineering per cartella clinica elettronica ambulatoriale Ellipse, Mrdoc per software Ophthal. Essi sono stati nominati responsabili esterni del trattamento ai sensi dell'art.28 GDPR. L'ASST Ovest Milanese e l'Ospedale di Circolo e Fondazione Macchi di Varese - ASST dei Sette Laghi si configurano come Titolari autonomi

Componenti tecnologiche

Componente	Descrizione
Applicazioni	**Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)**
	Cartella clinica elettronica ambulatoriale Ellipse (Engineering), software Ophthal (Mrdoc)
Infrastrutture IT	**Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)**
	OCT Spectralis (Heidelberg Engineering, Heidelberg, Germany) Swept-Source DRI OCT Triton Plus (Topcon Medical Systems Europe, Milan, Italy) iCare Eidon TrueColor Confocal fundus imaging system L'infrastruttura IT aziendale è conforme alla normativa AGID per i data center della Pubblica Amministrazione

Rete	**Descrizione sintetica (es. tipologia di rete, tecnologie utilizzate, relazioni con altre componenti)**
	Come da normativa AGID per i servizi digitali della Pubblica Amministrazione.

Componenti fisiche

Componente	Descrizione
Risorse ed asset materiali	**Descrizione (es. principali caratteristiche, tipologia di asset non latamente inteso come informatico, relazioni con altre componenti)**
	OCT Spectralis (Heidelberg Engineering, Heidelberg, Germany), Swept-Source DRI OCT Triton Plus (Topcon Medical Systems Europe, Milan, Italy), iCare Eidon TrueColor Confocal fundus imaging system presso SCDU Oftalmologia Computer presso Direzione Medica dei Presidi Ospedalieri e presso SCDU Oftalmologia
Sedi fisiche	**Descrizione (es. ubicazione delle sedi anche distaccate o periferiche, principale utilizzo, relazioni con altre componenti)**
	Direzione Medica dei Presidi Ospedalieri, SCDU Oftalmologia dell'AOU "Maggiore della Carità" di Novara. ASST Ovest Milanese

5. Valutazione della proporzionalità in relazione alla finalità

Tenuto conto che l'attività di trattamento sottoposta a valutazione comporta il trattamento delle categorie di dati personali sopra menzionati, in relazione alle categorie di interessati precedentemente citati, il titolare ritiene che dette categorie di dati siano necessarie e proporzionali al perseguimento della finalità:

Ricerca scientifica

6. Diritti e principi fondamentali

Diritti

Accesso	I dati saranno pseudonimizzati e presentati in forma aggregata, pertanto gli Interessati non dovrebbero poter riconoscere i propri dati nei risultati dello studio. Laddove questa possibilità dovesse verificarsi, è possibile esercitare il diritto di accesso dietro richiesta motivata alla Direzione Medica dei Presidi Ospedalieri.

Rettifica	I dati saranno pseudonimizzati e presentati in forma aggregata, pertanto gli Interessati non dovrebbero poter riconoscere i propri dati nei risultati dello studio. Laddove questa possibilità dovesse verificarsi, è possibile esercitare il diritto di rettifica dietro richiesta motivata alla Direzione Medica dei Presidi Ospedalieri.
Cancellazione	I dati saranno pseudonimizzati e presentati in forma aggregata, pertanto gli Interessati non dovrebbero poter riconoscere i propri dati nei risultati dello studio. Laddove questa possibilità dovesse verificarsi, è possibile esercitare il diritto di cancellazione dietro richiesta motivata alla Direzione Medica dei Presidi Ospedalieri.
Opposizione	I dati saranno pseudonimizzati e presentati in forma aggregata, pertanto gli Interessati non dovrebbero poter riconoscere i propri dati nei risultati dello studio. Laddove questa possibilità dovesse verificarsi, è possibile esercitare il diritto di opposizione dietro richiesta motivata alla Direzione Medica dei Presidi Ospedalieri.
Limitazione di trattamento	I dati saranno pseudonimizzati e presentati in forma aggregata, pertanto gli Interessati non dovrebbero poter riconoscere i propri dati nei risultati dello studio. Laddove questa possibilità dovesse verificarsi, è possibile esercitare il diritto di limitazione dietro richiesta motivata alla Direzione Medica dei Presidi Ospedalieri
Revoca del consenso	Il diritto di revoca del consenso si applica esclusivamente alla coorte prospettica, per la quale è raccolto il consenso.

Principi

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell’interessato	I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell’interessato: tali dati sono pseudonimizzati; la Direzione Medica dei Presidi Ospedalieri (DMPO) procede a scaricare i dati dello studio e a creare una chiave per la pseudonimizzazione. Tale chiave viene conservata presso la DMPO, mentre i dati pseudonimizzati sono analizzati dallo Sperimentatore Principale e dai Co-sperimentatori, che non possono pertanto risalire all'identità dei soggetti inclusi nello studio. Sul sito aziendale, all'interno della pagina "DPIA", saranno pubblicate la DPIA e l'informativa studio-specifica. Il personale che ha accesso a questi dati per finalità dello studio, ha seguito corsi di formazione in materia privacy.

I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità	I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità: in particolare, lo studio potrà essere avviato solamente a seguito di approvazione da parte del CEI di Novara, i dati saranno pseudonimizzati e sul sito aziendale, all'interno della pagina "DPIA", saranno pubblicate la DPIA e l'informativa studio-specifica. Tali dati non potranno essere utilizzati per finalità differenti rispetto a quanto dichiarato nel protocollo di studio e, laddove questo fosse necessario, lo sperimentatore principale procederà a presentare nuova istanza al CEI Novara.
I dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati	I dati sono trattati in forma pseudonima e in tale forma verranno conservati per la durata di 7 anni dalla conclusione del progetto
I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali	Le misure messe in atto dall'AOU per garantire un'adeguata sicurezza dei dati personali includono: pseudonimizzazione, minimizzazione dei dati, separazione tra dati clinici e dati identificativi, misure di controllo degli accessi (autenticazione forte e autorizzazioni basate sui ruoli), back-up periodici, protezione da malware, formazione del personale, accordi di riservatezza per il personale coinvolto, presenza di procedure operative standard per la gestione dei dati, degli incidenti e data breach, controllo degli accessi ai locali (chiavi).

7. Valutazione del rischio

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

$R_1 = f(M, p)$

IMPATTO (M)	
LIEVE	1
MEDIO	2
ALTO	3
ALTISSIMO	4

X

PROBABILITÀ (p)

IMPROBABILE	1
POCO PROBABILE	2
PROBABILE	3
ALTAMENTE PROBABILE	4

=

RISCHIO INIZIALE (R)

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

Dove per:

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

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

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

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

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

$$R_2 = R_1 - \left(M_n\right)$$

dove per:

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

All'interno del presente passaggio saranno presenti, in ordine

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

   https://doc.privacymanager.eu/manuale/valutazione_impatto.html#mitigazione-del-rischio-iniziale-somma-dei-valori
4. Rischio residuo (mitigato).

7.1 Misure di sicurezza

Misure di sicurezza trasversali relative ai trattamenti

Misura di sicurezza	Stato di adozione e implementazione

Politiche, regolamenti e manuali	
È stato definito un manuale per la gestione del protocollo informatico	Applicata
Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	Applicata
Formazione relativa alla normativa sulla protezione dei dati	Applicata
Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	Applicata
Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	Applicata
Ruoli e responsabilità	
Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	Applicata
Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	Applicata
I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	Applicata
Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	Applicata
Protezione dei Dati	
Sono in vigore procedure per classificare le categorie di dati	Applicata
Sono in vigore procedure gestire la conservazione dei dati.	Applicata
Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	Applicata
Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	Applicata
Gestione utenze	
È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	Applicata
La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	Applicata

Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	Applicata
I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	Applicata
È mantenuto un inventario delle utenze amministrative.	Applicata
Le utenze amministrative sono formalmente autorizzate.	Applicata
Copie di sicurezza	
Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	Applicata
Misure di sicurezza analogiche	
Contenitori (armadi, schedari, ecc.) muniti di serratura	Applicata
Chiusura a chiave dei locali	Applicata
Sistema di videosorveglianza	Applicata
Cartello per divieto di accesso a soggetti non autorizzati	Applicata
Sistemi di controllo degli accessi	Applicata
Sistemi antincendio	Applicata
Sistema antintrusione	Applicata

Misure di sicurezza trasversali relative agli asset

Misura di sicurezza	Stato di adozione e implementazione
Misure di sicurezza correlate con gli applicativi	
Credenziali	
Sono utilizzati sistemi centralizzati di gestione delle password (Single Sign On)	Applicata
Integrazione con il Domain Controller	Applicata
Cifratura	
Trasferimento dati usando SSL/TLS	Applicata
Chiavi di cifratura personali per ogni utente	Applicata

Cifratura del disco	Applicata
Cifratura della base dati	Applicata
Copie di sicurezza	
Viene effettuata una copia di sicurezza con cadenza settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema	Applicata
I backup sono effettuati con più di un sistema per contrastare malfunzionamenti in fase di ripristino	Applicata
ABSC 5	
1.1 - Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessit	Applicata

Misure di sicurezza specifiche relative al trattamento

Categoria	Misura	Stato di adozione e implementazione
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	Applicata
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	Applicata
	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	Applicata
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	Applicata
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	Applicata

	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	Applicata
	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	Applicata
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	Applicata
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	Applicata
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	Applicata
	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	Applicata
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	Applicata
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	Applicata
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	Applicata

	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	Applicata
	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	Applicata
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	Applicata
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	Applicata
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	Applicata
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	Applicata
	I backup completi devono essere eseguiti regolarmente.	Applicata
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	Applicata
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	Applicata
Misure di sicurezza analogiche	Sorveglianza da parte di personale autorizzato e formato	Applicata
Politiche, regolamenti e manuali	Formazione relativa al processo/applicativo in esame	Applicata

7.2 Valutazione del rischio

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Allagamento	Eventi naturali	Disponibilità	Contesto
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	80%	80%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Incendio	Eventi naturali	Disponibilità	Contesto
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%
	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%

	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%
	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%

	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%
	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%

	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%
	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%

	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%
	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%

	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%
	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%

	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	80%	80%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%
	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%

	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%
	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%

	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	
100%		100%	

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Terremoti, eruzioni vulcaniche	Eventi naturali	Disponibilità	Contesto
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	80%	80%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Malfunzionamento o distruzione di strumentazione it (client)	Hardware e Software	Disponibilità ; Riservatezza ; Integrità	Strumenti
Descrizione			
Hardware e software			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		3	Probabile
Livello di rischio iniziale		9	Molto alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	100%	100%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	80%	80%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Malfunzionamento o distruzione di strumentazione it (server)	Hardware e Software	Disponibilità ; Riservatezza ; Integrità	Strumenti
Descrizione			
Hardware e software			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		3	Probabile
Livello di rischio iniziale		9	Molto alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	100%	100%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	80%	80%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Malfunzionamento o distruzione di strumentazione it (rete)	Hardware e Software	Disponibilità ; Riservatezza ; Integrità	Strumenti
Descrizione			
Hardware e software			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		3	Probabile
Livello di rischio iniziale		9	Molto alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	100%	100%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	80%	80%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Distruzione o furto di strumentazione	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Uso non autorizzato della strumentazione	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano
Descrizione			
Incluso accesso non autorizzato alla rete			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	Categoria	Aree di impatto	Fonti di rischio
Divulgazione accidentale di informazioni	Comportamenti umani	Riservatezza	Umano
Descrizione			
Anche da parte dei dipendenti			
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Infezioni da virus, malware	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		3	Probabile
Livello di rischio iniziale		9	Molto alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Attacchi di ingegneria sociale	Comportamenti umani	Disponibilità ; Riservatezza ; Integrità	Umano
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		2	Medio
Probabilità		4	Altamente probabile
Livello di rischio iniziale		8	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Intercettazione del traffico	Hardware e Software	Riservatezza ; Integrità	Umano ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		3	Probabile
Livello di rischio iniziale		9	Molto alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	100%	100%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	100%	100%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	80%	80%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%
Elemento		**Valore finale numerico**	**Valore finale**
Impatto		1	Lieve
Probabilità		1	Improbabile
Livello di rischio finale		1	Basso
Mitigazione totale d'impatto		**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Accesso illegittimo ai dati	CNIL	Riservatezza	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		2	Poco probabile
Livello di rischio iniziale		6	Alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	80%	80%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Modifiche indesiderate dei dati	CNIL	Integrità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		3	Probabile
Livello di rischio iniziale		9	Molto alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	80%	80%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Minaccia	**Categoria**	**Aree di impatto**	**Fonti di rischio**
Perdita di dati	CNIL	Disponibilità	Umano ; Contesto ; Strumenti
Elemento		**Valore iniziale numerico**	**Valore iniziale**
Impatto		3	Grave
Probabilità		3	Probabile
Livello di rischio iniziale		9	Molto alto
Misure di sicurezza			
Categoria	**Misura**	**Mitigazione Impatto**	**Mitigazione probabilità**
Copie di sicurezza	È in via di definizione un piano di Disaster Recovery al fine di garantire la Continuità Operativa	100%	100%
	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	100%	100%
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione	70%	70%
	La gestione dei privilegi è soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	100%	100%

	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	100%	100%
	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	100%	100%
	È mantenuto un inventario delle utenze amministrative.	80%	80%
	Le utenze amministrative sono formalmente autorizzate.	100%	100%
Misure di sicurezza ENISA	I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	100%	100%

	Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.	100%	100%
	I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale.	100%	100%
	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	100%	100%
	Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	100%	100%

	Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	100%	100%
	Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	100%	100%
	Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali.	100%	100%
	Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale).	100%	100%

	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	100%	100%
	Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale.	100%	100%
	L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	100%	100%
	Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi.	100%	100%
	Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza.	100%	100%

	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	100%	100%
	Le workstation 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 l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati.	100%	100%
	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	100%	100%
	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	100%	100%
	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	100%	100%

	I backup completi devono essere eseguiti regolarmente.	100%	100%
	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.	100%	100%
	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	100%	100%
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	80%	80%
	Chiusura a chiave dei locali	80%	80%
	Sistema di videosorveglianza	80%	80%
	Cartello per divieto di accesso a soggetti non autorizzati	70%	70%
	Sistemi di controllo degli accessi	100%	100%
	Sistemi antincendio	100%	100%
	Sistema antintrusione	100%	100%
	Sorveglianza da parte di personale autorizzato e formato	100%	100%
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	100%	100%

	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	100%	100%
	Formazione relativa al processo/applicativo in esame	100%	100%
	Formazione relativa alla normativa sulla protezione dei dati	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	100%	100%
	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	100%	100%
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati	100%	100%
	Sono in vigore procedure gestire la conservazione dei dati.	100%	100%
	Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali	100%	100%

	Le procedure per la notificazione di gli incidenti di sicurezza e le violazioni dei dati personali fanno uso di strumenti automatizzati che riducono i tempi necessari ad individuare categorie di dati coinvolti, misure di sicurezza applicate.	100%	100%
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	100%	100%
	Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati	100%	100%
	I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza.	100%	100%
	Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo	100%	100%

Elemento	**Valore finale numerico**	**Valore finale**
Impatto	1	Lieve
Probabilità	1	Improbabile
Livello di rischio finale	1	Basso
Mitigazione totale d'impatto	**Mitigazione totale di probabilità**	

100%	100%

Riassunto ed esito dell'analisi del rischio

Minaccia	Rischio iniziale	Rischio residuo
Allagamento	6	1
Incendio	6	1
Terremoti, eruzioni vulcaniche	6	1
Malfunzionamento o distruzione di strumentazione it (client)	9	1
Malfunzionamento o distruzione di strumentazione it (server)	9	1
Malfunzionamento o distruzione di strumentazione it (rete)	9	1
Distruzione o furto di strumentazione	6	1
Uso non autorizzato della strumentazione	6	1
Divulgazione accidentale di informazioni	6	1
Infezioni da virus, malware	9	1
Attacchi di ingegneria sociale	8	1
Intercettazione del traffico	9	1
Accesso illegittimo ai dati	6	1
Modifiche indesiderate dei dati	9	1
Perdita di dati	9	1

Livello di rischio complessivo per area

Area di impatto	Livello di rischio

Disponibilità	Basso
Riservatezza	Basso
Integrità	Basso

Livello di rischio complessivo iniziale

Molto Alto

Livello di rischio complessivo residuo

Basso

8. Coinvolgimento delle parti interessate

Domanda	**Risposta**
Sono state raccolte le opinioni degli interessati o dei loro rappresentanti?	Sì
Le opinioni degli interessati o dei loro rappresentanti sono state raccolte per la coorte prospettica. Per la coorte retrospettiva, non è stato possibile raccogliere le opinioni degli interessati o dei loro rappresentanti per motivi di impossibilità organizzativa, connessi all'elevato numero complessivo dei soggetti da arruolare nello studio, e per la circostanza per cui la mancata raccolta dei dati relativi al numero di interessati non contattabili, in rapporto al numero complessivo dei soggetti che si intende arruolare nella ricerca, determinerebbe conseguenze significative sulla qualità e sull'affidabilità dei risultati della ricerca stessa.	
È stato coinvolto il Responsabile della Protezoione dei Dati?	Sì
Il DPO aziendale è stato coinvolto nella redazione del presente documento	

9. Note

Il Titolare del trattamento

AOU Maggiore della Carità di Novara