POLITICA INTEGRATA

DEI SISTEMI DI GESTIONE

SDP-ITA-PO 01-Politica integrata dei Sistemi di Gestione (ex MQI_5.2.A1)

Rev. 8 del 08/02/2025

Dedalus Italia S.p.A. con Socio Unico Dedalus Finance GmbH

Sede Legale:
Via di Collodi 6/c
50141 Firenze

Tel. +39 055 42471
Fax +39 055 451660
reception@dedalus.eu

Capitale sociale:
€ 11.634.062 i.v.
R.E.A. Firenze 591564

Codice fiscale, partita IVA
e registro imprese
05994810488

IMPORTANTE: L'unica versione ufficiale di questo documento e degli altri documenti del Sistema Qualità Integrato di Dedalus compresa la modulistica prevista si trova nell'archivio "Sistema Qualità Integrato" dello SharePoint aziendale in Office 365 che è sempre accessibile dal link https://dedalusspa.sharepoint.com/sites/quality, al quale bisogna sempre fare riferimento per consultare il documento e scaricare la modulistica.

Ogni altra fonte non è ufficiale e quindi non è attendibile.

Indice

1 GENERALITÀ SULLA POLITICA INTEGRATA

1.1 Obiettivo di Dedalus

L'obiettivo di Dedalus è di consolidare il proprio ruolo di player primario nel mercato globale degli Health Care Systems.

1.2 Contenuti e parti costituenti della Politica Integrata dei Sistemi di Gestione di Dedalus

A tale scopo l'Alta Direzione di Dedalus ha definito la **Politica Integrata dei Sistemi di Gestione – Integrated Management System Policy**, dell'organizzazione, che **contiene gli elementi ritenuti strategici** e quindi fondamentali **relativamente ai** seguenti sistemi di gestione:

1. Sistema di Gestione per la Qualità-Quality Management System (**SGQ-QMS**), per la conformità alla norma **ISO 9001**
2. Sistema di Gestione del Servizio-Service Management System (**SGS-SMS**), per la conformità alla norma **ISO/IEC 20.000-1**
3. Sistema di Gestione della Sicurezza delle Informazioni-Information Security Management System (**SGSI-ISMS**), per la conformità alla norma **ISO/IEC 27001** e alle relative estensioni ai servizi cloud e SaaS ISO/IEC **27017** e ISO/IEC **27018**, definita all'interno del documento SDP-ITA-PO 03-Information Security and Data Privacy General Policy
4. Sistema di Gestione Ambientale-Environmental Management System (**SGA_EMS**), per la conformità alla norma **ISO 14001**
5. Sistema di Gestione della Qualità dei Dispositivi Medici-Medical Device Quality Management System (**SGDM**), per la conformità alla norma **ISO 13485**
6. Sistema di Gestione della Responsabilità Sociale-Social Responsibility Management System (**SGRS-SRMS**), per la conformità allo standard **SA 8000**
7. Sistema di gestione della Parità di Genere-Gender equality Management System (**SGPG-GEMS**), per la conformità alla prassi **UNI PRD 125**
8. Sistema di Gestione della Continuità Operativa – Business Continuity Management System (BCMS), per conformità allo standard **ISO 22301**.

Inoltre, con riferimento al Sistema di Gestione per la prevenzione della corruzione, per la conformità alla norma **ISO 37001**, è stata adottata la Policy Anticorruzione del Gruppo Dedalus, approvata in data 22 dicembre 2022 dal Consiglio di Amministrazione di Dedalus S.p.A., cui si rimanda.

1.3 Caratteristiche della Politica Integrata dei Sistemi di Gestione

L'Alta Direzione assicura che tale politica:

- è **appropriata alle finalità e al contesto** dell'organizzazione e supporta i suoi obiettivi strategici;
- costituisce un **quadro di riferimento per** fissare gli **obiettivi** di tutti i sistemi di gestione applicabili, che sono sviluppati in coerenza con i principi generali e specifici e alle azioni indicate in questo documento;
- comprende un **impegno a soddisfare i requisiti applicabili** di tutti i sistemi di gestione, inclusi quelli cogenti e contrattuali, e a **migliorare** in modo continuo i **sistemi di gestione e** la loro **efficacia**;
- comprende l'**impegno** dell'organizzazione a rispettare i documenti internazionali come elencati nella sezione II della SA8000 sugli **Elementi Normativi** e loro Interpretazione;
- comprende l'impegno ad essere **conforme con le leggi nazionali**, le altre leggi applicabili e gli altri requisiti sottoscritti;
- comprende l'**impegno alla parità di genere**;
- è **disponibile** come informazione documentata;
- è **comunicata, compresa e applicata** all'interno dell'organizzazione;
- è resa **disponibile** alle parti interessate rilevanti;
- è **riesaminata** periodicamente per accertarne la continua idoneità.

2 POLITICA PER LA GESTIONE DELLA QUALITÀ GENERALE, DEL SERVIZIO E DEI DISPOSITIVI MEDICI

2.1 Standard applicabili alla sezione

Questa sezione della politica integrata dei sistemi di gestione è riferita in particolare ai requisiti delle norme **ISO 9001, ISO/IEC 20000-1** ed **ISO 13485**.

2.2 Principi applicabili

L'Alta Direzione di Dedalus, convinta dei miglioramenti interni e verso i clienti conseguenti all'adozione di un sistema qualità integrato ha definito la propria politica della qualità, basata sui seguenti **principi**:

- garantire e migliorare costantemente la **soddisfazione dei clienti**, soddisfacendone le attese ed ottemperando ai **requisiti del prodotto e del servizio** allo scopo di divenire per loro un partner sempre più importante;
- garantire che **i clienti ricevano valore reale attraverso** l'erogazione dei propri **servizi** mediante la definizione ed il rispetto delle SLA;
- sviluppare il **miglioramento continuo della qualità dei prodotti, del servizio, dell'efficacia** del sistema qualità;
- **rispondere prontamente al**l'evolvere del **mercato** mediante una organizzazione flessibile e competitiva;
- raggiungere e mantenere la **conformità dei** propri **dispositivi medici ai requisiti regolatori** dei paesi in cui vengono immessi in commercio;
- **coinvolgere** nei propri processi tutto **il personale**, consentendogli di **crescere** professionalmente e di sentirsi parte attiva del sistema qualità.

2.3 Azioni sviluppate

L'attuazione di questa politica ha comportato l'attivazione delle seguenti **azioni**:

- definire e precisare le **responsabilità, i ruoli, i compiti** per le diverse fasi dei processi;
- mettere a punto le **regole interne** assunte come standard di riferimento organizzativo, procedurale ed operativo nella gestione delle attività;
- **prevenire** il verificarsi di **non conformità** durante lo svolgimento dei processi;
- identificare e registrare le non conformità, promuovendo l'attivazione di idonee **azioni correttive** e il consolidamento delle soluzioni adottate;
- promuovere lo **sviluppo delle competenze delle risorse** professionali, favorendo l'integrazione e la collaborazione tra le aree organizzative interne ed attivando azioni di formazione permanente;
- **valorizzare il know-how posseduto**, attivando la diffusione delle buone prassi e perseguendone l'ottimizzazione per rendere patrimonio comune, i metodi di lavoro ed le esperienze acquisite;
- assicurare la promozione della **focalizzazione sul cliente** nell'ambito dell'intera organizzazione, oltre che l'integrità del sistema di gestione stesso.

L'Alta Direzione di Dedalus ha stabilito appropriati processi di **comunicazione interna** quali ad esempio tramite il sito aziendale, e-mail, newsletter, video conferenze, riunioni/incontri fisici e virtuali tra gruppi di lavoro, strumenti e tool

per la condivisione delle informazioni nel massimo rispetto della sicurezza delle informazioni delle stesse.

Per la **comunicazione esterna** sono utilizzati sostanzialmente i seguenti strumenti: advertising, produzione di brochure e documentazione informativa sull'organizzazione, siti internet, organizzazione di eventi, attività di ufficio stampa, partecipazione ad eventi, portali di condivisione delle conoscenze, aree aziendali specificamente dedicate alla sperimentazione e al coinvolgimento del cliente e degli stakeholder nei processi di sviluppo delle conoscenze.

3 POLITICA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI ESTESA AL CLOUD COMPUTING

La politica per la sicurezza delle informazioni è definita nel documento SDP-ITA-PO 03-Information Security and Data Privacy General Policy, che è allegato alla presente, ma che ha un suo ciclo approvativo distinto. (ALLEGATO E PARTE INTEGRATE DI QUESTO DOCUMENTO)

4 POLITICA AMBIENTALE

4.1 Standard applicabili alla sezione

La parte del Sistema di Gestione per la Qualità che riguarda la Gestione Ambientale è il SGA (Sistema di Gestione Ambientale); la norma di riferimento per tale sistema è l'**ISO 14001**.

4.2 Principi applicabili

Gli impatti sull'ambiente delle attività lavorative di DEDALUS sono limitati; tuttavia, la Direzione aziendale ritiene molto importante che le **attività dell'organizzazione** siano svolte con attenzione alla salvaguardia e al **rispetto dell'ambiente,** alla **prevenzione dell'inquinamento**, alla **riduzione** degli impiatti ambientali dovuti ai **consumi di energia e** alla **carbon footprint** derivanti dalle attività e con l'impegno alla **progettazione green** delle infrastrutture ICT. A tale scopo, il Sistema di Gestione Integrato è stato sviluppato anche per garantire il miglioramento continuo dell'impatto sull'ambiente che possono avere le attività dell'organizzazione, in conformità ai requisiti della norma ISO 14001.

Gli **obiettivi** generali del SGA sono:

- assicurare la conformità e il continuo **rispetto delle prescrizioni legislative applicabili** e di quelle contrattuali che abbiano impatto **sull'ambiente**;
- **migliorare costantemente i processi dell'organizzazione** in relazione al loro impatto sull'ambiente, al consumo di energia correlato, alla riduzione della carbon footprint, all'impegno alla progettazione green delle infrastrutture e alla prevenzione e minimizzazione continua dell'inquinamento.

Tali obiettivi generali sono poi dettagliati di anno in anno attraverso obiettivi specifici, che possono comprendere ad esempio i seguenti elementi: ridurre gli impatti correlati agli spostamenti per attività aziendali, aumentare la sostenibilità ambientale negli uffici e incentivare gli acquisti sostenibili, il riutilizzo e il riciclo, e infine promuovere la riduzione della quantità di email inviate.

4.3 Azioni sviluppate

Tali obiettivi vengono resi concreti attraverso la **pianificazione delle attività di miglioramento dell'impatto ambientale** e con la definizione di **traguardi ambientali** il cui raggiungimento viene periodicamente verificato.

Il sviluppato SGA è sviluppato per l'organizzazione dove può avere il massimo impatto, ma per quanto possibile intende promuovere comportamenti coerenti e ambientalmente consapevoli **anche di fornitori, clienti e degli stakeholders** in generale.

5 POLITICA RESPONSABILITÀ SOCIALE

5.1 Standard applicabili alla sezione

La parte del Sistema di Gestione per la Qualità che riguarda la Responsabilità sociale è il SGRS (Sistema di Gestione della Responsabilità Sociale); lo standard di riferimento per tale sistema è la **SA8000**.

5.2 Principi applicabili

La Direzione aziendale conferisce a tutte le aree il mandato di migliorare in modo continuativo e sistematico le prestazioni di salute e sicurezza, la riduzione dei rischi e la difesa dei diritti umani e del lavoro. La Direzione si impegna a non fornire o realizzare prodotti/servizi, se le attività lavorative non potranno essere svolte in piena sicurezza per il personale e per l'ambiente e per i diritti e la dignità delle persone. La Direzione, inoltre, punta ad accrescere le potenzialità aziendali in termini di occupazione e crescita.

In particolare, i principi applicabili sono i seguenti:

- Promozione del coinvolgimento e partecipazione consapevole del Personale dell'organizzazione a tutti i livelli nell'attuazione del Sistema di Gestione Integrato, coinvolgendo anche i terzisti che operano stabilmente con l'organizzazione;
- Impegno al costante aggiornamento e rispetto della legislazione in vigore e di tutte le altre prescrizioni sottoscritte dall'organizzazione compresi lo standard SA8000 e le norme e leggi da esso richiamate;
- Attenzione alle risorse e consapevolezza dell'importanza del loro ruolo nella dinamica aziendale, che attribuisce un ruolo di preminenza alla formazione ed allo sviluppo di tutto il personale;
- Continua e costante ricerca che muove e proietta l'organico aziendale verso soluzioni e tecnologie all'avanguardia nel rispetto della salute e sicurezza e a basso impatto ambientale;
- Continua partecipazione congiunta dei lavoratori e del management nella tutela dei diritti umani per identificare e correggere le non conformità e assicurare il mantenimento della conformità;
- Impegno costante ad adeguarsi a tutti i requisiti dello standard per la Responsabilità Sociale ed al rispetto degli strumenti internazionali opportuni (ILO-ONU ecc.);
- Impegno a non impiegare, nel proprio organico, personale che possa rientrare all'interno della definizione di "bambino" o di "giovane lavoratore" e/o il divieto a sostenere altre realtà che utilizzino o favoriscano il lavoro infantile;
- Promozione del dialogo e del confronto con tutti i portatori d'interesse interni ed esterni (autorità pubbliche, cittadini, associazioni, ecc.), tenendo conto delle loro istanze, esigenze ed aspettative attivando adeguati strumenti di partecipazione e comunicazione in modo trasparente le prestazioni delle attività aziendali.

A tale scopo, il Sistema di Gestione Integrato è stato sviluppato anche per garantire il miglioramento continuo di processi e attività del sistema di responsabilità sociale, in conformità ai requisiti dello standard SA8000.

Gli **obiettivi** generali del SGRS sono:

- assicurare la conformità e il continuo **rispetto delle prescrizioni legislative applicabili** e di quelle contrattuali che abbiano impatto **sulla responsabilità sociale**;

- **migliorare costantemente i processi dell'organizzazione** in relazione al loro impatto sulla responsabilità sociale.

Tali obiettivi generali sono poi dettagliati di anno in anno attraverso obiettivi specifici, che possono comprendere ad esempio i seguenti elementi: migliorare la parità di genere, favorire la formazione interna delle persone, migliorare l'impegno sociale dell'organizzazione, diffondere i principi di responsabilità sociale lungo la propria catena di fornitura.

5.3 Azioni sviluppate

Tali obiettivi vengono resi concreti attraverso la **pianificazione delle attività di miglioramento del sistema di responsabilità** il cui raggiungimento viene periodicamente verificato.

6. POLITICHE GENERALI E SPECIFICHE PER LA PARITÀ DI GENERE

6.1 Standard applicabili alla sezione

La parte del Sistema di Gestione Integrato che riguarda la Parità di Genere è il SGPG (Sistema di Gestione per la Parità di Genere); lo standard di riferimento per tale sistema è la prassi **UNI/PDR 125**.

6.2 Politica generale della parità di genere

La Direzione di Dedalus, **in coordinamento con il Comitato Guida per la Parità di Genere** e in linea con il valore del DNA del Gruppo Dedalus, ha stabilito questa politica generale della parità di genere.

La **figura responsabile del coordinamento** della realizzazione di questa politica per la parità di genere è il Direttore delle Risorse umane per Dedalus Italia, in allineamento con la strategia D&I di gruppo.

Tale politica prevede che:

- In Dedalus **l'innovazione inizia con l'inclusione**. Come azienda, siamo guidati dai **nostri valori fondamentali**; sappiamo che la diversità e l'inclusione sono **fattori chiave per il nostro successo e la nostra crescita**.
- La nostra presenza internazionale unisce persone da tutto il mondo e per questo ci impegniamo a **valorizzare background**, **competenze ed**

esperienze diverse e a creare un ambiente che rispecchi le **numerose comunità che raggiungiamo**.

- "Perseguire la diversità e l'inclusione" è uno dei nostri valori fondamentali e una componente del nostro DNA Dedalus, che ci spinge a costruire un **ambiente rispettoso, diversificato e inclusivo**, riconoscendo **l'unicità dei bisogni, delle prospettive e del potenziale** di tutti i membri della nostra comunità. Dedalus è orgogliosa di promuovere la diversità, l'inclusione, l'equità e l'uguaglianza, e si impegna a creare **una cultura sicura e inclusiva in cui si valorizzi la diversità in tutte le sue forme** e **si incoraggi ognuno** a dare il meglio di sé.
- Dedalus valorizza le diversità presenti nei ruoli che operano nell'organizzazione e mantiene processi in grado di sviluppare l'empowerment di tutto il personale, compreso quello delle persone del sesso numericamente meno rappresentato, nelle attività di business.

I principi cardine sono i seguenti:

- Ognuno di noi guida con rispetto, attraverso l'esempio e ponendosi come modello, i colleghi, i manager, i leader, i fornitori, i clienti e altri soggetti.
- Accogliendo le differenze, eliminando i pregiudizi e contrastando i comportamenti negativi, possiamo fare parte di una cultura in cui tutti noi proviamo un senso di appartenenza.
- Attraverso la diversità dei nostri background, delle nostre esperienze, opinioni o convinzioni, è in questo modo che, insieme, costruiamo un'azienda sostenibile.

Dedalus, nel promuovere e assicurare il raggiungimento e il mantenimento di tale scopo, focalizza i propri sforzi nelle seguenti 6 aree di azione, definite dalla prassi UNI/PDR 125:

1. Cultura e strategia
2. Governance
3. Processi Human Resources
4. Opportunità
5. Equità remunerativa
6. Genitorialità

Dedalus intende assicurare la parità di genere attraverso azioni concrete che, oltre a risultare conformi ai requisiti/KPI stabiliti nelle singole aree indicate, risultino di

reale e concreto apprezzamento da parte delle donne presenti in organizzazione, che sono le reali parti interessate.

L'organizzazione, con la volontà di riporre attenzione a tale soddisfazione in qualunque momento e in qualunque circostanza della vita lavorativa della donna nell'organizzazione, ha scelto di guardare a tale "ciclo di vita" attraverso i seguenti aspetti:

- Selezione ed assunzione (recruitment)
- Gestione della carriera
- Equità salariale
- Genitorialità, cura
- Conciliazione dei tempi vita-lavoro (work-life balance)
- Prevenzione abusi e molestie

Per ciascuno dei seguenti aspetti, Dedalus Italia ha stabilito delle politiche più specifiche che sono riportate di seguito. A ciascuna politica che esprime i principi a cui Dedalus Italia si ispira, l'organizzazione ha associato degli obiettivi di parità, specifici e misurabili indicati nel piano strategico.

6.3 Politiche specifiche per la parità di genere

Dedalus Italia, in relazione all'analisi dei propri processi di business, ha compreso e stabilito i principi da rispettare in riferimento a ciascuno dei seguenti punti.
Tali principi costituiscono i criteri ispiratori dei processi volti ad affrontare:

- I gap esistenti in riferimento agli indicatori stabiliti dalla prassi UNI/PDR 125
- le esigenze delle donne presenti in organizzazione, viste come le parti principali interessate ai concreti risultati del modello organizzativo

6.3.1 Politica per la selezione ed assunzione (recruitment)

Dedalus Italia, nel processo di selezione ed assunzione del personale da impiegare nelle attività di business rispetta, nella prospettiva del miglioramento, i seguenti principi:

- La selezione della persona candidata deve essere esercitata in maniera neutrale rispetto al genere
- I criteri di selezione devono prendere in considerazione i requisiti rivolti alle qualità personali come la professionalità, la competenza, la specializzazione, l'esperienza
- La selezione non deve prevedere questioni relative a matrimonio, gravidanza e responsabilità familiari
- La selezione deve considerare che la presenza delle donne e degli uomini nell'organico deve essere bilanciata rispetto al totale delle persone presenti
- I ruoli di riporto al vertice e con delega al budget devono essere distribuiti in maniera equilibrata tra i generi

- La posizione lavorativa, prevista in fase di assunzione, deve prevedere una retribuzione riferita alle mansioni e alle responsabilità e non influenzata dal genere
- La selezione deve considerare che le percentuali di donne e uomini il cui contratto prevede una remunerazione variabile siano bilanciate

6.3.2 Politica per la gestione della carriera

Dedalus è consapevole che i risultati economici raggiunti dipendono anche dalle persone che vi lavorano e tutte le occasioni di sviluppo di tale carriera intende riferirle ai soli risultati e al solo merito della persona a prescindere dal genere. Dedalus, nella prospettiva del miglioramento, gestisce le carriere del personale interno rispettando i seguenti principi:

- L'attribuzione di ruoli e mansioni deve considerare un bilanciamento di leadership di genere
- La progettazione dei percorsi di carriera e la loro presentazione devono essere rivolte a tutti i generi
- I percorsi di carriera del personale sono accessibili a tutte le persone che possono appurare, in maniera trasparente, il mantenimento degli equilibri riferiti alla parità di genere
- L'ambiente lavorativo nel quale si trascorre la gran parte della giornata deve assicurare la possibilità (tecnologica e fisica) a tutte le persone di esprimersi ed il benessere visto come sicurezza e comfort
- La formazione per lo sviluppo delle competenze e della consapevolezza rappresenta un processo fondamentale inteso a rimuovere eventuali difficoltà di carriera e a ripristinare eventuali equilibri di leadership nel genere
- Le fasi di distacco del personale dall'organizzazione in caso di licenziamento sono strettamente esaminate verificando il turnover in base al genere
- Le promozioni tengono sempre conto del bilanciamento del genere in riferimento al livello funzionale
- Il garantire che i generi siano equamente rappresentati tra i relatori del panel di tavole rotonde, eventi, convegni o altro evento anche di carattere scientifico

6.3.3 Politica per l'equità salariale

Dedalus, in fase di assunzione e durante tutta la carriera del personale intende assicurare l'equità salariale a prescindere dal genere. L'organizzazione non considera asimmetricamente i costi da sostenere per remunerare le persone di genere diverso. Nel provvedere alla determinazione, alla corresponsione e alle modifiche della retribuzione, l'organizzazione rispetta i seguenti principi:

- La retribuzione delle persone è riconosciuta in relazione al ruolo e alle responsabilità e, eventuali aggiunte a titolo di benefit e di premio a tale retribuzione, si intendono esclusivamente basate sui risultati prodotti e riconosciuti

- La retribuzione, la corresponsione di premi e l'assegnazione di benefit, per trasparenza, sono documentate e accessibili all'intero personale
- I criteri di retribuzione, premi e benefit sono documentati e accessibili all'intero personale
- A chiunque del personale è riconosciuto il diritto di segnalare eventuali disparità

6.3.4 Politica per la genitorialità e la cura

Dedalus intende non costituire alcun ostacolo alla genitorialità, supportando la maternità e la paternità attraverso attività intese a soddisfare le esigenze di chi, in ragione del proprio stato connesso alla genitorialità, deve bilanciare il proprio impegno tra il lavoro e le nuove occorrenze emerse. L'organizzazione sostiene tale intenzione alla luce dei seguenti principi:

- La maternità e la paternità sono sostenute da programmi di formazione, informazione e re-inserimento
- La maternità è assistita prima, durante e dopo la nascita
- Il congedo di paternità deve essere promosso affinché ne usufruiscano tutti i potenziali beneficiari per l'intero periodo previsto dalla legge
- I rientri dal congedo sono supportati da specifiche iniziative di ri-orientamento
- Dedalus assume un ruolo attivo nel supportare, con iniziative concrete le attività di caregiver (prendersi cura del nascituro/a)

6.3.5 Politica per la conciliazione dei tempi vita-lavoro (work-life balance)

Dedalus intende poter fornire al proprio personale la possibilità di gestire il tempo da dedicare alla vita e al lavoro attraverso un bilanciamento di equilibri che tenga conto sia degli obiettivi aziendali, sia del benessere psicofisico del lavoratore derivante da una maggiore libertà di autodeterminazione. I principi alla base della conciliazione dei tempi di vita-lavoro sono i seguenti:

- Le misure work life balance sono rivolte a tutto il personale a prescindere dal genere
- Dedalus adotta il part time per i ruoli ove questo è possibile, la flessibilità degli orari e lo smart working
- Dedalus permette il collegamento telematico con tutto il personale che lavora dall'esterno (a prescindere dal contratto), per operazioni di lavoro e la partecipazione alle riunioni

6.3.6 Politica per la prevenzione abusi e molestie

Dedalus ripudia ogni forma di abuso e di molestia, per tale proposito esercita un'attività di prevenzione e repressione del fenomeno a **tolleranza zero**. Dedalus attua la sua prevenzione attraverso azioni concrete i cui principi prevedono:

- Che i rischi relativi ad abusi e molestie siano individuati
- Che Dedalus pianifichi in relazione a tale rischio delle azioni di prevenzione

- La possibilità di segnalare sospetti e/o fatti inerenti ad abusi e molestie attraverso il processo corporate di whistle blowing
- L'assoluta tutela, da parte di Dedalus delle persone segnalanti, da successive eventuali ritorsioni
- Che Dedalus analizzi e comprenda eventuali episodi di abusi e molestie
- Lo sviluppo di una comunicazione gentile e neutrale rispetto al genere

6.4 Azioni sviluppate

Tali obiettivi vengono resi concreti attraverso la **pianificazione delle attività di miglioramento del sistema gestione della parità di genere** il cui raggiungimento ed aggiornamento viene periodicamente verificato.

7 BUSINESS CONTINUITY POLICY

7.1 Standard applicabili alla sezione

La parte dell'Integrated Management System che riguarda la Continuità Operativa è il Business Continuity Management System; lo standard di riferimento per tale sistema è l'**ISO 22301**.

7.2 Principi applicabili

in linea con la Norma di riferimento ISO22301 (nella sua ultima versione), la Direzione aziendale è attivamente coinvolta ed impegnata a promuovere all'interno di Dedalus Italia le azioni e le attività di pianificazione, implementazione, verifica, mantenimento e miglioramento del Business Continuity Management System (BCMS) come componente dell'Integrated Management System.

Il BCMS di Dedalus ha l'obiettivo di facilitare il raggiungimento degli obiettivi di business, a fronte di eventi interruttivi che potrebbero compromettere l'erogazione dei prodotti e servizi offerti.

La Direzione aziendale ritiene infatti che la continuità operativa dei processi aziendali sia fondamentale per garantire il rispetto di tutti gli impegni presi dall'organizzazione nei confronti di clienti e stakeholders e, in generale, per garantire la sopravvivenza dell'organizzazione stessa in caso di disastri o altri eventi straordinari che possano metterne a rischio la normale operatività.

La Direzione aziendale si impegna a soddisfare tutti i requisiti di continuità operativa applicabili attraverso l'implementazione ed il miglioramento continuo del Business Continuity Management System.

Gli **obiettivi** generali del BCMS sono:

- garantire il **rispetto degli impegni di continuità dei servizi erogati, inclusi i servizi erogati in SaaS**, presi dall'organizzazione nei confronti di clienti e stakeholders;
- prevenire, per quanto possibile, situazioni "critiche" per la **continuità del business**;
- mitigare gli **impatti negativi** sul business, a seguito del possibile verificarsi di situazioni "critiche" per la continuità operativa;
- garantire la **sopravvivenza dell'organizzazione stessa in caso di disastri o altri eventi straordinari** che possano mettere a rischio la normale operatività dell'organizzazione;
- accrescere la **fiducia di clienti e stakeholders** nei confronti di Dedalus Italia e dei servizi erogati.

Tali obiettivi generali sono poi dettagliati di anno in anno attraverso obiettivi specifici.

7.3 Azioni sviluppate

Tali obiettivi vengono resi concreti attraverso le attività previste dal BCMS ed in particolare attraverso:

- lo sviluppo periodico di **Business Impact Analysis (BIA)** per l'individuazione dei servizi e processi critici, inclusi i servizi in SaaS;
- l'esecuzione di **Analisi di Rischio**, per la valutazione degli scenari di indisponibilità derivanti dagli eventi che costituiscono il panorama di rischi aziendali;
- lo sviluppo di **Piani di Continuità Operativa**, anche relativi ai servizi SaaS;
- il **test** programmato di tali Piani di Continuità Operativa e l'adozione di adeguate **contromisure e miglioramenti** per gli eventuali aspetti da ottimizzare;
- l'esecuzione di **campagne di formazione** volte a sensibilizzare la popolazione aziendale e a diffondere la **conoscenza** in merito alla tematica della Business Continuity.

8 I PRINCIPI GENERALI A CUI CI ISPIRIAMO

Siamo convinti che per ottenere reale qualità a 360 gradi, ognuno di noi debba adottare quotidianamente i seguenti principi:

- bisogna **agire con determinazione**, perché la qualità e la soddisfazione del cliente si ottengono solo attraverso azioni concrete, con un costante impegno e un profondo senso di responsabilità da parte di ognuno di noi;
- bisogna **fare bene le cose fin dalla prima volta**, con l'obiettivo di rispettare i requisiti di prodotto e di servizio, inclusi quelli cogenti applicabili;
- bisogna essere **tempestivi nel rispondere** agli eventuali incidenti e reagire con la **volontà di eliminare i problemi sottostanti**;
- bisogna agire attuando una **attenta e continua prevenzione**, così come facciamo quando sono in gioco i nostri interessi personali;
- bisogna **pensare a tutti i riflessi** che le **nostre azioni** o le nostre decisioni hanno sulla struttura aziendale, preoccupandoci così di attuare una tempestiva e completa **comunicazione a tutti i soggetti interessati** il cui intervento seguirà al nostro nel processo organizzativo e/o produttivo che si sta espletando;
- bisogna **considerare "Clienti" tutti coloro che ricevono i nostri servizi e/o i nostri prodotti**; sono quindi Clienti gli utilizzatori finali, ma anche i nostri colleghi, gli altri reparti dell'organizzazione e i collaboratori esterni, quando l'organizzazione del lavoro preveda che da parte nostra debba essere consegnato a loro un prodotto od erogato un servizio propedeutico al conseguimento del risultato finale, garantendo anche in tal caso conformità alle specifiche pattuite con il "Cliente" stesso; siamo infatti consapevoli che sarà molto **improbabile conseguire la Qualità del Servizio alla fine del processo** produttivo **se non** si sono **attuate in Qualità una o più delle fasi intermedie**;
- bisogna avere la consapevolezza che la **scarsa aderenza alle specifiche di Servizio originano un costo elevato** per l'organizzazione, in termini di necessità di cambiamento dei prodotti o di **ri-erogazione dei servizi** e in termini di **perdita di immagine** verso il mercato.

Riteniamo poi che il **vantaggio competitivo** sia sempre più **generato dal capitale intellettuale** (ricercato attraverso il continuo confronto e il coinvolgimento dei nostri dipendenti in processi interni e nella generazione di soluzioni) **e dall'organizzazione** aziendale. Crediamo che le menti più interessanti siano quelle che sanno liberare la fantasia, porsi domande inedite, affrontare le sfide e tracciare la strada per chi segue

Crediamo che un'organizzazione aziendale di successo debba essere basata sulla **passione** delle proprie persone e imperniata su di un'efficace e continuativa comunicazione interna, sull'**orientamento alla soluzione dei problemi**,

sull'obiettivo di originare la **soddisfazione** dei propri stakeholders e **del Cliente** in particolare: a favore di quest'ultimo, insomma, vogliamo essere un partner a tutto campo e non un semplice fornitore.

L'ALTA DIREZIONE di DEDALUS ITALIA SPA

SDP-ITA-PO 03-Politica generale sulla sicurezza delle informazioni e sulla privacy dei dati

Rev. 2 del 08/02/2025

Le modifiche rispetto alla precedente versione pubblicata sono identificate con una riga a margine come per queste righe di esempio e documentate nella cronologia delle revisioni. Le versioni maggiori non riportano le revisioni tracciate esplicitamente per garantire la leggibilità del documento.

SOMMARIO

1 AMBITO DI APPLICAZIONE

La presente politica si applica a Dedalus Italia e a tutte le società del gruppo Dedalus indicate nel documento di governance QARA-ITA-GR-Legal entities che hanno adottato il IMS di Dedalus Italia (indipendentemente dai siti, dalle strutture e dalle operazioni); in questo documento tali società sono indicate collettivamente come "Dedalus".

Questa politica si applica anche a tutto il personale, ai fornitori, agli appaltatori e ai consulenti (indipendentemente dalla natura o dalla durata del loro lavoro o dalla loro posizione geografica), a tutte le soluzioni, i prodotti e i servizi (indipendentemente dalla forma, dalla tecnologia utilizzata, dalla posizione fisica (on prem, cloud privato o pubblico) o dalla fase del ciclo di vita della soluzione, del prodotto o del servizio in questione).

L'Information Security Management System (ISMS) è incorporato nell'Integrated Management System (IMS) di Dedalus Italia.

2 SCOPO

Dedalus si impegna a supportare gli operatori sanitari nella protezione dei dati personali e in particolare dei dati sanitari dei loro pazienti, fornendo prodotti e servizi sicuri.

Questa politica esprime la visione del management di Dedalus sulla sicurezza delle informazioni e sulla privacy dei dati (IS&DP). In generale, ciò comprende la protezione dei sistemi informatici, la sensibilizzazione degli utenti in materia di sicurezza e privacy, la gestione dei fornitori e altri ambiti di sicurezza delle informazioni.

Questo documento si concentra sui domini di sicurezza delle informazioni corrispondenti alle clausole ISO/IEC 27001:2022 e alle relative linee guida ISO/IEC 27017:2017 e ISO/IEC 27018:2019 per il cloud:

- A.5 Controlli organizzativi
- A.6 Controlli sulle persone
- A.7 Controlli fisici
- A.8 Controlli tecnologici

3 POLITICA

3.1 Dichiarazioni di politica

Dedalus è un produttore di prodotti informatici. Opera in un mercato caratterizzato da sistemi sempre più digitalizzati e interconnessi e da un aumento delle normative e dei requisiti dei clienti.

3.1.1 Definizione delle parti interessate e delle loro responsabilità

L'ISMS di Dedalus è riferito a tutte le parti interessate, che sono elencate con i loro requisiti IS&DP (Information Security & Data Privacy) e le aspettative relative all'ISMS di Dedalus:

Parte interessata interna	Requisiti e aspettative delle parti interessate all'ISMS di Dedalus
Il Leadership Team di Dedalus Italia (LT)	Essi definiscono gli obiettivi dell'ISMS di Dedalus e vogliono svolgere la propria attività con fiducia ed essere informati sui rischi e sugli impatti legati alle loro decisioni.
Gruppo Dedalus IT	Ha la necessità e chiede indicazioni su come: • implementare applicazioni e infrastrutture in modo sicuro • garantire la conformità alle norme sulla privacy dei dati per l'archiviazione delle Informazioni di identificazione personale (PII), delle Informazioni sanitarie protette (PHI) e di altri dati sanitari sui sistemi Dedalus Fornisce servizi di cybersecurity: • Gestione degli incidenti di sicurezza interni a Dedalus • Supporto alla gestione degli incidenti di sicurezza nell'infrastruttura cloud di Dedalus e nelle installazioni on-premise dei clienti.

Parte interessata interna	Requisiti e aspettative delle parti interessate all'ISMS di Dedalus
	• Fornitura di strumenti, compreso il SIEM, per il monitoraggio, il rilevamento, la risposta e il ripristino della sicurezza. • Fornitura del servizio SOC per l'infrastruttura interna e cloud di Dedalus
Sales	Hanno la necessità e chiedono indicazioni su come: • integrare l'IS&DP nelle loro attività di vendita e servizi rivolti ai clienti in modo efficiente dal punto di vista delle risorse (ad es. gare d'appalto, contratti, requisiti dei clienti)
Order fulfilment / Program management	Ha la necessità e chiede indicazioni su come: • distribuire, mantenere e utilizzare prodotti e strumenti in conformità con le normative e le best practice IS&DP. • garantire il rispetto dei principi di security by design e privacy by design durante l'implementazione di software on-premise e nel cloud • garantire il corretto trattamento delle informazioni personali
Solution Development	Ha la necessità e chiede indicazioni su come: • realizzare prodotti in linea con le normative e le best practice IS&DP. • integrare IS&DP nei propri processi (ad es. utilizzo dei dati, gestione dei fornitori)
After Sales / Managed Services and delivery	Ha la necessità e chiede indicazioni su come: • supportare i clienti nell'utilizzo dei prodotti e degli strumenti in conformità alle normative e alle best practice IS&DP e

Parte interessata interna	Requisiti e aspettative delle parti interessate all'ISMS di Dedalus
	• gestire i reclami in conformità alle normative e alle best practice di IS&DP. • gestire gli incidenti di sicurezza relativi ai clienti • garantire il corretto trattamento delle informazioni personali
Funzioni di supporto globale e locale come le risorse umane, gli approvvigionamenti	Hanno la necessità e chiedono indicazioni su come integrare i requisiti trasversali di IS&DP nei loro processi.
Responsabile della protezione dei dati (DPO)	Ha la necessità di definire controlli e misure per garantire una corretta gestione della privacy dei dati PII e PHI all'interno di Dedalus.
Sindacati e comitati dei lavoratori	Hanno la necessità e chiedono indicazioni su come definire controlli e misure per garantire una corretta gestione della privacy dei lavoratori in azienda di Dedalus
Lavoratori (dipendenti e collaboratori di Dedalus)	Gestione corretta degli strumenti e delle informazioni aziendali Attenzione alla gestione dei propri dati nel rispetto della normativa vigente in materia di privacy Necessità e richiesta di indicazioni su riservatezza, disponibilità e integrità dei dati di Dedalus.

Parte interessata esterna	Requisiti IS&DP e aspettative delle parti interessate all'ISMS di Dedalus
Clienti	Riservatezza, disponibilità, integrità delle informazioni gestite attraverso il software utilizzato dai clienti, indipendentemente dal fatto che sia distribuito on-premise o nel cloud, e attraverso i servizi, inclusi i servizi cloud, forniti. Grande attenzione alla gestione dei dati sanitari sensibili dei pazienti nel rispetto di tutte le normative sulla privacy applicabili, del GDPR e delle normative sulla privacy dei Paesi extraeuropei.
Gli utenti (persone) dei servizi forniti da Dedalus al cliente (medici, infermieri, personale amministrativo, ecc.)	Riservatezza, disponibilità, integrità dei dati dell'utente utilizzati o memorizzati all'interno del software, dell'infrastruttura e dei servizi cloud di Dedalus. Conformità alle normative vigenti in materia di privacy dei dati.
Pazienti	Riservatezza, disponibilità, integrità delle PII dei pazienti e dei dati sanitari utilizzati o conservati all'interno del software, dell'infrastruttura e dei servizi cloud di Dedalus.
Fornitori	Riservatezza, disponibilità, integrità dei dati dei fornitori utilizzati o conservati all'interno del software, dell'infrastruttura e dei servizi cloud di Dedalus. Conformità alle norme sulla privacy. Supporto agli audit per garantire il rispetto del livello richiesto per IS&DP all'interno del proprio perimetro e dei propri servizi.
Le Autorità di protezione dei dati dei paesi in cui Dedalus opera	Conformità del software e delle soluzioni alle normative e alle linee guida internazionali, nazionali e locali applicabili. Maggiore sicurezza nel trattamento dei dati con l'utilizzo di strumenti e servizi, incluso il servizio cloud, sviluppati/gestiti da Dedalus / dalle società del gruppo

Organismi di certificazione e autorità di regolamentazione	Possono verificare o ispezionare la posizione in termini di IS&DP di Dedalus, periodicamente o senza preavviso, e possono, a seconda del loro mandato, imporre azioni esecutive, ad esempio il ritiro di un certificato, l'imposizione di una multa, la revoca del diritto di vendita in un mercato locale o il divieto di un'attività di trattamento dei dati.
Investitori del Gruppo e delle società del Gruppo	Compatibilità dei software e delle soluzioni Dedalus con la normativa sulla privacy e con i provvedimenti del Garante della Privacy, del GDPR e delle normative dei Paesi in cui Dedalus opera. Maggiore sicurezza nel trattamento dei dati con l'utilizzo di strumenti e servizi, compresi i servizi cloud, sviluppati/gestiti o utilizzati da Dedalus.

3.1.2 Ambito di applicazione ed esclusioni dell'ISMS

Il campo di applicazione dell'ISMS è definito nell'IMS Handbook (paragrafo 1) e nel documento di governance ISP-ITA-GR-01-Dedalus Italia Statement of Applicability (SoA), per una panoramica dei controlli nel campo di applicazione e dei controlli esclusi.

3.1.3 Obiettivi della sicurezza delle informazioni e della privacy dei dati

Dedalus si impegna a supportare i fornitori di servizi di cura nella protezione della privacy dei dati dei loro pazienti, fornendo prodotti e servizi sicuri; a tal fine il top management di Dedalus ha definito i seguenti obiettivi:

1. Assicurare il regolare reporting dei KPI della sicurezza delle informazioni alla direzione e definire le necessarie azioni di follow-up.
2. Stabilire un programma efficace di sensibilizzazione, formazione e istruzione in materia di sicurezza delle informazioni, informando tutti i dipendenti e le altre parti interessate a tutti i livelli pertinenti dei loro obblighi in materia di sicurezza delle informazioni stabiliti nelle politiche di sicurezza delle informazioni, negli obiettivi, ecc.

3. 90% di completamento del Dedalus Security Awareness Training per i dipendenti delle aziende che rientrano nel campo di applicazione del SGI di Dedalus Italia definito in QARA-ITA-GR 01-Enti legali che hanno adottato l'IMS di Dedalus Italia
4. Ridurre al minimo l'esposizione dell'organizzazione ai rischi per la sicurezza delle informazioni.
5. Implementare la protezione tecnica e il monitoraggio necessari per evitare incidenti di sicurezza.
6. Garantire l'implementazione delle migliori pratiche di codifica sicura, security by design e privacy by design all'interno del processo di sviluppo.
7. Garantire attivamente la prevenzione e il rilevamento degli incidenti di sicurezza delle informazioni.
8. Garantire la conformità alle normative sulla privacy dei dati e sulla sicurezza delle informazioni applicabili alla nostra organizzazione e ai nostri clienti.

3.2 Principi della politica

Nello standard ISO/IEC 27002:2022 (Sicurezza delle informazioni, cybersicurezza e protezione della privacy - Controlli di sicurezza delle informazioni), c'è una sezione che menziona cinque attributi di controllo. Gli attributi di controllo sono utilizzati per classificare i controlli. Dedalus dovrebbe utilizzare questi attributi con valori basati sui requisiti dell'organizzazione per comprendere la posizione attuale della sicurezza. Per informazioni dettagliate sugli attributi di controllo, consultare lo standard ISO/IEC 27002:2022 e le relative linee guida per il cloud e le linee guida ISO/IEC 27017:2017 e ISO/IEC 27018:2019 per il cloud.

Di seguito sono riportati i cinque attributi di controllo con i relativi valori:

1. Tipi di controllo

Valori degli attributi:

- Preventivo (controllo per evitare il verificarsi di un incidente di sicurezza delle informazioni),
- Detectivo (controlli che agiscono quando si verifica un incidente di sicurezza delle informazioni)

- Correttivo (controlli effettuati dopo che si è verificato un incidente di sicurezza delle informazioni)

2. Proprietà della sicurezza delle informazioni

Valori degli attributi:

- Riservatezza,
- Integrità e
- Disponibilità

3. Concetti di cybersecurity

Valori degli attributi:

- Identificare
- Proteggere
- Rilevare
- Rispondere
- Recuperare

4. Capacità operative

Valori degli attributi: Governance, Gestione delle risorse, Protezione delle informazioni, Sicurezza delle risorse umane, Sicurezza fisica, Sicurezza dei sistemi e delle reti, Sicurezza delle applicazioni, Configurazione sicura, Gestione delle identità e degli accessi, Gestione delle minacce e delle vulnerabilità, Continuità, Sicurezza delle relazioni con i fornitori, Legale e conformità, Gestione degli eventi di sicurezza delle informazioni e Garanzia della sicurezza delle informazioni.

5. Domini di sicurezza

Valori degli attributi:

- Governance ed ecosistema,
- Protezione,
- Difesa e resilienza

Per raggiungere gli obiettivi di sicurezza delle informazioni, Dedalus ha adottato i principi della politica di sicurezza delle informazioni elencati di seguito che corrispondono alla norma ISO/IEC

27001:2022; questa politica considera anche i requisiti delle linee guida ISO/IEC 27017:2017 e ISO/IEC 27018:2019 per il cloud.

3.2.1 Controlli organizzativi (A.5)

I controlli organizzativi si concentrano su politiche, processi, procedure, responsabilità e altre misure organizzative.

Totale controlli coperti: 37

Politiche per la sicurezza delle informazioni:

Dedalus deve disporre di requisiti e linee guida per la sicurezza informatica al fine di proteggere i sistemi informatici dell'organizzazione. Le politiche e le procedure dettagliate per la sicurezza delle informazioni devono essere definite, riviste, approvate dal responsabile del processo di sicurezza delle informazioni e comunicate regolarmente ai dipendenti e alle parti esterne interessate. La revisione della politica globale sulla sicurezza delle informazioni e sulla privacy dei dati (IS&DP) e delle procedure deve essere effettuata almeno annualmente.

Ruoli e responsabilità in materia di sicurezza delle informazioni:

Organizzazione interna:

Il Leadership Team (LT) di Dedalus Italia, guidato dal CEO di Dedalus, è responsabile della governance aziendale.

La gestione e il controllo dei rischi di IS&DP sono parte integrante di questa governance aziendale.

Il Leadership Team (LT), guidato dal CEO di Dedalus Italia, indica la direzione strategica generale approvando attraverso il CEO questa Politica generale sulla sicurezza delle informazioni e sulla privacy, ma delega le responsabilità tattiche:

- all'Ufficio CISO (esperto di standard ISO 270XX) in relazione al contenuto tecnico del Information Security Management System e
- al ISMS Manager in relazione al framework, che fa parte dell'Integrated Management System (IMS) di Dedalus Italia, gestito da QARA.

Per consentire una promozione, un'implementazione e un'integrazione efficienti e coordinate di questa politica IS&DP, i ruoli e le responsabilità devono essere definiti e assegnati all'interno dell'organizzazione. La segregazione dei compiti deve essere mantenuta per ridurre il rischio di modifiche non autorizzate o di uso improprio delle risorse.

Organizzazione esterna:

Gli appaltatori e i consulenti di Dedalus devono rispettare ed essere informati sulla politica e sui documenti di processo IS&DP. I loro termini e condizioni di lavoro devono includere accordi e/o clausole di non divulgazione e riservatezza.

- Gestione del patrimonio: Si tratta di identificare, proteggere, gestire e mettere in sicurezza tutti gli asset di Dedalus. È necessario stabilire e mantenere l'inventario degli asset associati alle informazioni e ai sistemi informativi. Per ogni asset, o gruppo di asset, deve essere identificata e documentata una classificazione e la proprietà. L'uso delle apparecchiature aziendali da parte dei dipendenti deve essere gestito in modo sicuro. La proprietà deve essere assegnata a una persona con una conoscenza adeguata del suo ruolo nei processi aziendali di Dedalus. Al termine del rapporto di lavoro, il dipendente deve restituire tutti i beni dell'organizzazione. Per evitare divulgazioni e modifiche non autorizzate, le informazioni devono essere classificate ed etichettate secondo lo schema di classificazione adottato da Dedalus. Le informazioni memorizzate su supporti devono essere gestite secondo le procedure di Dedalus e smaltite in modo sicuro quando non sono più necessarie.

- Controllo degli accessi: Per prevenire l'accesso non autorizzato ai sistemi e ai servizi, il controllo degli accessi deve essere documentato e rivisto ogni anno e deve essere delineato come parte delle procedure di governance degli accessi. L'accesso ai sistemi e ai servizi dell'infrastruttura di rete deve essere concesso solo agli utenti autorizzati. L'assegnazione o la revoca del diritto di accesso di un utente deve essere documentata, gestita e approvata come da documento delle Procedure di Governance degli Accessi. La ricertificazione dell'accesso degli utenti ai sistemi e ai servizi dell'infrastruttura di rete deve essere effettuata su base annuale. Devono essere assegnati nomi utente individuali unici per consentire il non ripudio del trattamento delle informazioni. Per garantire un accesso sicuro ai sistemi, è necessario implementare procedure di accesso sicure, la segregazione dei compiti e un sistema di gestione delle password. L'uso di programmi di utilità privilegiati o del codice sorgente dei programmi deve essere

limitato e strettamente controllato e monitorato. Devono essere implementati meccanismi di registrazione e tracciamento. L'accesso ai servizi di rete interni ed esterni deve essere controllato e deve essere implementata un'autenticazione forte per un accesso sicuro alle applicazioni e soprattutto agli utenti remoti. La connessione alla rete interna di Dedalus tramite rete pubblica o dial-in deve essere protetta in modo adeguato.

- Sicurezza delle informazioni nelle relazioni con i fornitori: Per garantire che il processo di gestione dei fornitori sia eseguito in conformità ai requisiti IS&DP:
  - deve essere definita una politica IS&DP per il fornitore, per mitigare il rischio del suo accesso agli asset di Dedalus
  - i contratti con i fornitori terzi devono includere accordi e/o clausole di non divulgazione e riservatezza
  - i contratti o gli accordi con i fornitori devono includere clausole per la gestione dei rischi della catena dei fornitori, ogniqualvolta ciò sia pertinente e necessario.

- Gestione degli incidenti di sicurezza delle informazioni: L'IS&DP si concretizza nella salvaguardia della riservatezza, dell'integrità e della disponibilità dei dati e dei sistemi informativi. Qualsiasi violazione di uno di questi elementi può rappresentare una minaccia per Dedalus, per i clienti e per i dati di Dedalus, ed è considerata un incidente di IS&DP. Un sistema di gestione degli incidenti deve garantire l'identificazione, la valutazione, la comunicazione, il follow-up e la risoluzione tempestiva degli incidenti, nonché la riduzione o l'evitamento di incidenti simili. Ove possibile, devono essere attivati meccanismi di registrazione e tracciamento per agevolare le indagini sugli incidenti di sicurezza. Gli incidenti di sicurezza devono essere gestiti, risolti e documentati. I dipendenti di Dedalus devono essere informati sulla natura degli incidenti IS&DP e sulle procedure per segnalarli. Devono segnalare qualsiasi incidente IS&DP e qualsiasi vulnerabilità nota o sospetta il prima possibile.

- Aspetti di sicurezza delle informazioni nella gestione della continuità operativa: L'interruzione delle attività principali, causata da incidenti gravi o disastri, può avere un impatto economico e reputazionale significativo su Dedalus. Particolare attenzione deve essere prestata a:

- minacce alla continuità aziendale durante la valutazione dei rischi per le soluzioni
- la continuità dei processi di assistenza post-vendita in presenza di accordi sul livello di servizio con i clienti
- la continuità dei processi di sviluppo delle soluzioni
- e, in generale, ai servizi con certificazione ISO 20000-1 e al SaaS con qualifica ACN (Agenzia per la cybersicurezza nazionale).
- Le procedure di gestione della continuità operativa devono essere documentate e devono essere pianificate, implementate, verificate, riesaminate e valutate annualmente, anche in conformità al Sistema di Gestione della Continuità Operativa di Dedalus sviluppato per il SaaS e in conformità ai requisiti di qualificazione ACN.

- Conformità: Gli obblighi legali e contrattuali, nonché i diritti di proprietà intellettuale e i requisiti di protezione della privacy dei dati devono essere considerati in tutti i processi dell'organizzazione. Per garantire ciò, i requisiti e gli obblighi devono essere chiaramente identificati e considerati durante lo sviluppo delle politiche e dei documenti di processo IS&DP. Per garantire la conformità alla politica IS&DP di Dedalus, sono necessarie verifiche periodiche e audit. I sistemi e i processi devono essere analizzati per garantire che soddisfino i livelli di IS&DP previsti

- Procedure operative documentate: Per garantire il funzionamento corretto e sicuro dei sistemi informativi, devono essere redatti documenti di processo. Non è richiesta alcuna prova per gli aspetti che si presume siano ragionevolmente conosciuti dai dipendenti attraverso l'uso logico o ripetuto o la deduzione.

  Particolare attenzione deve essere prestata alla documentazione dei processi e/o delle procedure nell'ambito di:

  - servizio operativo quotidiano
  - l'elaborazione, l'accesso, lo scambio e la rimozione di informazioni sensibili
  - gestione di log e audit trail

  Ove possibile, deve essere stabilita e documentata la separazione dei compiti.

- Trasferimento di informazioni: Garantire la protezione delle informazioni nella rete e la sicurezza durante il trasferimento delle informazioni all'interno o all'esterno dell'organizzazione.

  Particolare attenzione deve essere prestata alla documentazione dei processi e/o delle procedure nell'ambito di:

  - politica e procedura di trasferimento delle informazioni
  - accordo di riservatezza e non divulgazione per proteggere le informazioni riservate e il trasferimento delle informazioni all'interno e all'esterno dell'organizzazione.

- Informazioni sulle minacce: Fornire la consapevolezza dell'ambiente di minaccia dell'organizzazione in modo da poter intraprendere azioni di mitigazione appropriate. Le informazioni relative alle minacce alla sicurezza informatica devono essere raccolte, analizzate e contestualizzate per produrre informazioni sulle minacce

- Sicurezza delle informazioni per l'utilizzo dei servizi cloud: Specificare e gestire la sicurezza delle informazioni per l'utilizzo dei servizi cloud. Gli accordi sui servizi cloud devono essere definiti e rivisti con il fornitore di servizi cloud.

  Particolare attenzione deve essere prestata alla documentazione dei processi e/o delle procedure nell'ambito di

  - Requisiti di sicurezza delle informazioni per i servizi cloud
  - Definire e documentare l'ambito, i ruoli, le responsabilità e la gestione dei servizi cloud.
  - controlli sulla sicurezza delle informazioni gestiti dal fornitore di servizi cloud e/o dal cliente del servizio cloud
  - eseguire valutazioni del rischio per identificare i rischi per la sicurezza delle informazioni e i rischi residui associati ai servizi cloud
  - gestire gli incidenti di sicurezza delle informazioni che si verificano con l'utilizzo dei servizi cloud
  - rivedere e monitorare l'uso continuo dei servizi cloud per gestire i rischi per la sicurezza delle informazioni
  - per modificare o interrompere l'utilizzo del servizio cloud.

Per implementare la gestione del SaaS fornito ai propri clienti Dedalus ISMS è stato progettato e implementato in conformità alle linee guida ISO 27017 e ISO 27018, nonché per soddisfare i requisiti della qualifica ACN.

- Prontezza ICT per la continuità operativa: Dedalus deve definire l'obiettivo del tempo di ripristino (RTO) e l'analisi dell'impatto sul business (BIA) per garantire la disponibilità delle informazioni dell'organizzazione e degli altri asset associati durante le interruzioni. Il sistema di gestione della continuità operativa per i servizi SaaS forniti ai clienti Dedalus deve essere conforme alle norme ISO/IEC 27017:2017 e ISO/IEC 27018:2019 e standard definiti nella parte del Sistema di Gestione della Continuità Operativa del SGI di Dedalus.

3.2.2 Controlli sulle persone (A.6)

Il controllo delle persone si concentra sulla gestione delle risorse umane, sulla sicurezza del personale e sulla formazione in materia di sicurezza.

Totale controlli coperti: 8

Sicurezza delle risorse umane: Questa sicurezza serve a garantire che i dipendenti comprendano il proprio ruolo e adempiano alle proprie responsabilità in materia di sicurezza delle informazioni. Vengono implementate linee guida specifiche per garantire IS&DP durante le seguenti fasi dell'impiego:

- Prima dell'impiego
- Durante l'impiego
- Alla cessazione e in caso di modifica del rapporto di lavoro

3.2.2.1 Prima dell'impiego

Dopo l'assunzione, i dipendenti devono essere informati sulle responsabilità IS&DP del loro ruolo nella loro funzione e nell'organizzazione. Saranno comunicate le possibili azioni disciplinari in caso di mancato rispetto della politica IS&DP di Dedalus. I termini e le condizioni di assunzione devono includere accordi e/o clausole di non divulgazione e riservatezza.

3.2.2.2 Durante l'impiego

I dipendenti di Dedalus devono essere consapevoli del loro ruolo e delle loro responsabilità in materia di IS&DP. In particolare, i dipendenti che hanno accesso ai dati di Dedalus, come le informazioni sensibili (PHI, informazioni sulla sicurezza, PII, proprietà intellettuale e altre informazioni relative all'azienda), devono essere informati della natura privata e confidenziale di questi dati e dell'impatto che potrebbe avere una gestione non appropriata delle informazioni. Devono essere adottate iniziative per garantire la creazione e il mantenimento della consapevolezza IS&DP in tutta Dedalus. Deve essere previsto un processo disciplinare formale per prendere provvedimenti contro i dipendenti che hanno commesso violazioni della sicurezza delle informazioni. Il lavoro a distanza comporta implicazioni per la sicurezza delle informazioni che devono essere considerate e documentate. La politica di lavoro a distanza deve delineare dove e quando è consentito il lavoro a distanza, la fornitura di dispositivi, l'accesso autorizzato e quali informazioni possono essere consultate a distanza.

3.2.2.3 Cessazione e modifica del rapporto di lavoro

Quando un dipendente assume un'altra posizione all'interno di Dedalus o lascia Dedalus, devono essere intraprese le azioni necessarie per garantire la continua protezione dei dati. Quando si lascia Dedalus o si cambia posizione, gli asset posseduti e messi a disposizione da Dedalus devono essere restituiti. L'accesso all'infrastruttura fisica e software di Dedalus deve essere revocato immediatamente dopo l'ultimo giorno lavorativo di un dipendente per garantire la protezione e l'integrità dei dati.

3.2.3 Controlli fisici (A.7)

Il controllo fisico si concentra sulla protezione delle risorse tangibili dalle minacce fisiche.

Totale controlli coperti: 14

Sicurezza fisica:

- Devono essere predisposti controlli fisici all'ingresso per consentire l'accesso ai siti e agli uffici di Dedalus solo agli utenti autorizzati. I registri devono essere mantenuti e monitorati per tutte le persone non autorizzate che accedono ai locali, a scopo di tracciabilità in caso di violazione della sicurezza fisica. La ricertificazione dell'accesso degli utenti alle infrastrutture fisiche deve essere effettuata su base annuale.

- I locali fisici devono essere monitorati da:
    - sistemi di sorveglianza (ad esempio, guardie di sicurezza, allarmi antintrusione, sistemi di monitoraggio video e TVCC)
    - sistemi di monitoraggio continuo (ad esempio, TVCC, rilevatori di contatto, rilevatori di movimento e sensori sensibili al suono)
    - sistema anti-intrusione per notificare qualsiasi intrusione non autorizzata al di fuori dell'orario di lavoro.

Sicurezza ambientale: Le informazioni e i sistemi informativi devono essere protetti contro il furto, la perdita, il danneggiamento dei beni attraverso meccanismi di prevenzione, rilevamento o protezione in caso di incendio, furto o perdita, danni causati dall'acqua e un'adeguata alimentazione alternativa o altre misure per prevenire l'interruzione dei servizi impegnati (ad esempio, attraverso accordi di servizio). Devono essere attuati piani in caso di interruzione dell'alimentazione e di altre interruzioni per garantire la disponibilità delle apparecchiature agli utenti Dedalus. Ovunque si trovi il cablaggio, le stanze o gli armadietti dei cavi devono essere chiusi a chiave e assegnati ad aree di accesso di sicurezza. È necessario adottare una politica di pulizia delle scrivanie per i documenti e i supporti di memorizzazione rimovibili e una politica di schermo trasparente per le strutture di elaborazione delle informazioni. Per salvaguardare i supporti di memorizzazione e le strutture di elaborazione delle informazioni, devono essere adottate istruzioni di lavoro per la scrivania pulita e lo schermo trasparente.

3.2.4 Controlli tecnologici (A.8)

I controlli tecnologici si concentrano sui controlli necessari per impostare e mantenere sicuri i sistemi tecnologici, lo sviluppo e la gestione del codice.

Totale controlli coperti: 34

- Crittografia: Deve essere definita una politica sui controlli crittografici per proteggere le informazioni all'interno di Dedalus. Questi controlli aiutano a raggiungere gli obiettivi di sicurezza delle informazioni, come la riservatezza, l'integrità e l'autenticazione. Tutte le chiavi crittografiche devono essere gestite e protette contro l'uso e la divulgazione non autorizzati.

- Sicurezza delle operazioni: Per garantire il funzionamento corretto e sicuro dei sistemi informativi, devono essere stabiliti documenti di processo.

  Particolare attenzione deve essere prestata alla documentazione dei processi e/o delle procedure nell'ambito di:

  - attività di change management sui processi
  - allestimento e configurazione dei sistemi
  - protezione da virus e codici maligni
  - attacchi alla sicurezza come phishing, vishing e smishing
  - gestione delle vulnerabilità tecniche dei sistemi informativi
  - roll-out di nuovi software o aggiornamenti sull'infrastruttura del cliente
  - backup
  - Servizi SaaS

  Ove possibile, deve essere stabilita e documentata la separazione dei compiti.

- Acquisizione, sviluppo e manutenzione del sistema: I controlli del ciclo di vita dello sviluppo del software (SDLC), i controlli dei test e della distribuzione e la gestione delle modifiche di emergenza devono essere definiti, rivisti, approvati e documentati annualmente. Ove possibile, deve essere stabilita e documentata la separazione dei compiti.

  All'interno di Dedalus si possono distinguere due tipi di sistemi informativi:

  - applicazioni interne (sia on premise che su cloud): quelle utilizzate per garantire il buon funzionamento dei diversi processi aziendali e di supporto all'interno di Dedalus
  - prodotti e servizi per i clienti: i sistemi informativi progettati e realizzati per supportare le imprese del Gruppo.

  Entrambi si atterranno a solidi principi di IS&DP, in particolare:

  - deve essere attiva una solida procedura di sviluppo sicuro
  - i principi di ingegneria dei sistemi sicuri devono essere definiti e applicati
  - le attività di sviluppo del sistema in outsourcing devono essere strettamente monitorate e controllate

Applicazioni interne:

I requisiti di sicurezza delle informazioni devono essere documentati nelle specifiche dei sistemi informativi e delle applicazioni nuovi o da modificare. Tali requisiti devono essere in linea con la natura privata e riservata delle informazioni elaborate o memorizzate e in linea con i principi dettati dal presente documento e dai requisiti normativi. Particolare attenzione deve essere prestata, ad esempio, ai seguenti aspetti

- mezzi per proteggere la riservatezza, l'integrità e la disponibilità dei dati in transito
- forte controllo dell'accesso (autenticazione e autorizzazione) ai dati basato sul principio del minor privilegio
- disponibilità della domanda e delle informazioni
- audit e log protetti per la creazione, la consultazione, la modifica e la cancellazione dei dati
- applicazioni gestite in un ambiente cloud

Considerazioni analoghe devono essere fatte quando si valuta il sistema informativo e/o l'applicazione di una terza parte.

L'uso incontrollato dei dati non è consentito nell'ambiente di sviluppo o di test. I dati di prova devono essere resi anonimi quando possibile o devono essere pseudonimizzati se l'anonimizzazione non è possibile. Questa operazione deve essere effettuata in un'area protetta nell'ambiente originale in cui sono memorizzati i dati, sempre prima di importare i dati nel sistema.

I principi del controllo degli accessi devono essere applicati sia nell'ambiente di sviluppo che in quello di test.

Prodotti e servizi per i clienti:

Al fine di fornire prodotti e servizi sicuri ai nostri clienti, le misure o i controlli IS&DP devono essere inclusi in questi prodotti e servizi fin dalla fase di progettazione e requisiti. Devono essere presi in considerazione i seguenti controlli IS&DP:

- mezzi per proteggere la riservatezza, l'integrità e la disponibilità dei dati in transito
- misure di disponibilità per garantire che i dati siano disponibili quando necessario

- forte controllo dell'accesso (autenticazione e autorizzazione) ai dati basato sul principio del minor privilegio
- audit e log protetti per la creazione, la consultazione, la modifica e la cancellazione dei dati

- Sicurezza della rete: Garantire la protezione delle informazioni in rete e la sicurezza durante il trasferimento delle informazioni all'interno o all'esterno dell'organizzazione.

  Particolare attenzione deve essere prestata alla documentazione dei processi e/o delle procedure nell'ambito di:

  - controlli di rete per gestire e proteggere le informazioni
  - sicurezza di tutti i servizi di rete
  - la segregazione nelle reti (sistemi informativi, utenti e servizi informativi)
  - politica e procedura di trasferimento delle informazioni
  - accordi di riservatezza e non divulgazione per la protezione delle informazioni riservate e il trasferimento delle informazioni all'interno e all'esterno dell'organizzazione.

- Gestione della configurazione: Le configurazioni, comprese quelle di sicurezza di hardware, software, servizi e reti, devono essere stabilite, documentate, implementate, monitorate e riviste. L'organizzazione deve definire e implementare processi e strumenti per applicare le configurazioni definite (comprese le configurazioni di sicurezza) per l'hardware, il software, i servizi (ad esempio i servizi cloud) e le reti per i sistemi di nuova installazione e i sistemi operativi. Devono essere previsti ruoli, responsabilità e procedure per garantire un controllo adeguato di tutte le modifiche alla configurazione. Le modifiche alle configurazioni devono seguire il processo di gestione delle modifiche.

- Cancellazione delle informazioni: Le informazioni memorizzate nei sistemi informativi, nei dispositivi o in qualsiasi altro supporto di memorizzazione devono essere cancellate quando non sono più necessarie, tenendo conto della legislazione e delle normative pertinenti. Quando si cancellano le informazioni su sistemi, applicazioni e servizi, si devono prendere in considerazione le seguenti misure:

- selezionare un metodo di cancellazione (ad esempio, la sovrascrittura elettronica o la cancellazione crittografica) in base ai requisiti aziendali e alle leggi e ai regolamenti pertinenti
- registrare i risultati della cancellazione come prova
- ottenere la prova della cancellazione delle informazioni dal fornitore quando si utilizzano fornitori di servizi di cancellazione delle informazioni

- Mascheramento dei dati: Per limitare l'esposizione dei dati sensibili, comprese le PII, e per soddisfare i requisiti legali, statutari, normativi e contrattuali, è necessario implementare tecniche di mascheramento dei dati come la pseudonimizzazione o l'anonimizzazione, la crittografia, ecc.

- Prevenzione della fuga di dati: Per ridurre il rischio di divulgazione ed estrazione non autorizzata di informazioni da parte di individui o sistemi, Dedalus deve prendere in considerazione le seguenti misure:
  - identificare e classificare le informazioni per proteggerle dalla fuga di notizie (ad esempio, informazioni personali, progetti di test, informazioni sanitarie, ecc.)
  - monitoraggio dei canali di fuga dei dati (ad es. e-mail, trasferimenti di file, dispositivi mobili e dispositivi di archiviazione)
  - agire per impedire la fuga di informazioni (ad esempio, mettere in quarantena le e-mail contenenti informazioni sensibili, classificare i file e le e-mail in base al contenuto dei dati).

- Attività di monitoraggio: Dedalus deve promuovere un approccio proattivo al monitoraggio che miri a prevenire e a intraprendere azioni per valutare potenziali incidenti di sicurezza prima che si verifichino.

- Filtraggio web: Dedalus deve implementare controlli di filtraggio web appropriati per limitare e controllare l'accesso ai siti web esterni e prevenire le minacce alla sicurezza e i rischi, come le infezioni da malware, derivanti dall'accesso a siti web esterni con contenuti dannosi. L'organizzazione deve identificare i siti web esterni ad alto rischio e implementare controlli di accesso e di web filtering adeguati.

- Codifica sicura: Dedalus deve seguire i principi di codifica sicura per prevenire i rischi di sicurezza e le vulnerabilità che possono sorgere a causa di pratiche di codifica del software inadeguate

3.3 Obblighi

Questa politica impone i seguenti obblighi:

- proteggere i dati di Dedalus, come le informazioni di sicurezza, le informazioni di identificazione personale (PII), le informazioni sanitarie protette (PHI), la proprietà intellettuale e altre informazioni relative all'azienda
- garantire i prodotti ai nostri clienti
- garantire la sicurezza dei servizi Software as a Service forniti ai nostri clienti
- garantire i servizi tecnici e professionali per i nostri clienti
- garantire i servizi del Gruppo IT Dedalus
- garantire il nucleo di Dedalus Processi

4 NORME E REGOLAMENTI APPLICABILI

Questa politica è conforme ai seguenti standard:

Standard/Regolamento/Guida/Requisito	Titolo
ISO/IEC 27001:2022	Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione della sicurezza delle informazioni - Requisiti
ISO/IEC 27017:2015	Tecnologia dell'informazione - Tecniche di sicurezza - Codice di prassi per i controlli di sicurezza dell'informazione basato su ISO/IEC 27002 per i servizi cloud
ISO/IEC 27018:2019	Tecnologia dell'informazione - Tecniche di sicurezza - Codice di prassi per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che agiscono come processori di PII

La norma ISO/IEC 27001:2022 è uno standard internazionale che fornisce i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni, preservando la riservatezza, l'integrità e la disponibilità delle informazioni attraverso l'applicazione di un processo di gestione del rischio e dando fiducia alle parti interessate che i rischi sono adeguatamente gestiti. L'applicazione di questo standard aiuta a garantire l'implementazione di politiche di sicurezza delle informazioni end-to-end all'interno di un'organizzazione; queste politiche sono strategiche per qualsiasi organizzazione IT.

La norma ISO/IEC 27017:2015 fornisce le linee guida per i controlli di sicurezza delle informazioni applicabili alla fornitura e all'utilizzo di servizi cloud, prevedendo:

- ulteriori indicazioni per l'implementazione dei controlli pertinenti specificati nella norma ISO/IEC 27002;
- controlli aggiuntivi con indicazioni per l'implementazione che riguardano specificamente i servizi cloud.

Fornisce controlli e indicazioni per l'implementazione sia per i fornitori di servizi cloud che per i clienti di servizi cloud.

La norma ISO/IEC 27018:2019 stabilisce obiettivi di controllo, controlli e linee guida comunemente accettati per l'implementazione di misure di protezione delle informazioni di

identificazione personale (PII) in linea con i principi di privacy della norma ISO/IEC 29100 per l'ambiente di cloud computing pubblico.

In particolare, il presente documento specifica le linee guida basate sulla norma ISO/IEC 27002, prendendo in considerazione i requisiti normativi per la protezione delle PII che possono essere applicabili nel contesto del/i contesto/i di rischio per la sicurezza delle informazioni di un fornitore di servizi cloud pubblici.

È applicabile a organizzazioni di ogni tipo e dimensione, comprese aziende pubbliche e private, enti governativi e organizzazioni senza scopo di lucro, che forniscono servizi di elaborazione delle informazioni in qualità di elaboratori di PII tramite cloud computing in base a un contratto con altre organizzazioni; le linee guida contenute in questo documento possono essere rilevanti anche per le organizzazioni che agiscono come responsabili del trattamento delle PII. I responsabili del trattamento delle PII possono essere soggetti a leggi, regolamenti e obblighi aggiuntivi in materia di protezione delle PII, non applicabili ai responsabili del trattamento delle PII.

4.1 Processi e/o metodologie applicabili

4.1.1 Ciclo di Deming

Per attuare questa politica e l'intero ISMS, Dedalus ha adottato un approccio globale alla sicurezza delle informazioni basato sul rischio, in linea con il processo Plan-Do-Check-Act (PDCA), come parte del Sistema di Gestione Integrato di Dedalus Italia.

4.1.2 Le migliori pratiche

Oltre agli standard sopra elencati, Dedalus prenderà in considerazione le seguenti best practice in materia di sicurezza e privacy:

- ISO/IEC 27002:2022 Tecnologia dell'informazione - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni
- ISO/IEC 27799:2016 Informatica sanitaria - Gestione della sicurezza delle informazioni in ambito sanitario con l'utilizzo di ISO/IEC 27002
- ISO/IEC 27005:2019 Tecnologia dell'informazione - Tecniche di sicurezza - Gestione dei rischi per la sicurezza delle informazioni
- Legge sulla portabilità e la responsabilità dell'assicurazione sanitaria (HIPAA)

4.2 Responsabilità

Tipo di responsabilità	FUNZIONE RESPONSABILE
STRATEGICO	CEO di Dedalus Italia Membri del Leadership Team
TATTICO	Politica, guida tecnica e linee guida: • BPO • Chief Information Security Office (CISO Office) • Product Security Office (PSO) • Technology and Architecture Office (chiamato anche CTO)
	Framework del sistema: • ISMS Manager
OPERATIVO (organizzazione, processo, procedure, istruzioni di lavoro)	General Manager e team (Italia) Gestione della Business Unit (Globale e locale Italia) Responsabile organizzazione vendite e servizi (Regione Italia) Responsabile della funzione di supporto (MarCom, QARA, Legale, Risorse Umane, Approvvigionamenti, DITG, Ufficio CISO, Ufficio PSO, Ufficio CTO, Enterprise Risk and Compliance, DPO e DPM)

Il management responsabile può delegare le responsabilità, ma non può trasferire la propria responsabilità finale.

5 DEFINIZIONI E RIFERIMENTI

Acronimi

Terminologia	Spiegazione
BPM	Responsabile dei processi aziendali
BPO	Proprietario del processo aziendale
GSS	Servizio di assistenza globale
HIPAA	Legge sulla portabilità e la responsabilità dell'assicurazione sanitaria
HR	Risorse umane
IMS	Sistema di gestione integrato
IS&DP	Sicurezza delle informazioni e privacy dei dati
ISMS	Sistema di gestione della sicurezza delle informazioni
IT	Tecnologia dell'informazione
LT	Gruppo dirigente
PHI	sanitarie protette
PII	Informazioni di identificazione personale
QARA	Assicurazione qualità, Affari regolatori
SA	Contratto di servizio
SDLC	Ciclo di vita dello sviluppo del software

Definizioni

Terminologia	Spiegazione
Gestione della continuità operativa (BCM)	Il BCM fornisce all'organizzazione la capacità di rispondere efficacemente a minacce quali disastri naturali o violazioni dei dati e di proteggere gli interessi commerciali dell'organizzazione senza andare in fallimento.
Obbligo contrattuale	Si riferisce ai diritti e ai doveri di cui entrambe le parti sono legalmente responsabili in un accordo contrattuale.
Crittografia	cryptos + graphy significa scrittura nascosta. È una pratica per proteggere le informazioni e le comunicazioni utilizzando un algoritmo in modo che solo coloro a cui le informazioni sono destinate possano leggerle ed elaborarle.
Certificati digitali	Si tratta di un file elettronico che viene utilizzato per verificare l'identità di un soggetto su Internet e che consente connessioni crittografate. In parole povere, i certificati digitali sono come un passaporto elettronico.
Health Insurance Portability and Accountability Act (HIPAA)	Legge federale degli Stati Uniti che ha richiesto la creazione di standard nazionali per proteggere le informazioni sanitarie sensibili dei pazienti dalla divulgazione senza il consenso o la conoscenza del paziente.
Altri dati aziendali	I dati aziendali contengono informazioni riservate e critiche per il normale funzionamento di Dedalus. Queste informazioni comprendono tutti i dati relativi all'azienda, ad esempio documenti interni, comunicazioni, ecc.
Informazioni di identificazione personale - Personally Identifiable Information (PII)	Le informazioni di identificazione personale (PII) sono tutte le informazioni relative a una persona fisica identificata o identificabile. Queste informazioni comprendono il numero di previdenza sociale, il numero di telefono, l'indirizzo e-mail, gli identificatori online, ecc.

Terminologia	Spiegazione
Phishing	Il phishing è un tipo di attacco di ingegneria sociale in cui un aggressore chiama o invia un'e-mail o un messaggio fraudolento con lo scopo di attirare le persone a rivelare informazioni sensibili.
Prodotti	Prodotti Dedalus, strumenti interni, componenti dell'infrastruttura IT interna, sistemi dei clienti (comprendenti prodotti Dedalus e prodotti di terze parti)
Informazioni sanitarie protette - Protected Health Information (PHI)	Le informazioni sanitarie protette (PHI) sono tutte le informazioni identificabili individualmente relative allo stato di salute fisica o mentale di un individuo o alla fornitura di assistenza sanitaria o al pagamento dell'assistenza sanitaria. In questo documento e in tutti i documenti IS&DP questo termine viene utilizzato e comprende: - Dati sanitari - PID (Dati identificabili del paziente) (https://en.wikipedia.org/wiki/Protected_health_information)
Informazioni sulla sicurezza-Security information (SI)	Le informazioni sulla sicurezza sono l'insieme delle impostazioni sensibili di sicurezza e di rete e degli strumenti di comunicazione, software o hardware che controllano l'accesso a un sistema contenente PHI o forniscono mezzi per alterare l'integrità o il comportamento del sistema, ad esempio: password, dati di configurazione, parametri di comunicazione, software di sicurezza.
Segregazione dei compiti	Questo concetto garantisce che a nessuna persona venga assegnata la responsabilità di più compiti collegati tra loro.
Smishing	SMS + Phishing = Smishing. Un aggressore invia un messaggio di testo per indurre i destinatari a fare clic su un link o a scaricare un'applicazione, inviando così all'aggressore informazioni private o scaricando programmi dannosi su uno smartphone.

Terminologia	Spiegazione
Ciclo di vita dello sviluppo del software - Software Development Life Cycle (SDLC)	Una metodologia che descrive il ciclo di vita delle applicazioni software. Pianificazione -> Analisi -> Progettazione -> Implementazione -> Test -> Manutenzione
Vishing	Voce + Phishing = Vishing. Un aggressore convince un individuo a fornire informazioni sensibili per telefono.

6 ALLEGATO

6.1 Ruoli e responsabilità IS&DP dettagliati

6.1.1 Dedalus Leadership Team (LT)

Il Dedalus Leadership team (LT), guidato dal CEO di Dedalus Italia, è il **responsabile ultimo della corporate governance di Dedalus Information Security**.

La gestione e il controllo dei rischi IS&DP sono parte integrante di questa governance aziendale.

Il Leadership Team dà la direzione strategica generale approvando e dando mandato alla presente SDP-ITA-PO 03-Politica generale sulla sicurezza delle informazioni e sulla privacy (politica IS&DP), ma delega le responsabilità tattiche all'ufficio CISO, che è guidato dal BPO Information Security and Data Privacy, l'Amministratore Delegato di Dedalus Italia (delegato LT per la sicurezza delle informazioni e la privacy).

Le responsabilità IS&DP del team di leadership saranno almeno:

- delineare la politica IS&DP di Dedalus;
- approvare, sostenere e impegnarsi nella politica IS&DP di Dedalus;
- fornire competenze adeguate per attuare e mantenere una politica IS&DP efficiente ed efficace;
- condurre revisioni periodiche di IS&DP;
- esaminare e discutere gli incidenti, i problemi o i rischi IS&DP critici o non accettabili.

6.1.2 Ufficio CISO

L'ufficio CISO è responsabile delle responsabilità tattiche di IS&DP in relazione a politiche, guide tecniche e linee di base.

Questi devono essere almeno:

- sviluppare politiche strategiche IS&DP, guide e linee guida globali e istruzioni di lavoro;
- garantire lo sviluppo e il mantenimento della formazione IS&DP;
- monitorare e valutare lo stato della politica IS&DP e degli incidenti IS&DP all'interno di Dedalus;
- gestire - in stretta collaborazione con QARA e il - il processo di gestione del rischio IS&DP;
- se necessario, escalare i rischi critici nel processo di Azione Correttiva e Preventiva (CAPA);
- riferire lo stato della politica IS&DP e degli incidenti IS&DP al comitato per la sicurezza e all'LT.

6.1.3 Technology and Architecture Office (CTO)

L'Ufficio Tecnologia e Architettura (CTO) è responsabile di alcune responsabilità tattiche di IS&DP:

- sviluppare e far evolvere costantemente l'Architettura di Riferimento Dedalus (DRA) per le applicazioni software
- sviluppare ed evolvere costantemente il Dedalus Security Framework (DSF) per le applicazioni software
- identificare e fornire gli strumenti per supportare le attività di cui sopra
- formalizzare e documentare il DRA e il DSF
- garantire la formazione dei team di sviluppo in relazione alle architetture e ai framework identificati
- valutare i prodotti esistenti in relazione alla loro aderenza all'architettura e al framework definiti
- individuare tempestivamente le nuove normative (in particolare quelle nazionali ed europee) per garantire la continua conformità dell'architettura e del quadro di sicurezza dei prodotti Dedalus.

6.1.4 Business Unit, Vendite, Order Fulfilment, After Sales e altri processi aziendali del Dedalus Operating Model

I Directors / Business Owner identificati come la prima linea di relazione del CEO nell'attuale organigramma sono responsabili dell'implementazione dei controlli IS&DP.

Essi hanno almeno le seguenti responsabilità:

- progettare, rivedere e adeguare la politica e i documenti di processo IS&DP di Dedalus Italia e la loro attuazione;
- rivedere e discutere gli incidenti e i problemi di IS&DP e proporre soluzioni all'LT quando si verificano incidenti, problemi o rischi critici di IS&DP;
- rivedere e adottare nella politica IS&DP qualsiasi modifica rilevante delle leggi e dei regolamenti in materia di sanità;
- formalizzare la proprietà delle informazioni e dei sistemi informativi globali.

Sono i Risk Owner IS&DP per il loro processo e devono essere almeno:

- partecipare alla valutazione del rischio coordinata dal QARA;
- valutare i rischi legati al proprio processo/area;
- contribuire attivamente alla gestione dei rischi IS&DP in conformità con l'attuale metodologia di rischio IS&DP.

6.1.5 Gestione delle Business Unit , delle Vendite, dell'Order Fulfilment, dell'After Sales e di altri processi aziendali del Modello Operativo Dedalus.

Il management è responsabile delle attività IS&DP quotidiane e della conformità nell'ambito della propria area di competenza.

Le Business Unit, Sales, Order Fulfilment, After Sales e il management degli altri processi aziendali deve avere almeno le seguenti responsabilità:

- indirizzare/comunicare ai subordinati la politica e i documenti di processo IS&DP di Dedalus Italia prima e durante l'impiego;
- coordinare e monitorare la formazione IS&DP per i propri dipendenti;

- garantire l'attuazione e la conformità alla politica IS&DP, ai suoi requisiti minimi di base globali e ai documenti di processo;
- implementare i documenti del processo IS&DP nell'organizzazione che dirigono;
- comunicare la creazione, la modifica o la rimozione dei diritti di accesso di un dipendente attraverso il canale appropriato.
- contribuire alla valutazione dei rischi di IS&DP secondo l'attuale metodologia di rischio di IS&DP.

6.1.6 Owner di informazioni e sistemi informativi

Gli owner sono responsabili dell'IS&DP delle informazioni e/o dei sistemi informativi che le gestiscono.

Le loro responsabilità sono almeno:

- classificare le informazioni e i sistemi informativi;
- applicare la politica e i documenti di processo IS&DP di Dedalus Italia alle loro attività quotidiane;
- collaborare alla pianificazione, allo sviluppo e all'esecuzione della pianificazione della continuità operativa
- pianificare e sviluppare test di accettazione per le applicazioni;
- approvare o negare l'accesso alle informazioni riservate;

6.1.7 Dipendenti e appaltatori

I dipendenti devono rendere l'IS&DP parte integrante della qualità dei prodotti e dei servizi di Dedalus e dell'organizzazione e delle operazioni. Devono apprendere e adottare l'IS&DP nelle loro attività professionali.

I dipendenti Dedalus hanno almeno le seguenti responsabilità:

- conoscere le politiche IS&DP e i documenti di processo di Dedalus Italia rilevanti per il proprio ruolo;
- rispettare e impegnarsi a rispettare la politica e i documenti di processo IS&DP di Dedalus Italia nello svolgimento delle attività quotidiane;
- salvaguardare IS&DP nelle attività quotidiane;
- rispettare il codice di condotta;

- segnalare gli incidenti o i punti deboli di IS&DP al Service Desk;
- partecipare a iniziative di sensibilizzazione su IS&DP;
- collaborare agli audit (interni o esterni) di IS&DP.

6.1.8 Quality Assurance Regulatory Affairs (QARA)

L'ISMS è incorporato nel Integrated Management System (IMS) di Dedalus.

Le esigenze dell'ISMS devono essere affrontate nell'IMS e nei suoi processi.

QARA è responsabile, attraverso il Responsabile ISMS, di assicurare che il quadro dell'ISMS sia pienamente integrato nel quadro dell'IMS.

QARA collaborerà inoltre con i proprietari e i responsabili dei processi per garantire l'implementazione e la manutenzione dei controlli IS&DP selezionati nei processi, nelle applicazioni e nei sistemi informativi di Dedalus.

QARA è responsabile del mantenimento della certificazione ISO 27001 con tutte le relative estensioni ISO/IEC 27017 e ISO/IEC 27018; gli audit ricorrenti sono pianificati ed eseguiti da QARA.

Le responsabilità del QARA comprendono:

- conoscere i documenti di politica e processo IS&DP di Dedalus Italia e i controlli ISO 27001 selezionati con tutte le relative estensioni ISO/IEC 27017 e ISO/IEC 27018;
- sviluppare e seguire il piano di audit;
- segnalare al Leadership Team eventuali non conformità, osservazioni e/o raccomandazioni;
- informare le non conformità, le osservazioni e/o le raccomandazioni ai proprietari dei processi e alle parti interessate che devono seguire o che sono interessate.

Con la continua evoluzione dei requisiti aziendali e normativi, Dedalus deve assicurarsi che i rischi per la sicurezza delle informazioni che la sua azienda deve affrontare siano adeguatamente identificati dai Risk owner.

Pertanto, il QARA coordinerà l'esecuzione delle valutazioni ricorrenti dei rischi IS&DP da parte degli appropriati risk owner, in stretta collaborazione e con il coinvolgimento dell'Ufficio CISO.

Le responsabilità del responsabile del processo di rischio IS&DP sono almeno:

- coordinare le valutazioni dei rischi IS&DP;
- partecipare alla valutazione del rischio;

- riferire sullo stato e sul livello di IS&DP agli stakeholder che devono seguire o che sono interessati;
- raccomandare possibili miglioramenti nel trattamento del rischio.

6.1.9 Legale

Per rispettare le leggi sulla privacy e sulla sicurezza applicabili a Dedalus, ai suoi clienti o ai suoi fornitori, i requisiti legislativi locali devono essere monitorati e, se necessario, incorporati nei processi di Dedalus.

Le responsabilità del team legale sono almeno:

- identificare, mantenere e comunicare la legislazione IS&DP;
- fornire un feedback alle domande in merito a:
    - Domande di IS&DP nei contratti con terzi;
    - le legislazioni locali in materia di sanità e crittografia.

6.1.10 Risorse umane

Per garantire che tutti i dipendenti siano informati e comprendano l'IS&DP, le Risorse Umane (HR) assisteranno i manager di linea nell'implementazione di misure e linee guida specifiche per l'IS&DP.

Le Risorse Umane sono responsabili almeno di:

- affrontare l'IS&DP prima, durante e dopo l'impiego;
- affrontare l'IS&DP nei termini e nelle condizioni di lavoro;
- organizzare la sensibilizzazione e la formazione IS&DP per tutti i dipendenti;

6.1.11 Dedalus Global Shared Services (GSS)

I Global Shared Services (GSS) di Dedalus sono responsabili della fornitura di servizi a Dedalus che soddisfino i requisiti IS&DP di Dedalus.

6.1.12 Terze parti

Alcune terze parti (ad esempio, i fornitori) svolgono un ruolo fondamentale nel supporto e nella manutenzione dei prodotti commerciali di Dedalus. Pertanto, devono aderire alla politica IS&DP stabilita da Dedalus.

I terzi sono responsabili almeno per:

- rispettare i requisiti IS&DP come da accordi con terze parti.