


|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

|                    |                   |                  |                   |                            |                   |
|--------------------|-------------------|------------------|-------------------|----------------------------|-------------------|
| Redazione:<br>CISO | Data:<br>24/03/26 | Verifica:<br>CDS | Data:<br>30/03/26 | Approvazione:<br>Direzione | Data:<br>30/03/26 |
|--------------------|-------------------|------------------|-------------------|----------------------------|-------------------|

| <b>TABELLA DELLE REVISIONI</b> |                                  |                 |                  |
|--------------------------------|----------------------------------|-----------------|------------------|
| <b>PARAGRAFO</b>               | <b>DESCRIZIONE<br/>MODIFICHE</b> | <b>VERSIONE</b> | <b>REVISIONE</b> |
|                                |                                  |                 |                  |
|                                |                                  |                 |                  |

## SCOPO

Definire contenuti, modalità di istituzione, di revisione e responsabilità della Politica della Sicurezza delle Informazioni, l'Ambito di riferimento dell'ISMS ovvero i suoi confini, gli obiettivi e le aree di intervento.


## CAMPO D'APPLICAZIONE

La presente procedura si applica:

- in fase di realizzazione dell'ISMS, come passo successivo all'analisi del rischio ed alla definizione delle responsabilità di coordinamento e operative relative alla sicurezza;
- in fase di riesame, manutenzione, reazione agli incidenti, e comunque in tutti i casi previsti dal Manuale del Sistema di Gestione della Sicurezza delle Informazioni.

## RIFERIMENTI

- Procedura P04 "Analisi e Gestione dei rischi";
- Classificazione Minacce Service Tech (rivista annualmente);
- Norma ISO/IEC 27002;
- Norma ISO/IEC 27001;
- Report analisi rischi;
- Manuale della Conservazione;
- D.lgs 138/2024 (Decreto attuativo Direttiva NIS2).

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

## DEFINIZIONE DELLA POLITICA DI SICUREZZA

I contenuti del documento "Politica per la Sicurezza delle Informazioni" devono comprendere:

- lo scopo che l'azienda intende perseguire con l'istituzione dell'ISMS;
- l'ambito di riferimento dell'ISMS
- l'enunciazione della Politica ed i suoi obiettivi;
- la definizione delle responsabilità sia per quanto riguarda l'istituzione che il mantenimento e la revisione;
- i soggetti che sono tenuti ad applicarla.

## ISTITUZIONE, REVISIONE E DIFFUSIONE

L'istituzione della Politica per la Sicurezza delle Informazioni è responsabilità della Direzione e del Comitato della Sicurezza; il documento deve essere datato e firmato dal Amministratore Delegato a titolo di impegno dei vertici aziendali al sostegno dell'ISMS.

I contenuti Politica per la Sicurezza delle Informazioni vanno definiti con il contributo del Comitato della Sicurezza, secondo le autorità e competenza dei singoli rappresentanti.

Il Comitato della Sicurezza è incaricato di:


- rielaborare l'analisi di rischio con riferimento ai processi aziendali e ai beni in essi utilizzati al fine di produrre un report di facile lettura che ne sintetizzi i risultati e individui le linee di azione in materia di sicurezza;
- illustrare tale report alla Direzione;
- fornire la massima competenza in tema di sicurezza per supportare le decisioni della Direzione.

La Direzione si riserva di:

- prendere visione del report sull'analisi di rischio;
- esprimere obiettivi e priorità generali;
- valutare e approvare la Politica per la Sicurezza delle Informazioni;
- garantire la coerenza con le altre politiche aziendali.

Qualora i risultati delle analisi illustrati nel report fossero in contrasto con gli obiettivi e le priorità espresse dalla Direzione, essa avrà la facoltà di intervenire d'ufficio, ad esempio:

- valutando l'opportunità di non includere attività aziendali a patto che tale esclusione non comprometta l'efficacia dell'ISMS;
- giudicando non probabili determinate minacce o decidendo di escludere certe aree di intervento suggerite dall'analisi di rischio.

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

Le decisioni della Direzione devono essere chiaramente documentate e verbalizzate durante le riunioni del Comitato della Sicurezza; quest'ultimo è chiamato a valutare se tali decisioni non compromettano l'integrità del Sistema.

La Politica per la Sicurezza delle Informazioni deve essere riesaminata almeno con cadenza annuale, ed in ogni caso quando intervengono cambiamenti significativi che ne possano pregiudicare l'efficienza e l'efficacia.

La proposta di revisione può provenire sia dalla Direzione che dal Comitato della Sicurezza. Affinché tutte le funzioni aziendali tenute alla sua applicazione possano conoscere e perseguire la Politica della Sicurezza, essa deve essere divulgata secondo le modalità più appropriate anche attraverso sessioni di formazione e sensibilizzazione.

Inoltre, con riferimento al servizio di conservazione, la politica di sicurezza viene comunicata e condivisa con le società del gruppo Over produttrici di documenti da conservare, tramite il sito istituzionale.

## DEFINIZIONE DELL'AMBITO E DEGLI OBIETTIVI DI SICUREZZA


Per poter definire l'ambito e gli obiettivi di sicurezza vengono utilizzati:

- l'analisi dei rischi, che rispecchia la situazione aziendale ad una data di riferimento;
- la Politica per la Sicurezza delle Informazioni, che contiene le direttive e gli obiettivi generali di sicurezza.

Il documento dell'Ambito di riferimento dell'ISMS, allegato 2 alla presente procedura definisce il perimetro del Sistema di Gestione ed in particolare:

- confini, ovvero aree fisiche, sistemi, processi ed attività cui si intende applicare l'ISMS;
- aree di intervento che vengono classificate in:
  - aree di intervento focalizzate: si riferiscono a particolari risorse, processi o aree fisiche che si intendono proteggere;
  - aree di intervento trasversali: si riferiscono a particolari dimensioni della sicurezza, ad esempio sicurezza fisica.
- obiettivi di sicurezza misurabili (riduzione del rischio)

A seconda dei casi può essere più agevole ed efficace applicare una o l'altra tipologia di area di intervento: ad esempio si può utilizzare l'approccio trasversale nel caso di obiettivi di sicurezza applicati indistintamente a tutte le risorse comprese nei confini dell'ISMS, e definire in modo focalizzato l'intervento su quelle risorse per le quali si intendono perseguire obiettivi particolari.

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

## INDIVIDUAZIONE DELLE AREE DI INTERVENTO

Le aree di intervento possono essere compiutamente individuate in base alla Politica della Sicurezza e all'analisi di rischio. Si tenga presente che la formulazione adottata nella Politica di Sicurezza costituisce un orientamento rispetto agli ambiti di intervento possibili (Sistemi informativi/tecnologie di supporto, organizzazione, risorse umane, infrastrutture/ambiente di lavoro).

Nell'analisi dei rischi vengono quindi messi in relazione gli ambiti di intervento possibili con le attività previste dai processi aziendali.

## INDIVIDUAZIONE DEGLI OBIETTIVI MISURABILI

L'obiettivo generale che Service Tech si propone di raggiungere è quello di portare e mantenere i rischi inerenti complessivi ad un livello Basso.


A tale fine i responsabili sono incaricati di proporre azioni di mitigazioni per i rischi per cui l'analisi ha evidenziato un livello di rischio inerente complessivo superiore o uguale a Medio. Le azioni di mitigazione proposte dai responsabili vengono verificate dal CISO, approvate dal Comitato della Sicurezza e assegnate come obiettivi ai responsabili, i quali sono inoltre incaricati della valutazione dell'efficacia dell'azione di mitigazione e alla valutazione del rischio residuo.

Al termine di questa fase si dispone quindi di obiettivi misurabili per ogni area di intervento. Il CISO ha il compito di monitorare lo stato di avanzamento e di aggiornare, in merito, il Comitato della Sicurezza.

Il criterio di accettabilità del rischio residuo prevede l'accettazione del rischio a fronte dell'abbassamento dello stesso, in seguito alla realizzazione di azioni di mitigazione, a un livello "Basso" a meno dell'accettazione del rischio da parte della Direzione.

## RESPONSABILITÀ

La redazione del documento dell'Ambito di riferimento è compito del Comitato della Sicurezza. Dato che tale documento riceve in input l'analisi di rischio e la Politica della Sicurezza, ogni cambiamento di questi ultimi può riflettersi su di esso, e renderne quindi necessaria una revisione.

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

## **Allegato 1 - POLITICA PER LA SICUREZZA DELLE INFORMAZIONI**

La Direzione, con l'emissione della dichiarazione di seguito riportata, stabilisce la Politica Aziendale per l'Information Security evidenziando gli obiettivi e gli impegni assunti di conseguenza.

Tale politica, che è stata definita coerentemente con le finalità e il contesto in cui Service Tech opera e relative esigenze del mercato, viene comunicata a tutti i collaboratori attraverso la sua pubblicazione sulla intranet aziendale ed è disponibile a tutte le parti interessate attraverso la pubblicazione sul sito aziendale.

Almeno una volta all'anno, durante il Riesame della Direzione, la Direzione, in collaborazione con il Comitato della Sicurezza, riesamina i contenuti di tale politica ed emette gli obiettivi.

Al fine di conseguire i propri obiettivi societari, Service Tech attua una politica orientata a fornire servizi che:


- 1) Soddisfino ben definite esigenze di tutte le parti interessate e rispondano alle aspettative delle società del gruppo Over o dei clienti del gruppo;
- 2) Siano organizzati in modo tale da conseguire un costante accrescimento della soddisfazione delle parti interessate.

Inoltre, Service Tech intende preservare il patrimonio informativo, garantendo adeguati livelli di sicurezza nel trattamento delle informazioni strategiche utilizzate nei processi aziendali e nell'ambito dei servizi forniti ai clienti.

Service Tech, attraverso l'impegno e il coinvolgimento attivo di tutte le componenti aziendali, si impegna a:

- Basare la propria politica sull'analisi del contesto esterno ed interno, sulle esigenze delle parti interessate e sull'individuazione di rischi ed opportunità a livello strategico ed operativo;
- Definire le modalità necessarie per assicurare che tale politica sia compresa ed applicata a tutti i livelli aziendali;
- Garantire il miglioramento continuo degli standard di sicurezza in modo tale da soddisfare con continuità le esigenze delle parti interessate;
- Misurare e verificare periodicamente l'efficacia del Sistema di Gestione della Sicurezza;
- Preservare il patrimonio informativo, garantendo adeguati livelli di sicurezza nel trattamento delle informazioni strategiche nei processi aziendali.

Al fine di raggiungere l'obiettivo relativo alla sicurezza delle informazioni ci si propone di conoscere, attraverso appropriati strumenti e procedure, il valore delle informazioni e dei mezzi utilizzati per il loro trattamento e divulgazione, le minacce a cui sono esposti e la loro vulnerabilità, e di ricondurre i rischi ad una soglia di accettabilità attraverso la progettazione, l'implementazione e la formalizzazione di un "*Sistema di Gestione della Sicurezza delle Informazioni*", che risponda ai requisiti di legge (Direttiva NIS2, GDPR e AI Act) e che sia conforme alla norma ISO 27001.


|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

Al fine di perseguire tale mission ci si propone di realizzare un sistema di gestione sulla sicurezza delle informazioni che risponda ai fattori critici di successo del mercato di riferimento e alla norma ISO/IEC 27001.

Nello specifico, il SGSI si pone i seguenti obiettivi.

#### SICUREZZA DELLE INFORMAZIONI E DEI DATI PERSONALI

- Relativamente ai servizi erogati in ambiente SaaS garantire il mantenimento della continuità operativa dei processi aziendali;
- La gestione della riservatezza delle informazioni;
- La protezione contro accessi non autorizzati;
- La tutela dell'integrità delle informazioni;
- L'applicazione dei principi di security e privacy by design nei processi di trattamento delle informazioni, al fine di prevenire violazioni;
- Il continuo miglioramento ottenuto attraverso la valutazione delle possibili debolezze del sistema informativo aziendale;
- Migliorare la consapevolezza interna dei rischi sulla sicurezza delle informazioni;
- Il coinvolgimento dei fornitori al fine di elevare e allineare gli standard di sicurezza a quelli adottati da Service Tech;
- Coordinamento con le Autorità di controllo in materia di sicurezza informatica in conformità alle normative di riferimento.

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

## **Allegato 2**

### **Definizione dell'AMBITO DEL SGSI**

#### **Campo di applicazione del SGSI (Sistema di Gestione della Sicurezza delle Informazioni)**

Dal punto di vista descrittivo è possibile definire l'estensione del SGSI di Service Tech attraverso i seguenti elementi:

#### **1. Processi di business**

***Progettazione ed erogazione di servizi cloud rivolti al settore sociosanitario.***

Per la descrizione dettagliata dei singoli processi si rimanda alla sez. 4 del Manuale i Sistema di Gestione Information Security.

#### **2. Sedi operative di Service Tech:**


- **Sede di Milano:** Via Capuccini n.4;
- **Sede di Milano:** Via Pergolesi n. 5;
- **Sede di Genova:** Via Bartolomeo Bosco n.45.

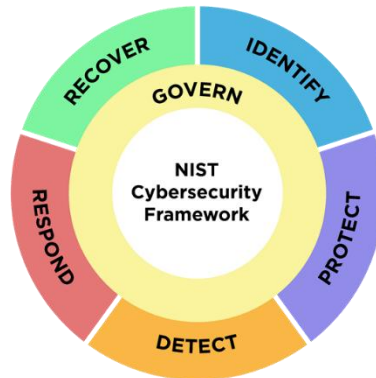
#### **3. Architettura di rete e dei sistemi informativi a supporto dei processi di Business per la cui descrizione si rimanda agli allegati alla Procedura P13 – Sicurezza delle Comunicazioni.**

#### **4. Cloud Service Provider e ambito di utilizzo**

#### **Mappatura dei processi di cybersecurity e relative procedure**


A seguito dell'introduzione nella norma ISO 27002:2022 degli attributi relativi ai principi di cybersecurity previsti dal Framework NIST, l'azienda ha individuato la corrispondenza tra funzioni del framework, processi interni e capacità operative (capability).

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|




Nella seguente tabella vengono riportate le procedure che soddisfano i requisiti del framework e le capacità operative a cui corrispondono.

| <b>NIST Cybersecurity Framework</b> | <b>Procedure</b>  | <b>Capability</b>   |
|-------------------------------------|---|---|
| Govern                              | P04 Analisi e Gestione dei rischi<br>P05 Ambito Politica e obiettivi di sicurezza<br>P06 Organizzazione interna per la sicurezza  | Governance  |
| Identify                            | P04 Analisi e Gestione dei rischi<br>P05 Ambito Politica e obiettivi di sicurezza<br>P06 Organizzazione interna per la sicurezza<br>P08 Gestione dei beni<br>P12 Sicurezza attività operative<br>P14 Acquisizione, sviluppo e manutenzione Sistemi<br>P15 Relazioni con i fornitori<br>P16 Incidenti di Sicurezza<br>P18 Conformità | Governance<br>Gestione degli Asset<br>Gestione delle minacce e delle vulnerabilità<br>Protezione delle informazioni<br>Sicurezza delle relazioni con i fornitori<br>Gestione degli eventi di sicurezza delle informazioni<br>Legale e di conformità<br>Garanzia di sicurezza delle informazioni<br>Sicurezza fisica<br>Sicurezza sistemi e reti<br>Sicurezza delle applicazioni<br>Continuità |
| Protect                             | P06 Organizzazione interna per la sicurezza<br>P07 Verifica competenze e sicurezza risorse umane  | Governance<br>Gestione dell'identità e degli accessi<br>Gestione degli Asset  |

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

|         |   |   |
|---------|---|---|
|         | P08 Gestione dei beni<br>P09 Controllo di accesso<br>P10 Crittografia<br>P11 Sicurezza Fisica e Ambientale<br>P12 Sicurezza attività operative<br>P13 Sicurezza comunicazioni<br>P14 Acquisizione, sviluppo e manutenzione Sistemi<br>P17 Sicurezza delle informazioni e continuità operativa | Gestione delle minacce e delle vulnerabilità<br>Protezione delle informazioni<br>Sicurezza delle relazioni con i fornitori<br>Gestione degli eventi di sicurezza delle informazioni<br>Continuità<br>Legale e di conformità<br>Garanzia di sicurezza delle informazioni<br>Sicurezza fisica<br>Sicurezza sistemi e reti<br>Sicurezza delle applicazioni<br>Configurazione sicura<br>Sicurezza delle risorse umane |
| Detect  | P11 Sicurezza Fisica e Ambientale<br>P12 Sicurezza attività operative<br>P16 Incidenti di Sicurezza   | Gestione delle minacce e delle vulnerabilità<br>Gestione degli eventi di sicurezza delle informazioni<br>Sicurezza fisica<br>Continuità<br>Sicurezza sistemi e reti<br>Sicurezza delle applicazioni   |
| Respond | P06 Organizzazione interna per la sicurezza<br>P07 Verifica competenze e sicurezza risorse umane<br>P12 Sicurezza attività operative<br>P16 Incidenti di Sicurezza<br>P17 Sicurezza delle informazioni e continuità operativa   | Governance<br>Gestione delle minacce e delle vulnerabilità<br>Gestione degli eventi di sicurezza delle informazioni<br>Sicurezza delle risorse umane<br>Continuità  |
| Recover | P06 Organizzazione interna per la sicurezza<br>P12 Sicurezza attività operative<br>P13 Sicurezza comunicazioni<br>P16 Incidenti di Sicurezza  | Governance<br>Gestione degli eventi di sicurezza delle informazioni<br>Gestione degli Asset<br>Sicurezza fisica<br>Sicurezza sistemi e reti<br>Sicurezza delle applicazioni   |

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

|  |   |  |
|--|---|--|
|  | P17 Sicurezza delle informazioni e continuità operativa | Configurazione sicura<br>Continuità<br>Gestione dell'identità e degli accessi<br>Gestione delle minacce e delle vulnerabilità<br>Gestione degli eventi di sicurezza delle informazioni<br>Continuità |
|--|---|--|

### **Individuazione degli ambiti di intervento**

L'analisi effettuata prevede la suddivisione dei rischi in 4 ambiti di intervento:

1. Sistemi informativi / Tecnologie di Supporto
2. Organizzazione
3. Risorse Umane
4. Infrastrutture / Ambiente di lavoro

### **Individuazione degli obiettivi misurabili e criteri di accettabilità del rischio**

#### **(*Arischio*)**

Nella Tabella seguente per ogni ambito di intervento, viene definita la priorità dal Comitato della Sicurezza anche in relazione alla disponibilità di risorse. Per ogni ambito viene definito l'obiettivo di miglioramento in termini di Indice di Rischio Attuale e Indice di Rischio Residuo Atteso.

Gli indici di rischio per ogni ambito vengono calcolati pesando 1 i rischi con livello A e 0,5 i rischi con livello M. Pertanto avremo:

- **Indice di Rischio Attuale (%)**:  $(\text{Numero di rischi con livello A} + \frac{1}{2} \text{Numero di rischi con livello M}) / n^{\circ} \text{ di rischi totali}$


Ponendoci l'obiettivo, per gli ambiti di intervento con priorità A, di ridurre del 50% i rischi di livello A portandoli a rischi di livello M, l'indice di Rischio Residuo Atteso viene così calcolato:

- **Indice di Rischio Residuo Atteso (%)**:  $(\frac{1}{2} \text{Numero rischi con livello A} + \frac{1}{2} \text{Numero di rischi con livello M}) / n^{\circ} \text{ di rischi totali}$

Ponendoci l'obiettivo, per gli ambiti di intervento con priorità M, di ridurre a livello M il 25% dei rischi di livello A, l'indice di Rischio Residuo Atteso viene così calcolato:

- **Indice di Rischio Residuo Atteso (%)**:  $(\frac{3}{4} \text{Numero rischi con livello A} + \frac{1}{2} \text{Numero di rischi con livello M}) / n^{\circ} \text{ di rischi totali}$

|  |  |                  |
|--|--|------------------|
|  |  | <b>Obiettivo</b> |
|--|--|------------------|

|   |   |  |
|---|---|--|
|  | <b>Procedura P05</b><br><b>Ambito, Politica e obiettivi della</b><br><b>sicurezza</b> | Data: 30/03/26<br>Rev. 0<br><b>Interno</b> |
|---|---|--|

| <b>Ambito di intervento</b>         | <b>Priorità Ambito di intervento (M,A)</b> | <b>Indice di Rischio Attuale (M,A)</b> | <b>Indice di Rischio Residuo Atteso (M,A)</b> |
|-------------------------------------|--|--|---|
| Risorse Umane                       | M  | IRA1                                   | IRR1  |
| Organizzazione                      | M  | IRA2                                   | IRR2  |
| SI e Tecnologie                     | A  | IRA3                                   | IRR3  |
| Infrastrutture e Ambiente di Lavoro | M  | IRA4                                   | IRR4  |

**Tabella 1**