

The logo of INAIL is displayed in white text on a dark blue rectangular background. The letters are bold and sans-serif.

**INAIL**

## TEMPLATE PIANO DI SICUREZZA

DIREZIONE CENTRALE PER  
L'ORGANIZZAZIONE DIGITALE

**INAIL**

DIREZIONE CENTRALE  
PER L'ORGANIZZAZIONE  
DIGITALE

## Indice del documento

1.	GENERALITÀ .....	4
1.1.	TABELLA DELLE VERSIONI.....	4
1.2.	TERMINI ED ACRONIMI.....	4
1.3.	RIFERIMENTI.....	4
2.	INTRODUZIONE.....	6
2.1.	OBIETTIVO.....	6
2.2.	PREMESSA .....	6
3.	INFORMAZIONI GENERALI .....	7
3.1.	REFERENTI.....	7
3.2.	STATO DI AVANZAMENTO DEL PROGETTO.....	7
3.3.	DESCRIZIONE DEL PROGETTO .....	7
3.3.1.	RELAZIONE CON I SERVIZI DI BUSINESS .....	7
4.	ELEMENTI ARCHITETTURALI.....	8
4.1.	DESCRIZIONE ARCHITETTURA LOGICA E FISICA.....	8
4.1.1.	ARCHITETTURA LOGICA.....	8
4.1.2.	ARCHITETTURA FISICA .....	8
4.1.3.	FLUSSI .....	8
4.2.	PRINCIPALI FUNZIONALITÀ .....	8
4.3.	RUOLI APPLICATIVI .....	8
4.4.	INTERAZIONI CON ALTRE APPLICAZIONI/SERVIZI .....	8
5.	ASSET .....	9
5.1.	DATI TRATTATI.....	9
5.2.	IDENTIFICAZIONE DEGLI ASSET .....	10
6.	TEST DI SICUREZZA .....	11
6.1.	RISULTANZE TEST DI SICUREZZA APPLICATIVA .....	11
6.2.	VA INFRASTRUTTURALI.....	11
7.	ANALISI DI CRITICITA' DEL PROGETTO .....	12
7.1.	CRITICITÀ PER LA DISPONIBILITÀ .....	12
7.2.	CRITICITÀ PER CLASSE DI DATO .....	12
7.3.	CRITICITÀ DEL PROGETTO .....	13
8.	ANALISI DELLE MISURE DI SICUREZZA .....	14
8.1.	LIVELLI DI SICUREZZA .....	14

8.2.	PIANO D'AZIONE.....	15
------	---------------------	----

# 1. GENERALITÀ

## 1.1. Tabella delle Versioni

Il documento in oggetto rappresenta il Piano di Sicurezza dell'iniziativa progettuale **<NOME IDENTIFICATIVO INIZIATIVA>**.

Come previsto dal processo di stesura del Piano di Sicurezza, il documento è periodicamente aggiornato. La tabella seguente illustra la cronologia delle varie revisioni del documento.

*[I dati inseriti nella seguente tabella fanno riferimento al template tracciandone lo storico delle modifiche. Sostituire le informazioni con i dati relativi al documento elaborato e cancellare la presente nota].*

Vers.	Data	Classif. <sup>1</sup>	Elabora	Verifica	Approva	Note
V01	26/10/2022	Dati non personali – Dati Interni	Team Security Governance	Michele Mellone Vittorio Baiocco	Michele Mellone Vittorio Baiocco	Prima versione del documento

## 1.2. Termini ed Acronimi

Termine	Definizione
DCOD	Direzione Centrale per l'Organizzazione Digitale
PdS	Piano di Sicurezza
GDPR	Regolamento UE 2016/679

## 1.3. Riferimenti

Nella seguente tabella sono elencati tutti i riferimenti citati all'interno del documento.

*<Questa sezione è importante perché molte delle informazioni che sono richieste nel piano di sicurezza sono di pertinenza di altri documenti.>*

*<Per garantire il corretto e costante allineamento delle informazioni riportate nel piano di Sicurezza, queste devono essere sempre referenziate con la fonte di provenienza. In*

- 
- <sup>1</sup> Le regole di classificazione sono riportate nel documento contenente lo schema di classificazione delle informazioni (par. Riferimenti)

*generale è preferibile un riferimento esterno piuttosto che una duplicazione di informazioni.>*

*<Inserire informazioni in tabella>*

Identificativo	Descrizione
DCOD_Tmp_DocumentoWord 26/02/2019 ver. 2.0	Template di riferimento
<a href="#">DCOD_SICU_LGd_CLASSIFICAZIONE DATI</a>	Schema di classificazione delle informazioni
<a href="#">DCOD_SICU_LGd_ETICHETTATURA E GESTIONE DELLE INFORMAZIONI</a>	Linee guida sulla corretta gestione delle informazioni in base alla loro etichettatura
DCOD_SICU_LGd_Implementazione PianoSicurezza Applicativa	Linee Guida sulla metodologia di Analisi del rischio applicativo e sugli strumenti di supporto per la compilazione del PdSA
DCOD_SICU_Pol_Sicurezza delle Informazioni	Politica sulla Sicurezza delle Informazioni
DCOD_SICU_Ele_Piano di Sicurezza	Analisi dei rischi operativa di sicurezza per il progetto
DCOD_Tmp_DocumentoWord del 14/06/2021 v07	Template di riferimento
<a href="#">DCOD_SICU_LGd_CLASSIFICAZIONE DATI</a>	Schema di classificazione delle informazioni
<a href="#">DCOD_SICU_LGd_ETICHETTATURA E GESTIONE DELLE INFORMAZIONI</a>	Linee guida sulla corretta gestione delle informazioni in base alla loro etichettatura
ISO/IEC 27001	
ISO/IEC 27005	

## 2. INTRODUZIONE

### 2.1. Obiettivo

Il presente documento rappresenta il piano di sicurezza dell'iniziativa progettuale **<NOME IDENTIFICATIVO INIZIATIVA>**.

Tale documento consentirà, in funzione delle caratteristiche dell'applicazione e/o dell'infrastruttura realizzata, di identificare le tipologie di rischio e valutare le relative misure di sicurezza.

Il documento rappresenta lo strumento adottato dalla DCOD per indirizzare la tematica della security e della privacy by-design.

### 2.2. Premessa

Quanto riportato in questo documento è soggetto ad aggiornamenti o modifiche.

### 3. INFORMAZIONI GENERALI

#### 3.1. Referenti

Referente	Riferimento
Responsabile di progetto:	<indicare il nome> - <email>
Responsabile sviluppo:	<indicare il nome> - <email>
Referente infrastrutture:	<indicare il nome> - <email>
Referente DBMS:	<indicare il nome> - <email>
Azienda fornitore:	<indicare il nome>
<b>Referente sicurezza:</b>	<indicare il nome> - <email>
Referente esercizio:	<indicare il nome> - <email>

Tabella 1 - Referenti

#### 3.2. Stato di avanzamento del progetto

Stato di avanzamento		
<X>	in esercizio	Data di avvio in produzione: <gg/mm/aaaa>
<X>	in fase di progettazione	
<X>	in sviluppo/collaudato	
<X>	in fase di manutenzione	

Tabella 2 - Stato avanzamento

#### 3.3. Descrizione del progetto

##### 3.3.1. Relazione con i servizi di business

Codice servizio di business	Nome servizio di business	Descrizione del supporto all'erogazione
<indicare il codice del servizio>	<indicare il nome del servizio>	<indicare se elemento applicativo o infrastrutturale principale o di supporto>

Tabella 3 - Relazione con servizi

## 4. ELEMENTI ARCHITETTURALI

### 4.1. Descrizione architettura logica e fisica

#### 4.1.1. Architettura logica

*<Riportare uno schema dell'architettura logica delle componenti infrastrutturali del progetto in esame. Evidenziare flussi logici tra i componenti e da/verso altre componenti esterne>.*

#### 4.1.2. Architettura fisica

*<Riportare uno schema dell'architettura fisica del progetto con l'indicazione dei componenti infrastrutturali: server, database, configurazioni di rete particolari, bilanciamento etc...>*

#### 4.1.3. Flussi

### 4.2. Principali funzionalità

*<Riportare una sintetica descrizione delle principali funzionalità erogate dalle componenti di progetto, includendo anche eventuali funzioni amministrative.>*

### 4.3. Ruoli applicativi

*<Riportare in questa sezione tutti i ruoli previsti nell'ambito del progetto ed una breve descrizione. In questa sezione riportare, ad esempio, le tipologie di utenti ai quali sono dedicate le funzionalità dell'iniziativa progettuale, gli utenti amministratori, eventuali utenze tecniche, ecc. Per ogni tipologia indicare il relativo ruolo, come ad esempio utilizzatore del sistema, amministrazione della componente X, ecc.>*

### 4.4. Interazioni con altre applicazioni/servizi

Applicazione esterna	Flusso IN	Flusso OUT	Bloccante IN	Bloccante OUT
	<S,N>	<S,N>	<S,N>	<S,N>

Tabella 4 - Interazione con altre applicazioni

## 5. ASSET

### 5.1. Dati trattati

<Riportare in questa sezione i principali dati che sono trattati all'interno del Si intenda per trattamento quanto specificato dal GDPR: >

"trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"

<Per ogni dato trattato specificare sinteticamente nella tabella che segue:

- nell'ambito di quali funzionalità, tra quelle indicate in 4.2 sono trattati;
- quali ruoli applicativi, tra quelli indicati in 4.3, trattano il dato;
- la modalità di accesso al dato (Lettura, Scrittura);
- quali flussi coinvolgono i dati (fare riferimento ai flussi logici identificati nell'architettura in 4.1.1).
- la classificazione dei dati secondo lo schema in uso in Istituto;
- il tempo di retention del dato se, secondo il criterio normativo, si tratta di dati personali>

<Inserire informazioni in tabella>

Funzionalità	Dato	Ruolo	Modalità	Flusso	Classificazione		Retention
					Criterio Normativo	Criterio Business	
			<L,S>		<ul style="list-style-type: none"> <li>Dati Non personali</li> <li>Dati personali</li> <li>Categorie Particolari di dati personali</li> <li>Dati personali relativi a condanne penali e reati</li> </ul>	<ul style="list-style-type: none"> <li>Dati pubblici</li> <li>Dati interni</li> <li>Dati riservati</li> <li>Dati strategici</li> </ul>	

Tabella 5 - Dati trattati

## 5.2. Identificazione degli asset

Id Asset	Tipologia di Asset	Descrizione/Note
	<Inserire la tipologia di asset, ad esempio: Web Server; Application Server; Database Server; Storage (physical); Storage (cloud); Client Nodes; Sistemi Mobile>	

Tabella 6 - Identificazione Asset

## 6. TEST DI SICUREZZA

### 6.1. Risultanze test di sicurezza applicativa

Data test	Moduli/Componenti	Esito e indicazioni su attività di rientro	Riferimento Seguro

Tabella 7 - Test applicativi

### 6.2. VA Infrastrutturali

Tipologia Test	Nome Host	Indirizzo IP	Tipologia Asset	Esito (High, Med., Low)	Data scansione
<VA/PT>					

Tabella 8 - VA

## 7. ANALISI DI CRITICITA' DEL PROGETTO

*<In questa sezione è definito un livello di criticità per il progetto in base ai tre principi fondamentali della sicurezza: Riservatezza, Integrità , Disponibilità. La criticità per disponibilità è definita direttamente dal risultato della BIA, mentre l'analisi per riservatezza e integrità derivano direttamente dalla classificazione dei dati processati dall'iniziativa progettuale.*

*Il valore di criticità del progetto sarà necessario per definire criteri di priorità di revisione e monitoraggio della sicurezza degli applicativi e infrastrutture dell'Istituto.>*

### 7.1. Criticità per la disponibilità

Impatto(D)=Classe di criticità risultante dalla BIA=<A/M/B>

RTO	RPO

Tabella 9 - RPO e RTO

### 7.2. Criticità per classe di dato

*<L'analisi delle classi di dato oggetto di trattamento nell'iniziativa progettuale prevede i seguenti passi operativi:*

- 1. Riprendere la tabella dei dati trattati identificata nella Tabella 5 - Dati trattati;*
- 2. Per ogni dato identificarne la tipologia rispetto alla classificazione prevista dall'Istituto avvalendosi della Tabella 10 - Schema Criticità per Classe di Dato e determinare il relativo livello di criticità.*

*Il livello di criticità per classe di dato è calcolato come il massimo dei valori di criticità dei dati trattati.>*

L'analisi delle classi di dato oggetto di trattamento nell'ambito delle componenti di progetto prevede, per ogni tipologia di dato identificato nella Tabella 5 - Dati trattati, la determinazione del relativo livello di criticità secondo lo schema:

		Strategico	Riservato	Interno	Pubblico
Personale	Sensibile	A	A	M	M
	Giudiziario	A	A	M	B
	Comune	A	M	M	B
Non Personale		A	M	B	B

Tabella 10 - Schema Criticità per Classe di Dato

Dato	Criticità
	<A/M/B>

Tabella 11 - Criticità per classe di dato

Ne risulta, quindi, una criticità

Criticità per Classe di Dato=<A/M/B>

Il livello di criticità per classe di dato è calcolato come il massimo dei valori di criticità dei dati trattati.

### 7.3. Criticità del progetto

**Criticità Progetto** = Max (Criticità per la Disponibilità; Criticità per classe di dato)  
=<A/M/B>

## 8. ANALISI DELLE MISURE DI SICUREZZA

### 8.1. Livelli di sicurezza

*<Eseguire nel documento excel "DCOD\_SICU\_Ele\_PianodiSicurezza" l'analisi dei livelli di sicurezza indicando lo stato di implementazione delle misure di sicurezza necessarie in base alla classe di sicurezza definita nella sezione precedente.*

*Sarà necessario riportare i risultati nel foglio di riepilogo in questa sezione per poter giustificare le eventuali non conformità ed accettare il rischio o indicare nel piano d'azione le attività pianificate per colmare i gap definiti.>*

Famiglia Misure	Livello di sicurezza	Contestualizzazione
Autenticazione	Da Gestire	
Autorizzazione	Da Gestire	
Audit e Monitoraggio	Da Gestire	
Protezione dei Dati	Da Gestire	
Protezione del software	Da Gestire	
Disponibilità Dati e Servizi	Da Gestire	
Sicurezza Rete	Da Gestire	
Cloud e Api	Da Gestire	
Infrastrutturale	Da Gestire	
Privacy	Da Gestire	
Autenticazione	Da Gestire	
Autorizzazione	Da Gestire	

Tabella 12 - Livelli di Sicurezza

## 8.2. Piano d'azione

<Indicare le azioni pianificate per arrivare a un livello di sicurezza adeguato per ogni famiglia di sicurezza ove il foglio indica "Da Gestire" o in "Fase di implementazione".

Famiglia	Contromisura	Contestualizzazione	Pianificazione
Protezione dei dati	Crittografia DB	WP XXXXX	Inizio Marzo 2022 Termine Luglio 2022

Tabella 13 - Piano d'azione