



Versione 4.5

# P042 – Piano per la sicurezza delle informazioni e la protezione dei dati (piano SIPD)

del 19 dicembre 2013 (stato: 1° settembre 2023)

Secondo l'articolo 11 capoverso 1 lettera e dell'ordinanza del 27 maggio 2020 sui ciber-rischi (OCiber, RS 120.73), il delegato alla cibersecurity emana la seguente direttiva per la protezione elevata di cui all'articolo 14d OCiber.



## Indice

<b>1</b>	<b>P042 – Piano SIPD</b> .....	<b>2</b>
<b>1.1</b>	<b>Validità del piano SIPD</b> .....	<b>3</b>
<b>2</b>	<b>Ausili per l'attuazione del piano SIPD</b> .....	<b>4</b>
<b>2.1</b>	<b>P042-Hi01 – Piano SIPD</b> .....	<b>4</b>
<b>2.2</b>	<b>P042-Hi02 – Analisi dei rischi</b> .....	<b>4</b>
<b>2.3</b>	<b>P042-Hi03 – Piano di emergenza</b> .....	<b>5</b>

# 1 P042 – Piano SIPD

Se dall'analisi del bisogno di protezione risulta un bisogno di protezione elevato, oltre all'attuazione delle direttive in materia di sicurezza per la protezione di base le unità amministrative (UA) definiscono, sulla base di un'analisi dei rischi, ulteriori misure di sicurezza, le documentano e le attuano (art. 14d cpv. 1 OCiber). Il piano SIPD contiene la descrizione delle misure di sicurezza e della loro attuazione per l'oggetto informatico da proteggere nonché la descrizione dei rischi residui.

Se vengono trattati dati personali per i quali dall'esame preliminare<sup>1</sup> risulta un rischio elevato per i diritti fondamentali della persona interessata, occorre coinvolgere anche il consulente per la protezione dei dati. In tal caso deve essere effettuata una valutazione d'impatto sulla protezione dei dati (VIPD) secondo l'articolo 22 della legge federale del 25 settembre 2020 sulla protezione dei dati (LPD; RS 235.1) e redatta la relativa documentazione, che è parte integrante del presente piano SIPD. La VIPD deve essere effettuata sulla base della pertinente guida<sup>2</sup>.

La stesura del piano SIPD compete al responsabile SIPD (nell'ambito di un progetto) o al responsabile dell'applicazione. Nella definizione del piano SIPD si può rinviare a piani di sicurezza già esistenti relativi a tematiche specifiche. L'NCSC mette a disposizione il modello aggiornato di tale documento in formato Word (*P042-Hi01 – Piano SIPD*).

L'attuazione delle direttive e delle misure in materia di sicurezza deve essere documentata e verificata dalle UA incaricate (art. 14 cpv. 3 e art. 14d OCiber).

I requisiti di sicurezza sono convenuti per scritto con i fornitori di prestazioni, sia per lo sviluppo e l'esercizio sia per la messa fuori esercizio di mezzi informatici. Le UA documentano e verificano l'attuazione delle misure di sicurezza.

Il piano SIPD deve essere verificato almeno dall'incaricato della sicurezza informatica dell'UA (ISIU)<sup>3</sup> nonché approvato dal committente e dal responsabile dei processi aziendali.

Le UA rilevano e documentano i rischi che non possono essere ridotti o possono esserlo soltanto in misura insufficiente (rischi residui). Il committente del progetto, il responsabile dei processi aziendali e la direzione dell'UA prendono atto dei rischi residui e ne danno conferma per scritto (art. 14d cpv. 2 OCiber).

Spetta al responsabile dell'UA competente decidere se assumere i rischi residui noti (art. 14d cpv. 3 OCiber).

Nel piano SIPD si devono rilevare almeno i seguenti dati:

- descrizione dell'oggetto informatico da proteggere;
- elenco dei documenti rilevanti per la sicurezza;
- classificazione secondo la direttiva «P041 – Analisi del bisogno di protezione»;
- descrizione del sistema rilevante per la sicurezza, compresi interlocutore / responsabilità, descrizione del sistema globale, descrizione dei dati da trattare, diagramma dell'architettura / matrice delle comunicazioni e descrizione della tecnologia di base;
- analisi dei rischi e misure di sicurezza, compresi i rischi che non possono essere ridotti o possono esserlo soltanto in misura insufficiente (rischi residui) – *occorre considerare i quattro aspetti della confidenzialità, dell'integrità, dell'accessibilità e della tracciabilità dei dati*;

<sup>1</sup> [www.bj.admin.ch](http://www.bj.admin.ch) > Stato & Cittadino > Protezione dei dati > Informazioni destinate agli organi federali

<sup>2</sup> [www.bj.admin.ch](http://www.bj.admin.ch) > Stato & Cittadino > Protezione dei dati > Informazioni destinate agli organi federali

<sup>3</sup> Nel caso dei servizi standard, la verifica compete al pertinente incaricato della sicurezza informatica.

- ripristino della capacità operativa – *per gli oggetti informatici da proteggere che supportano un processo aziendale critico*;
- osservanza / verifica / collaudo delle misure di sicurezza, compreso il collaudo del sistema;
- disattivazione;
- firme di: ISUI, committente, responsabile dei processi aziendali e capo dell'UA (o membro della direzione) – *deve essere effettuato prima dell'attivazione*.

Ulteriori dati possono essere richiesti o aggiunti nel singolo caso.

## **1.1 Validità del piano SIPD**

Il piano SIPD è valido per cinque anni al massimo.

## 2 Ausili per l'attuazione del P042

Durante l'allestimento del piano SIPD si devono considerare e stilare diversi documenti:

- il piano SIPD vero e proprio;
- l'analisi dei rischi;  
il piano di emergenza (in caso di oggetti informatici da proteggere che supportano processi aziendali critici).

L'elaborazione principale di questi documenti avviene preferibilmente durante la fase di concezione.

Per ciascun documento è disponibile un ausilio, ovvero un modello che può essere utilizzato per applicare correttamente le direttive vigenti. Il suo utilizzo (in particolare il contenuto) può essere adeguato alle proprie esigenze e obiettivi. I modelli vanno intesi come ausili per attuare correttamente tutte le direttive in materia di sicurezza e fungono da lista di controllo per tutti gli aspetti rilevanti dal punto di vista della sicurezza da prendere in considerazione. Tutti i documenti citati devono essere controllati in caso di modifiche (all'oggetto informatico da proteggere) e, se necessario, adeguati. Dopo un periodo massimo di cinque anni devono essere obbligatoriamente rielaborati<sup>4</sup>.

La documentazione deve essere firmata dall'ISIU, dal committente, dal responsabile dei processi aziendali e dal responsabile dell'UA (o da un membro della direzione) prima dell'attivazione.

### 2.1 P042-Hi01 – Piano SIPD

Il *piano SIPD* è considerato il documento principale per la sicurezza delle informazioni e la protezione dei dati nel corso del progetto e nella fase operativa. Contiene i dati necessari per mantenere e migliorare la sicurezza delle informazioni e la protezione dei dati e riassume gli aspetti della sicurezza delle informazioni e della protezione dei dati nel progetto.

Oltre alla sintesi e alla valutazione dei rischi residui di cui viene a conoscenza che devono essere sostenuti dai servizi responsabili<sup>5</sup>, il *piano SIPD* contiene una descrizione delle funzionalità rilevanti per la sicurezza del sistema globale e dei punti da osservare per la disattivazione.

Il piano SIPD non può essere omesso per i sistemi rilevanti per la sicurezza. È possibile tuttavia tralasciare alcuni sottocapitoli se non sono importanti.

### 2.2 P042-Hi02 – Analisi dei rischi

L'*analisi dei rischi* contiene una descrizione dei fattori di rischio rilevanti (accessibilità, confidenzialità, integrità e tracciabilità) nonché un elenco e una valutazione dei rischi. Fornisce altresì una panoramica sul potenziale di rischio presente nel sistema esaminato. Se vengono trattati dati personali per i quali dall'esame preliminare risulta un rischio elevato per i diritti fondamentali della persona interessata, tali rischi devono essere identificati e valutati separatamente o nell'ambito del piano SIPD. Questo ausilio supporta la valutazione degli effetti.

---

<sup>4</sup> Art. 14e OCiber

<sup>5</sup> Art. 14d OCiber

## **2.3 P042-Hi03 – Piano di emergenza**

Secondo la misura 17.1.1 della protezione di base TIC devono essere sviluppati, documentati e attuati piani per garantire l'operatività. Il *piano di emergenza* descrive la pianificazione dei casi di emergenza e la prevenzione delle catastrofi al fine di garantire il mantenimento e il ripristino dell'operatività in situazioni straordinarie.

L'NCSC mette a disposizione delle UA e dei responsabili di progetto un ausilio (modello) per la predisposizione di un piano di emergenza.