Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC
Sicurezza informatica della Confederazione

Versione 4.4

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

del 19 dicembre 2013 (stato: 1° aprile 2021)

Ai sensi dell'articolo 11 capoverso 1 lettera e dell'ordinanza del 27 maggio 2020 sui cyber-rischi (OCiber), il delegato alla cibersicurezza emana la seguente direttiva per la protezione elevata di cui all'articolo 14*d* OCiber.

Indice

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. 14*d* 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.

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. 14*d* 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)[1] 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. 14*d* cpv. 2 OCiber).
Spetta al responsabile dell'UA competente decidere se assumere i rischi residui noti (art. 14*d* cpv. 3 OCiber).

Nell'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, in particolare: interlocutore / responsabilità, descrizione del sistema globale, descrizione dei dati da elaborare (con riferimento al regolamento per il trattamento dei dati secondo l'art. 21 OLPD, se necessario), diagramma dell'architettura / matrice delle comunicazioni, 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 tener conto dei quattro aspetti della confidenzialità, dell'integrità, della disponibilità e della tracciabilità dei dati*
- Ripristino della capacità operativa – *per gli oggetti informatici da proteggere che supportano un processo aziendale critico*
- Osservanza / Verifica / Collaudo delle misure di sicurezza, in particolare: 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 in singoli casi.

[1] Nel caso dei servizi standard, la verifica compete al pertinente incaricato della sicurezza informatica.

1.1 Validità dell’analisi del piano SIPD

Il piano SIPD è valido per cinque anni al massimo.

2 Piano SIPD e relativa documentazione

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);
- il regolamento per il trattamento dei dati (se del caso, conformemente all'art. 21 OLPD).

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[2].

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[3], 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 (disponibilità [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.

[2] Art. 14*e* OCiber
[3] Art. 14*d* 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.

2.4 P042-Hi04 − Regolamento per il trattamento dei dati

Il regolamento per il trattamento dei dati provvede alla necessaria trasparenza nell'ambito dello sviluppo dei sistemi nonché del trattamento dei dati.
Il piano SIPD è la base su cui poggia il *regolamento per il trattamento dei dati*, che rientra nell'ambito dei progetti informatici dell'Amministrazione federale. Il titolare di una collezione di dati automatizzata emana un regolamento per il trattamento dei dati se tale collezione di dati presenta le seguenti caratteristiche (cfr. art. 21 OLPD):

- contengono dati personali degni di particolare protezione o profili della personalità;
- sono utilizzate da parecchi organi federali;
- sono accessibili a Cantoni, autorità estere, organizzazioni internazionali o privati; oppure
- sono collegate ad altre collezioni di dati.

Il regolamento per il trattamento dei dati provvede alla necessaria trasparenza nell'ambito dello sviluppo e dell'adattamento dei sistemi nonché del **trattamento elettronico dei dati personali**.