|  |  |
| --- | --- |
|  | **Dopo la compilazione: AD USO INTERNO** |

|  |
| --- |
|  |

P042-Hi01 – Piano per la sicurezza delle

informazioni e la protezione dei dati (piano SIPD)

< Nome del progetto/dell’oggetto da

proteggere >

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classificazione | AD USO INTERNO/CONFIDENZIALE/SEGRETO |
| Stato | In corso di elaborazione/in corso di verifica/approvato |
| Numero del progetto |  |
| Capoprogetto (CP BP) |  |
| Versione | Template – versione 4.4 |
| Data |  |
| Committente |  |
| Elaborato da |  |

Controllo delle modifiche

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Data | Descrizione/Osservazioni | Nome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribuzione

|  |  |  |
| --- | --- | --- |
| Funzione | Nome  | Dipartimento/Ufficio |
| ISIU |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Verifica del documento secondo le fasi del progetto

Le tabelle con le persone che verificano le singole fasi (e le confermano) possono essere integrate liberamente.

Avvio – prima dell’avvio del progetto

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Funzione | Nome | Data |
|  | RSIPD |  |  |
| ISIU |  |  |
|  |  |  |

Concezione – prima dell’avvio della fase

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Funzione | Nome  | Data |
|  | RSIPD |  |  |
| ISIU |  |  |
|  |  |  |

Realizzazione – prima dell’avvio della fase

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Funzione | Nome  | Data |
|  | RSIPD |  |  |
| ISIU |  |  |
|  |  |  |

Introduzione – prima dell’attivazione

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Funzione | Nome  | Data |
|  | ISDS-V |  |  |
| ISIU |  |  |
|  |  |  |

Indice

1 Considerazioni generali 5

1.1 Descrizione 5

1.2 Scopo del documento 5

1.3 Validità del documento 5

2 Compendio 6

2.1 In generale 6

2.2 Sintesi dei rischi residui 6

2.3 Osservazioni finali 6

2.4 Autorizzazione 7

3 Elenco dei documenti rilevanti per la sicurezza 8

4 Classificazione secondo la direttiva «P041 – Analisi del bisogno di protezione» 8

5 Descrizione del sistema rilevante per la sicurezza 10

5.1 Interlocutore/Responsabilità 10

5.2 Descrizione del sistema globale 10

5.3 Descrizione dei dati da elaborare 10

5.4 Diagramma dell’architettura/Matrice delle comunicazioni 11

5.5 Descrizione della tecnologia di base 12

6 Analisi dei rischi e misure di protezione 13

6.1 Rischi residui 13

7 Ripristino della capacità operativa 14

8 Osservanza/Verifica/Collaudo delle misure di protezione 14

8.1 Collaudo del sistema 14

9 Disattivazione 14

10 Abbreviazioni 15

11 Allegato 15

# Considerazioni generali

**Indicazioni per la compilazione del documento**

Il processo di sicurezza si prefigge di considerare concretamente l’aspetto della sicurezza informatica nell’ambito dei progetti e nelle fasi di introduzione e utilizzo dei mezzi informatici. A garanzia di ciò, vengono richiesti documenti specifici. Per questo l’NCSC mette a disposizione appositi modelli, il cui utilizzo (in particolare il contenuto) può essere adeguato alle proprie esigenze e agli obiettivi personali. Tali modelli, che devono essere considerati un ausilio per il corretto adempimento delle istruzioni in materia di sicurezza, fungono da lista di controllo per verificare il rispetto di tutti gli aspetti rilevanti ai fini della sicurezza.

* Le parti di testo in nero, corrispondenti alle prescrizioni, dovrebbero essere trasposte senza alcuna modifica, ammesso che siano coerenti con il resto del testo.
* Il testo in blu è un ausilio per la compilazione del documento e deve essere cancellato una volta inserito il testo relativo a un progetto concreto specifico.
* Il testo in rosso evidenzia importanti indicazioni o questioni che richiedono un chiarimento particolare oppure che devono essere descritte concretamente.
* Se dalla classificazione eseguita conformemente al capitolo 4 (classificazione secondo la direttiva «P041 – Analisi del bisogno di protezione») non risulta un elevato bisogno di protezione e, tuttavia, si deve realizzare un piano SIPD (ad es. come conseguenza della/deroga alla protezione di base delle TIC) l’analisi dei rischi può essere tralasciata (conformemente al capitolo 6).

## Descrizione

Descrizione dell’oggetto da proteggere

## Scopo del documento

Il piano SIPD contiene i dati necessari per mantenere e migliorare la sicurezza delle informazioni e la protezione dei dati.

Il presente documento riassume gli aspetti della sicurezza delle informazioni e della protezione dei dati nel progetto.

L’articolo 4 capoverso 1 e l’articolo 14 capoverso 3 dell’ordinanza del 27 maggio 2020 sui ciber-rischi (OCiber) sono elementi essenziali per stabilire una base corretta di un progetto TIC.

Tutte le misure di sicurezza per i singoli oggetti informatici da proteggere devono essere documentate in maniera attuale (conformemente all’art. 14cpv. 3 OIAF). Questo è uno degli scopi del piano SIPD (art. 14*d* cpv. 1 OCiber).

## Validità del documento

Il piano SIPD è valido per cinque anni al massimo.

# Compendio

Il compendio dovrebbe essere formulato in modo tale da risultare comprensibile anche per chi non dispone di conoscenze tecniche approfondite («nella lingua dell’affare»).

## In generale

Sintesi dei dati contenuti nel documento sull’analisi dei rischi effettuata, sulla sicurezza delle informazioni e sulla protezione dei dati. Fornisce una panoramica sul potenziale di rischio presente nel sistema esaminato.

## Sintesi dei rischi residui

In base al capitolo 6 si deve fare una sintesi dei rischi residui e provvedere alla relativa valutazione. Spetta al responsabile dell’unità amministrativa competente decidere se prendere in considerazione rischi residui noti.

## Osservazioni finali

Importanti osservazioni finali e conclusione sul presente oggetto informatico da proteggere.

## Autorizzazione

Le firme di autorizzazione e accettazione dei rischi residui devono essere apposte prima dell’avvio dei processi.

Apponendo la propria firma, l’incaricato/a della sicurezza informatica di un’unità amministrativa (ISIU) conferma di aver verificato il documento concernente l’attuazione della protezione di base delle TIC. L’incaricato/a ha verificato, in particolare, se il documento è stato compilato in ogni sua parte e se tutte le misure richieste sono state documentate. Inoltre, ha analizzato i dati con spirito critico, verificandone la coerenza e la loro correttezza in relazione all’oggetto informatico da proteggere.

Il/la committente e il/la responsabile dei processi operativi approvano il piano SIPD apponendovi la propria firma.

Il/la responsabile dell’unità amministrativa competente decide se assumere i rischi residui di cui viene a conoscenza[[1]](#footnote-1). A seconda del regolamento interno dell’Ufficio, il documento può essere anche firmato da un altro responsabile, membro della direzione.

|  |  |
| --- | --- |
| Data/Nome/Firma**ISIU**: | …………………………………………………...…... |
| Data/Nome/Firma**Committente**:  | …………………………………………………...…... |
| Data/Nome/Firma**Responsabile dei processi****aziendali**:  | …………………………………………………...…... |
| Data/Nome/Firma**Capo dell’UA o del membro della Direzione**:  | …………………………………………………...…... |

**È possibile apporre altre firme, ad esempio quella del responsabile del FP.**

**Le firme possono essere apposte anche in forma elettronica (in un file PDF).**

# **Elenco dei documenti rilevanti per la sicurezza**

Di seguito sono da elencare le basi giuridiche su cui si basa il progetto informatico (da realizzare). È preferibile definirle in collaborazione con il Servizio giuridico dell’UA o del dipartimento.

Un modello utile per documentare le corrispondenti basi giuridiche è disponibile sul sito <http://www.hermes.admin.ch/onlinepublikation/index.xhtml?element=ergebnis_rechtsgrundlagenanalyse.html>.

I rischi e i pericoli possono essere parzialmente coperti mediante piani di sicurezza sovraordinati o SLA. Questi documenti devono essere elencati di seguito.

Il presente elenco deve essere completato con i documenti interni dei dipartimenti e/o degli Uffici.

|  |  |
| --- | --- |
| Tipologia di documento | Titolo |
| Legge | [Legge federale del 19 giugno 1992 sulla protezione dei dati (LPD; RS *235.1*)](http://www.admin.ch/ch/i/sr/c235_1.html) |
|  | [Legge federale del 26 giugno 1998 sull’archiviazione (LAr; RS *152.1*)](http://www.admin.ch/ch/i/sr/c152_1.html) |
|  |  |
| Ordinanza | [Ordinanza del 27 maggio 2020 sui ciber-rischi (OCiber; RS *120.73*)](https://www.fedlex.admin.ch/eli/cc/2020/416/it) |
|  | [Ordinanza del 4 luglio 2007 sulla protezione delle informazioni della Confederazione (OPrl; RS *510.411*)](https://www.admin.ch/opc/it/classified-compilation/20070574/index.html) |
|  | [Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD; RS *235.11*)](https://www.admin.ch/opc/it/classified-compilation/19930159/index.html) |
|  | [Ordinanza del 25 novembre 2020 sulla trasformazione digitale e l'informatica (OTDI; RS *172.010.58*)](https://www.fedlex.admin.ch/eli/cc/2020/988/it) |
|  | [Ordinanza del 22 febbraio 2012 sul trattamento di dati personali derivanti dall’utilizzazione dell’infrastruttura elettronica della Confederazione (RS *172.010.442*)](https://www.admin.ch/opc/it/classified-compilation/20111415/index.html) |
|  |  |
| Istruzioni |  |
|  |  |
| Strategia | [Strategia TIC della Confederazione](https://www.bk.admin.ch/bk/it/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb000-ikt-strategie-des-bundes.html) |
| Metodo | [HERMES - Metodo per la gestione di progetti](http://www.hermes.admin.ch/) |
|  |  |
| Piani di sicurezza sovraordinati |  |
| SLA |  |
|  |  |
| Altro | 🡺 L’elenco deve essere compilato dall’autore |

# Classificazione secondo la direttiva «P041 – Analisi del bisogno di protezione»

La classificazione dell’oggetto informatico da proteggere deve essere eseguita secondo la direttiva «P041 – Analisi del bisogno di protezione» (Schuban).

Con le valutazioni dell’analisi del bisogno di protezione devono essere stimate e descritte nel documento anche le eventuali ripercussioni finanziarie dei requisiti di sicurezza.

Il risultato dell’analisi del bisogno di protezione approvata deve essere riportato in questo documento, in forma adeguata (l’analisi del bisogno di protezione completa può, ad esempio, essere inserita nell’allegato).

# Descrizione del sistema rilevante per la sicurezza

Descrizione dettagliata degli elementi del sistema, delle applicazioni, delle raccolte di dati esistenti ed elaborate e dei loro processi rilevanti per la sicurezza.

## Interlocutore/Responsabilità

|  |  |
| --- | --- |
| Persona | Nome |
| Responsabile delle applicazioni |  |
| Titolare dei dati |  |
| Operatore del sistema FP |  |
| Capoprogetto BP |  |
| Interlocutore presso il FP |  |
| ISID |  |
| ISIU |  |
| CPDU |  |
| Cerchia di utenti |  |
| Altri Servizi |  |

## Descrizione del sistema globale

Descrizione delle funzionalità rilevanti per la sicurezza come i ruoli, il metodo di autenticazione, il backup, i processi di supporto e manutenzione (eventualmente manutenzione a distanza), SLA ecc. È possibile fare riferimento anche a documenti corrispondenti (nome, data di creazione, unità di salvataggio ecc.). La descrizione deve essere formulata in maniera esaustiva, comprensibile e chiara anche per le persone non direttamente coinvolte.

## Descrizione dei dati da elaborare

Descrizione dei dati e delle strutture (ad es. banca dati utilizzata).

Le seguenti questioni devono essere chiarite e/o descritte in sede di elaborazione dei dati personali:

* La collezione di dati è stata notificata all’IFPDT?

In questo punto si stabilisce se il trattamento dei dati è conforme alle prescrizioni della legge sulla protezione dei dati. In particolare, si deve verificare se la collezione di dati deve essere notificata o meno all’incaricato federale della protezione dei dati e della trasparenza (IFPDT).

* Si deve predisporre un regolamento per il trattamento dei dati?
Quali strumenti ausiliari sono disponibili il Regolamento per il trattamento dei dati e l’ordinanza relativa alla LPD e la [Guida ai provvedimenti tecnici e organizzativi concernenti la protezione dei dati](https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/dokumentation/guide/provvedimenti-tecnici-e-organizzativi-concernenti-la-protezione-.html).
In caso affermativo, inserire il rimando al documento corrispondente.
* Esiste una base giuridica sul trattamento elettronico dei dati?
* I dati devono essere forniti all’Archivio federale in forma elettronica?
* Nel caso di informazioni classificate si devono osservare l’ordinanza sulla protezione delle informazioni (OPrl; RS *510.411*) e le [prescrizioni in materia di trattamento](https://intranet.vbs.admin.ch/de/wissen/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb.detail.document.html/vbs-intranet/de/documents/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb/Bearbeitungsweisungend.pdf.html) dei dati (Intranet; disponibili solo in tedesco). ‘
* Se l’oggetto da proteggere è rilevante per il processo di verifica RINA, inserire un rimando alla relativa documentazione.
	1. **Diagramma dell’architettura/Matrice delle comunicazioni**

Inserire un diagramma dell’architettura e una matrice delle comunicazioni oppure inserire un rimando al relativo documento di cui si è in possesso.





## Descrizione della tecnologia di base

Descrizione delle tecnologie utilizzate come, ad esempio, piattaforme di server, sistemi operativi, ambienti di sistema, reti, funzioni crittografiche ecc. Queste tecnologie devono essere descritte in maniera esaustiva, comprensibile e chiara anche per le persone non direttamente coinvolte. Altrimenti inserire un rimando al documento corrispondente di cui si è in possesso.

1. **Analisi dei rischi e misure di protezione**

Descrizione dei fattori di rischio rilevanti (disponibilità, confidenzialità, integrità, tracciabilità), elenco e valutazione dei rischi, compresi i rischi che hanno un’eventuale rilevanza per il processo di verifica RINA.

L’[analisi dei rischi](https://www.isb.admin.ch/isb/it/home/ikt-vorgaben/prozesse-methoden/p042-informationssicherheits-und-datenschutzkonzept_ISDS.html) dettagliata deve essere effettuata in base al documento Excel allegato al presente piano. Le indicazioni per la compilazione sono contenute nel documento Excel.

Risultati dell’analisi dei rischi:

Nella cartella di lavoro «Matrice dei rischi residui» viene descritta la categoria in cui si trova il rischio residuo valutato.

Verde: rischi inerenti all’oggetto da proteggere in quanto tale oppure che possono essere tralasciati. Tali rischi devono poter essere ridotti al minimo con semplici misure;

giallo: rischi con ripercussioni considerevoli che devono pertanto essere ridotti;

rosso: grandi rischi con ripercussioni critiche o catastrofiche che devono assolutamente essere ridotti.

🡺 I rischi che non vengono ridotti o che vengono ridotti in numero limitato (evidenziati in rosso o in giallo nella matrice dei rischi residui) devono essere indicati nel piano SIPD (capitolo 6.1). I rischi devono essere indicati e comunicati per iscritto al committente e al responsabile dei processi aziendali. La decisione se prendere in considerazione rischi residui noti spetta al responsabile dell’unità amministrativa competente.

I rischi residui devono essere riassunti brevemente anche nel compendio (capitolo 2.2).

## Rischi residui

Inserire in questo punto la griglia della «Matrice dei rischi residui» tratta dall’analisi dei rischi.



Nella tabella seguente si deve inserire una motivazione dei rischi residui (evidenziati in rosso o in giallo).

|  |  |  |
| --- | --- | --- |
| **N.** | **Rischio** | **Motivazione** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Ripristino della capacità operativa

Se un oggetto da proteggere supporta un processo aziendale critico, si deve elaborare un piano d’emergenza in cui viene descritta la pianificazione d’emergenza e la prevenzione dei rischi dell’oggetto informatico da proteggere per mantenere e ripristinare l’operatività in situazioni straordinarie. Al riguardo può essere utile il documento «P042-Hi03 – Vorlage Notfallkonzept»[[2]](#footnote-2) (disponibile in tedesco e francese).

In ogni caso, è necessario creare un rimando ai documenti BCM a livello di Ufficio.

# Osservanza/Verifica/Collaudo delle misure di protezione

Descrizione della regolamentazione per l’esecuzione nell’ambito del progetto o successiva-mente nella fase operativa, di revisioni e verifiche delle attività di sicurezza delle informazioni (comunicate o meno).

## Collaudo del sistema

🡺 Durante i processi di sviluppo è necessario sottoporre i sistemi nuovi e aggiornati a una verifica e controlli approfonditi. Inoltre, i sistemi devono essere oggetto di una pianificazione dettagliata delle attività, dell’esecuzione di test e dei costi attesi in condizioni diverse. Come per i progetti di sviluppo interni, tali verifiche devono essere eseguite dapprima dal team di sviluppo. Successivamente devono essere effettuati collaudi indipendenti (sia nel caso di progetti di sviluppo interni sia per quelli esterni) in modo da garantire che il sistema funzioni solo e soltanto come previsto (cfr. ISO/IEC 27002:2013 capitoli 14.1.1 e 14.1.2). La portata dei controlli dovrebbe essere commisurata all’importanza e alle caratteristiche del sistema.

Riassunto della verifica effettuata (chi, quando, cosa e risultato).

# Disattivazione

Descrizione dei punti da osservare per la disattivazione.

# Abbreviazioni

**Definizioni, acronimi e abbreviazioni**

|  |  |
| --- | --- |
| Termine / Abbreviazione | Significato |
| CPDU | Consulente per la protezione dei dati dell’unità amministrativa |
| CP | Capoprogetto  |
| IFPDT | Incaricato federale della protezione dei dati e della trasparenza |
| ISIU | Incaricato della sicurezza informatica di un’unità amministrativa |
| ISID | Incaricato della sicurezza informatica del Dipartimento |
| WIsB | Istruzioni del Consiglio federale sulla sicurezza TIC nell’Amministrazione federale |
| LPD | Legge federale sulla protezione dei dati |
| NCSC | Centro nazionale per la cibersicurezza |
| OLPD | Ordinanza relativa alla legge federale sulla protezione dei dati |
| Piano SIPD | Piano per la sicurezza dell’informazione e la protezione dei dati |
| RA | Responsabile delle applicazioni |
| RINA | Metodo di gestione del rischio per ridurre lo spionaggio dei servizi di informazione |
| RS | Responsabile dei sistemi |
| RSIPD | Responsabile della sicurezza informatica e della protezione dei dati nel quadro del progetto, secondo HERMES |
| Schuban | Analisi del bisogno di protezione |
| SLA | Service Level Agreement |

# Allegato

Qui vengono allegati altri documenti pertinenti, tra cui:

* P041-Hi01- Analisi del bisogno di protezione
* P042-Hi02- Analisi dei rischi
1. Art. 14*d* cpv. 3 OCiber [↑](#footnote-ref-1)
2. [intranet.ncsc.admin.ch](https://intranet.ncsc.admin.ch/ncscintra/it/home.html), Direttive e ausili > Procedura di sicurezza > Protezione elevata >

P042 - Piano per la sicurezza delle informazioni e la protezione dei dati (piano SIPD) [↑](#footnote-ref-2)