Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

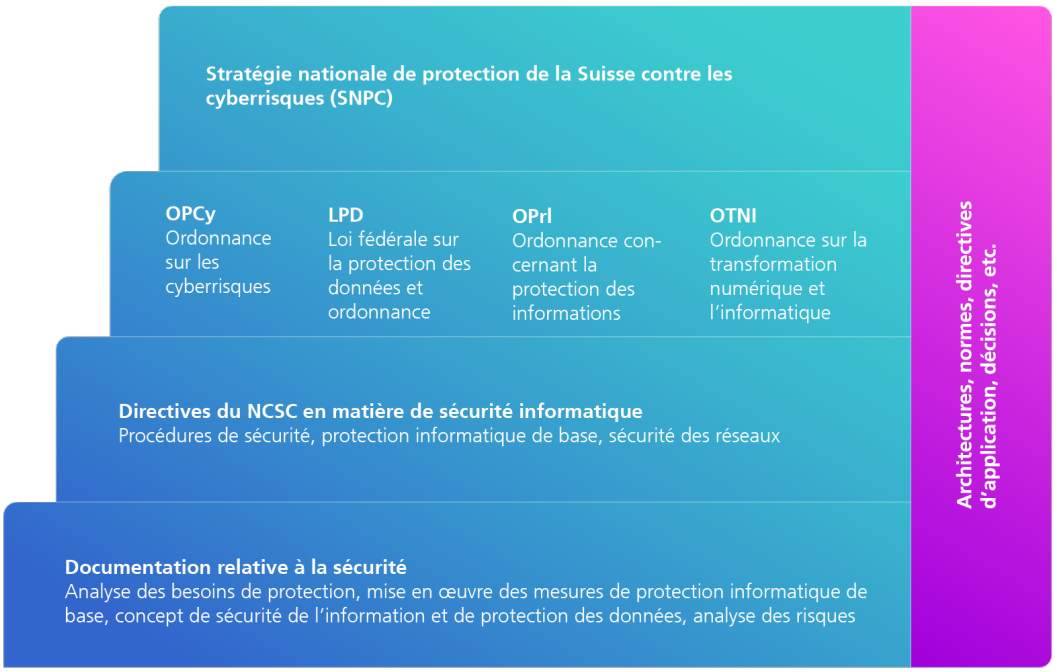
Centre national pour la cybersécurité NCSC
Sécurité informatique de la Confédération SEC

Version 4.5

P042 - Concept de sécurité de l'information et de protection des données (concept SIPD)

du 19 décembre 2013 (état au 1er septembre 2023)

En vertu de l'art. 11, al. 1, let. e, de l'ordonnance du 27 mai 2020 sur les cyberrisques (OPCy), le délégué à la cybersécurité édicte la directive suivante, qui s'applique à la protection accrue conformément à l'art. 14*d* OPCy.



Contenu

1 P042 – Concept SIPD

Si l'analyse révèle des besoins de protection accrus, les unités administratives définissent, en plus de la mise en œuvre des directives en matière de sécurité relevant de la protection de base, d'autres mesures de sécurité sur la base d'une analyse des risques, documentent ces mesures et les mettent en œuvre (art. 14*d*, al. 1, OPCy). Le concept SIPD décrit les mesures de sécurité applicables à un objet informatique à protéger, leur mise en œuvre et les risques résiduels.

S'il y a un traitement de données personnelles qui, selon l'examen préalable des risques[1], présente un risque élevé pour les droits fondamentaux des personnes concernées, le conseiller à la protection des données doit être lui aussi sollicité sur la question. Une analyse d'impact relative à la protection des données personnelles (AIPD) au sens de l'art. 22 LPD doit être réalisée et documentée dans le cadre du concept SIPD. L'AIPD doit s'effectuer selon le guide correspondant[2].

L'établissement du concept SIPD incombe au responsable SIPD (dans le cadre d'un projet) ou au responsable d'application. Le concept SIPD peut faire référence à des concepts de sécurité existants pour des domaines spécifiques. Le NCSC fournit le modèle actuel sous la forme d'un document Word (*P042-Hi01- Concept SIPD*).La mise en œuvre des directives et des mesures de sécurité doit être documentée et vérifiée par les unités administratives concernées (art. 14, al. 3, et 14*d* OPCy).
Les exigences de sécurité doivent être convenues par écrit avec les fournisseurs de prestations en ce qui concerne aussi bien le développement et l'exploitation que la mise hors service de moyens informatiques. Les unités administratives documentent et vérifient la mise en œuvre des mesures de sécurité.

Le concept SIPD doit être contrôlé au moins par le délégué à la sécurité informatique de l'unité administrative (DSIO)[3]. Il doit être approuvé par le mandant et par le responsable du processus d'affaires.

Les unités administratives mettent en évidence les risques qui ne peuvent être réduits ou qui ne peuvent l'être que de manière insuffisante (risques résiduels) et documentent ces risques. Le mandant du projet, le responsable du processus d'affaires et le responsable de l'unité administrative prennent connaissance des risques résiduels et confirment par écrit qu'ils l'ont fait (art. 14*d*, al. 2, OPCy).
La décision d'assumer ou non les risques résiduels connus appartient au responsable de l'unité administrative compétente (art. 14*d*, al. 3, OPCy).

Les aspects suivants au moins doivent être définis dans le concept SIPD:

- Description de l'objet informatique à protéger
- Liste des documents relatifs à la sécurité
- Classification d'après le P041 – Analyse des besoins de protection
- Description du système relative à la sécurité, en particulier: interlocuteurs et responsabilités, description du système global, description des données à traiter, esquisse de l'architecture et matrice de communication, description de la technologie sous-jacente
- Analyse des risques et mesures de sécurité, en particulier: risques qui ne peuvent pas être réduits ou qui ne peuvent l'être que de manière insuffisante (risques résiduels) – *ici les aspects de la confidentialité, de l'intégrité, de la disponibilité et de la traçabilité*

[1] www.bj.admin.ch > État et Citoyen > Protection des données > Informations destinées aux organes fédéraux
[2] www.bj.admin.ch > État et Citoyen > Protection des données > Informations destinées aux organes fédéraux
[3] Pour les services standard, il doit être vérifié par le responsable de la sécurité informatique des services standard.

des données doivent être pris en considération
- Rétablissement des activités – *pour les objets informatiques à protéger qui soutiennent des processus d’affaires critiques*
- Respect, contrôle et approbation des mesures de sécurité, en particulier: contrôle de la réception du système
- Liquidation
- Signatures des personnes suivantes: DSIO, mandant, responsable du processus d’affaires et responsable de l’unité administrative (ou membre de la direction) – *doit avoir lieu avant la mise en service*

D’autres indications peuvent être exigées ou ajoutées au cas par cas.

1.1 Validité du concept SIPD

Le concept SIPD est valable durant cinq ans au maximum.

2 Outils de mise en œuvre du P042

Différents documents doivent être pris en compte et établis lors de l'élaboration du concept SIPD:

- le concept SIPD lui-même;
- l'analyse des risques;
- le plan d'urgence (pour les objets informatiques à protéger qui soutiennent des processus d'affaires critiques*)*;

L'essentiel du traitement de ces documents a lieu de préférence pendant la phase de conception.

Pour chaque document, un modèle est disponible à l'aide duquel les directives peuvent être appliquées correctement. Il est possible d'adapter ces modèles (notamment le contenu) à ses propres besoins et objectifs. Ces modèles doivent être considérés comme des outils aidant à respecter toutes les directives de sécurité. Ils servent de liste de contrôle pour tenir compte de tous les aspects concernant la sécurité. Tous les documents cités doivent être vérifiés en cas de modifications (de l'objet informatique à protéger) et être adaptés si nécessaire. Ils doivent impérativement être révisés après 5 ans au maximum[4].

Cette documentation doit être signée par le DSIO, le mandant, le responsable du processus d'affaires ainsi que le responsable de l'unité administrative (ou un membre de la direction de celle-ci) avant la mise en service.

2.1 P042-Hi01 – Concept SIPD

Le *concept SIPD* constitue le document principal de la sécurité de l'information et de la protection des données dans le projet et pendant l'exploitation. Il définit les informations nécessaires pour le respect et l'amélioration de la sécurité de l'information et de la protection des données. Il récapitule les aspects de la sécurité de l'information et de la protection des données dans le cadre du projet.
Le *concept SIPD* comprend, entre autres, un résumé et une évaluation des risques résiduels connus qui doivent être assumés par les services responsables[5]. Il contient aussi une description des fonctionnalités importantes pour la sécurité du système global. La mise hors service de celui-ci doit aussi être prise en compte.

Le concept SIPD est obligatoire pour les systèmes importants du point de vue de la sécurité. Certains sous-chapitres peuvent toutefois être omis s'ils ne sont pas pertinents.

2.2 P042-Hi02 – Analyse de risque

L'*analyse de risque* comprend une description des facteurs de risques pertinents (disponibilité, confidentialité, intégrité et traçabilité) ainsi que la liste et l'évaluation des risques. Elle donne une image du potentiel de risque du système examiné. S'il y a un traitement de données personnelles qui, selon l'examen préalable des risques, présente un risque élevé pour les droits fondamentaux des personnes concernées, les risques en question doivent être identifiés et évalués soit séparément, soit dans le cadre du concept SIPD. Cette analyse permet également d'évaluer les conséquences.

[4] Art. 14*e* OPCy
[5] Art. 14*d* OPCy

2.3 P042-Hi03 – Plan d’urgence

Selon la mesure 17.1.1 de la protection informatique de base, des plans doivent être développés, documentés et mis en œuvre pour assurer la marche des affaires. Le *plan d’urgence* décrit la planification des cas d’urgence et la prévention des catastrophes afin de garantir le maintien et le rétablissement des activités dans les situations extraordinaires.
Le NCSC fournit aux unités administratives et aux chefs de projet un modèle pour les aider à établir un plan d’urgence.