Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Directives du Conseil fédéral concernant la sécurité informatique dans l'administration fédérale

du 16 janvier 2019

Le Conseil fédéral suisse
édicte les directives suivantes:

1 Dispositions générales

1.1 Objet

Les présentes directives règlent, en exécution de l'art. 14, let. d, de l'ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale (OIAF)[1], les exigences requises ainsi que les mesures à prendre dans les domaines de l'organisation, du personnel et de la technique pour assurer une protection adéquate de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des objets à protéger relevant de l'informatique de l'administration fédérale.

1.2 Champ d'application

Le champ d'application des présentes directives est régi par l'art. 2 OIAF[2].

1.3 Définitions

Au sens des présentes directives, on entend par:

a. *objets informatiques à protéger:* applications, services, systèmes, réseaux, fichiers de données, infrastructures et produits relevant de l'informatique; plusieurs objets identiques ou connexes peuvent être regroupés en un seul objet informatique à protéger;

b. *processus de sécurité:* procédures et mesures visant à assurer une sécurité informatique adéquate durant tout le cycle de vie d'un objet informatique à protéger;

c. *analyse des besoins de protection:* définition des exigences en matière de sécurité des objets informatiques à protéger;

1 RS **172.010.58**
2 RS **172.010.58**

d. *concept de sécurité de l'information et de protection des données (concept SIPD):* description des mesures de protection des objets informatiques à protéger et de leur mise en œuvre ainsi que des risques résiduels;

e. *réseau:* dispositif permettant à différents systèmes informatiques de communiquer entre eux;

f. *zone:* ensemble logique de systèmes informatiques qui se caractérisent par des exigences de sécurité similaires et sont soumis à la même réglementation;

g. *réglementation applicable à la zone:* description, établie par le propriétaire d'une zone, des exigences et prescriptions applicables aux systèmes informatiques de la zone, à la zone elle-même et à la communication interne et externe autorisée pour cette zone;

h. *modèle de zone Confédération:* modèle générique pour la création de zones dans l'administration fédérale;

i. *portefeuille informatique:* liste uniforme des projets informatiques prévus ou en cours ainsi que des applications relevant d'un domaine de compétences déterminé.

2 Compétences

2.1 Délégués à la sécurité informatique

1 Les départements et la Chancellerie fédérale désignent chacun un délégué à la sécurité informatique (DSID).

2 Les DSID ont notamment les tâches suivantes:

a. ils coordonnent les aspects de la sécurité informatique au sein du département ou de la Chancellerie fédérale ainsi qu'avec les services supradépartementaux et sont les premiers interlocuteurs de l'Unité de pilotage informatique de la Confédération (UPIC) dans le cadre de la sécurité informatique;

b. ils élaborent les bases nécessaires pour la mise en œuvre des règles de sécurité informatique et pour l'organisation au niveau du département ou de la Chancellerie fédérale.

3 Les unités administratives désignent chacune un délégué à la sécurité informatique (DSIO).

4 Les DSIO ont notamment les tâches suivantes:

a. ils coordonnent les aspects de la sécurité informatique au sein de l'unité administrative ainsi qu'avec les services départementaux et sont les premiers interlocuteurs des DSID et des organisations de sécurité des fournisseurs de prestations;

b. ils élaborent les bases nécessaires à la mise en œuvre des règles de sécurité informatique et à l'organisation au niveau de l'unité administrative.

c. ils informent le responsable de leur unité administrative au moins tous les six mois de l'état de la sécurité informatique dans leur unité administrative.

5 Les départements, la Chancellerie fédérale et les unités administratives veillent à ce que les DSIO accomplissent leurs tâches sans conflits d'intérêts. Ils règlent les relations entre le DSID et le DSIO, notamment la conduite technique en matière de sécurité.

6 L'UPIC désigne un délégué à la sécurité informatique des services standard. Celui-ci assume les tâches visées à l'al. 4 pour les services informatiques standard.

2.2 Bénéficiaires de prestations

1 En tant que bénéficiaires de prestations, les unités administratives veillent à l'application du processus de sécurité.

2 Les responsables d'une application, d'un processus d'affaires ou d'un fichier de données au sein d'une unité administrative fixent, en accord avec le DSIO, les exigences de sécurité applicables aux objets informatiques à protéger. Les unités administratives gèrent un portefeuille informatique contenant les informations relatives à la sécurité. 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 contrôlent la mise en œuvre des mesures de sécurité ainsi que leur efficacité.

3 Les unités administratives vérifient régulièrement les besoins de protection des objets informatiques à protéger et adaptent aussi bien les documentations concernant la sécurité que les mesures de sécurité.

4 Elles veillent à ce que les collaborateurs connaissent, au niveau qui les concerne et selon leur fonction, les compétences ainsi que les procédures applicables en matière de sécurité informatique dans leur environnement de travail.

5 Les collaborateurs de l'administration fédérale qui utilisent des moyens informatiques sont responsables de la sécurité lors de leur utilisation. Les unités administratives doivent les sensibiliser et les former aux enjeux de la sécurité informatique à leur entrée en fonction puis à intervalles réguliers.

6 Les unités administratives veillent à ce que les personnes non soumises à l'OIAF[3] ne puissent avoir accès à l'infrastructure informatique de la Confédération que s'ils s'engagent à respecter les règles de sécurité informatique.

7 Elles édictent, avec l'aide du DSIO ou du DSID, des règles supplémentaires ou spécifiques pour l'utilisation sécurisée des moyens informatiques et les mettent à jour régulièrement; elles définissent notamment une procédure de traitement des incidents informatiques.

3 RS **172.010.58**

2.3 Fournisseurs de prestations

1 Les exigences définies pour les bénéficiaires de prestations visés au ch. 2.2 s'appliquent par analogie aux fournisseurs de prestations.

2 Les fournisseurs de prestations mettent en œuvre les mesures de sécurité nécessaires lors de l'exploitation des moyens informatiques, les documentent et les contrôlent. Ils transmettent les résultats aux bénéficiaires de prestations sous une forme appropriée.

3 Les responsabilités et les besoins de protection au niveau opérationnel doivent être décrits dans les accords de projets et les conventions de prestations passés entre les fournisseurs et les bénéficiaires de prestations. Doivent en particulier être réglées les compétences décisionnelles concernant les mesures d'urgence à prendre en cas d'incident.

4 Les fournisseurs de prestations veillent à pouvoir gérer rapidement et efficacement les incidents informatiques avec des organisations de sécurité permanentes ou ad hoc. Celles-ci sont chargées d'effectuer l'analyse technique des incidents et de coordonner leur résolution. Elles collectent les informations techniques, les analysent en tenant compte d'éventuels événements similaires et informent le DSID ou le DSIO compétent.

3 Processus de sécurité

3.1 Règles de sécurité

1 En complément des présentes directives, l'UPIC édicte les règles concernant le processus de sécurité et les instruments correspondants au niveau de la Confédération, notamment:

a. pour l'analyse des besoins de protection;

b. pour un processus d'audit visant à réduire les activités menées par des services de renseignement;

c. pour la protection informatique de base;

d. pour le concept SIPD.

2 Elle définit le modèle de zone Confédération.

3.2 Analyse des besoins de protection, concept SIPD et évaluation des risques

1 Tout projet informatique doit faire l'objet d'une analyse préalable des besoins de protection. Les cas à risques devront également être identifiés dans ce cadre, conformément au processus d'audit visant à réduire les activités menées par des services de renseignement (ch. 3.1, al. 1, let. b).

2 Pour les objets informatiques existants, une analyse valable des besoins de protection doit être disponible.

3 Les règles de sécurité minimales (protection informatique de base) doivent être mises en œuvre pour tous les objets informatiques à protéger; la mise en œuvre doit être documentée.

4 Si l'analyse révèle des besoins de protection élevés, un concept SIPD comprenant une analyse des risques doit être élaboré en plus de la documentation de la mise en œuvre de la protection informatique de base. Lors de l'élaboration du concept SIPD, il peut être fait référence à des concepts de sécurité existants pour des domaines spécifiques.

5 Si des cas à risques sont identifiés selon le processus d'audit visant à réduire les activités menées par des services de renseignement, le processus d'audit doit être mené à terme; la mise en œuvre doit être documentée.

6 Les analyses des besoins de protection, la documentation de la mise en œuvre de la protection informatique de base, la documentation du processus d'audit visant à réduire les activités menées par des services de renseignement et les concepts SIPD doivent être vérifiés au moins par le DSIO ou, le cas échéant, par le délégué à la sécurité informatique des services standard. Ils doivent être autorisés par le mandant et par le responsable du processus d'affaires.

7 Si le processus d'audit visant à réduire les activités menées par des services de renseignement révèle que la fourniture d'une prestation informatique est en lien avec d'autres processus informatiques et que cela constitue une menace potentielle, les unités administratives compétentes en informent l'UPIC.

8 Si une unité administrative souhaite utiliser de nouvelles technologies de l'information et de la communication (matériel et logiciels) ou des technologies existantes dans un nouveau domaine d'application, elle doit les soumettre préalablement à une évaluation des risques. Le résultat de cette évaluation doit être transmis au délégué à la sécurité informatique compétent et à l'UPIC.

9 Les documentations concernant la sécurité ont une durée de validité maximale de cinq ans. Si l'objet informatique à protéger ou la situation en matière de menace subissent des modifications ayant une incidence sur la sécurité, elles doivent être mises à jour dans les plus brefs délais.

3.3 Normes internationales

Les mesures de sécurité informatique se fondent sur les normes internationales en vigueur, notamment les normes ISO concernant les processus de sécurité informatique.

3.4 Risques résiduels

1 Les risques qui ne peuvent être réduits, ou seulement de manière insuffisante (risques résiduels), doivent être mis en évidence et communiqués par écrit au mandant, au responsable du processus d'affaires et au responsable de l'unité administrative.

2 La décision d'assumer ou non les risques résiduels connus appartient au responsable de l'unité administrative compétente.

3.5 Coûts

Les coûts de la sécurité informatique font partie des coûts de projet et d'exploitation. Ils doivent être suffisamment pris en compte lors de la planification.

4 Sécurité des réseaux. Compétences et règles de sécurité

1 Seules des zones conformes au modèle de zones de la Confédération et autorisées par l'UPIC peuvent être créées et exploitées dans l'administration fédérale.

2 L'UPIC établit une liste de toutes les zones autorisées. Sur cette liste figurent notamment:

a. le nom de la zone;

b. le nom du propriétaire de la zone;

c. la référence à la réglementation applicable à la zone;

d. l'exploitant de la zone.

3 Toutes les zones doivent disposer de leur réglementation propre. Cette réglementation requiert l'approbation de l'UPIC.

4 L'UPIC édicte les règles supplémentaires concernant la sécurité des réseaux.

5 Dispositions finales

5.1 Abrogation d'autres directives

Les directives du Conseil fédéral du 1er juillet 2015 concernant la sécurité des TIC dans l'administration fédérale[4] sont abrogées.

5.2 Dispositions transitoires

1 Les analyses des besoins de protection et les concepts SIPD antérieurs à l'entrée en vigueur des présentes directives conservent leur validité et doivent être actualisés lors de vérifications et de révisions.

2 Les processus de sécurité et d'audit visant à réduire les activités menées par des services de renseignement, prévus au ch. 3.2, al. 1, 5, 6 et 7, ne sont pas applicables aux projets informatiques pour lesquels un mandat d'initialisation a été émis avant le 1er janvier 2016. Les unités administratives compétentes et leurs fournisseurs de prestations doivent avoir vérifié au 1er janvier 2021 au plus tard tous les objets

4 FF **2015** 5313

informatiques à protéger qui étaient déjà dans une phase HERMES[5] ou en exploitation au 1er janvier 2016.

3 Les zones qui, à l'entrée en vigueur des présentes directives, remplissent les conditions prévues au ch. 4, al. 1, et disposent d'une réglementation[6] approuvée par l'UPIC selon le ch. 4, al. 3, peuvent continuer d'être exploitées avec leur autorisation dérogatoire.

4 Les réseaux qui, à l'entrée en vigueur des présentes directives, sont en service et ne font pas partie d'une zone qui remplit les conditions prévues au ch. 4, al. 1, peuvent continuer d'être exploités mais doivent être transférés dans une zone qui remplit les conditions prévues au ch. 4, al. 1, lors du prochain réaménagement, au plus tard dans un délai de dix ans à compter de l'entrée en vigueur des présentes directives.

5.3 Entrée en vigueur

Les présentes directives entrent en vigueur le 15 février 2019.

16 janvier 2019

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ueli Maurer
Le chancelier de la Confédération, Walter Thurnherr

5 www.hermes.admin.ch
6 Sont visés ici le domaine de réseau bleu, la *Shared Service Zone* (SSZ), la *Central Access Zone* (CAZ), le réseau AVS/AI et le domaine de réseau *Law Enforcement Monitoring Facility* (LEMF).