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

du 1er juillet 2015

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, de la technique et de la construction 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;

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;

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;

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

f. *domaine de réseau*: ensemble logique de toutes les connexions et de toutes les composantes d'un réseau;

g. *réglementation applicable au domaine de réseau*: réglementation des conditions de connexion et des exigences relatives à la communication entre différents réseaux et systèmes.

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;

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.

[5] Les départements, la Chancellerie fédérale et les unités administratives veillent à ce que les délégués de la sécurité informatique accomplissent leurs tâches sans conflits d'intérêts.

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 des informations relatives à la sécurité. Les exigences de sécurité doivent être convenues par écrit avec les fournisseurs de prestations aussi bien en ce qui concerne le développement et l'exploitation que la mise hors service de moyens informatiques. Les unités admi-

nistratives 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 et adaptent les mesures de sécurité en conséquence.

4 Elles veillent à ce que les collaborateurs connaissent, au niveau qui les concerne, 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 ou font exploiter des moyens informatiques sont responsables de la sécurité lors de leur utilisation. Les unités administratives doivent les sensibiliser et les former aux thèmes de la sécurité informatique lors de leur entrée en fonction et à intervalles réguliers par la suite.

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.

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 sont décrits dans les accords de projets et les conventions de prestations passés entre les fournisseurs et les bénéficiaires de prestations.

3 Processus de sécurité

3.1 Règles de sécurité

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 pour:

a. l'analyse des besoins de protection;

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

c. la protection de base;

d. le concept SIPD.

3 RS **172.010.58**

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, 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 de base) doivent être mises en œuvre pour tous les objets à protéger ; la mise en œuvre doit être documentée.

4 Si l'analyse révèle des besoins de protection élevés, un concept SIPD doit être élaboré en plus de la protection 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, les règles de sécurité supplémentaires, 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 et 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.

3.3 Normes internationales

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

3.4 Risques résiduels

1 Les risques qui ne peuvent être totalement éliminés (risques résiduels) doivent être mis en évidence et communiqués par écrit au mandant et au responsable du processus d'affaires.

2 La décision d'assumer ou non les risques résiduels connus appartient au chef 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 L'UPIC établit une liste de tous les domaines de réseau exploités pour les unités administratives. Sur cette liste figurent notamment:

a. le nom du domaine de réseau;

b. le nom du propriétaire du domaine de réseau;

c. la référence à la réglementation applicable au domaine de réseau;

d. les accords conclus entre les domaines de réseau et d'autres domaines de réseau.

2 Tous les domaines de réseau doivent disposer de leur propre réglementation applicable au domaine de réseau. Cette réglementation requiert l'approbation de l'UPIC.

3 Les conventions conclues en matière de domaines de réseau entre les unités administratives de la Confédération ou entre des unités administratives de la Confédération et des tiers requièrent l'approbation de l'UPIC.

4 Si des tiers sont directement connectés à un domaine de réseau de la Confédération, l'unité administrative compétente doit régler au moyen d'une convention le respect des règles de sécurité informatique selon les présentes directives et vérifier régulièrement le respect de ces règles. Les conventions requièrent l'approbation de l'UPIC.

5 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 14 août 2013 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 directives du Conseil fédéral du 14 août 2013 concernant la sécurité des TIC dans l'administration fédérale[5] conservent leur validité et doivent être actualisés lors de vérifications et de révisions.

4 FF **2013** 6003
5 FF **2013** 6003

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, sont applicables à tous les projets pour lesquels un mandat d'initialisation est émis dès l'entrée en vigueur des présentes directives. Les unités administratives compétentes et leurs fournisseurs de prestations doivent vérifier dans un délai de cinq ans tous les objets informatiques à protéger qui sont dans une phase HERMES[6] ou en exploitation lors de l'entrée en vigueur des présentes directives.

5.3 Entrée en vigueur

Les présentes directives entrent en vigueur le 1er janvier 2016.

1er juillet 2015 Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Simonetta Sommaruga
La chancelière de la Confédération, Corina Casanova

6 www.hermes.admin.ch