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 5.0

Si001 – Protection informatique de base dans l'administration fédérale

du 1er mars 2022

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 sur la protection informatique de base dans l'administration fédérale.

La directive Si003 – Sécurité des réseaux dans l'administration fédérale, version 3.1 du 19 décembre 2013 (état au 1er avril 2021), est abrogée à l'entrée en vigueur du présent document.

Illustration 1: Résumé des bases de la sécurité informatique

Table des matières

1 Dispositions générales

1.1 Objet

[1] La présente directive définit les exigences minimales de la sécurité informatique de l'administration fédérale sur les plans de l'organisation, du personnel et de la technique ainsi que les objets informatiques à protéger (objets à protéger) dans le cadre de l'art. 14, al. 2, OPCy.

[2] Chaque unité administrative (UA) est responsable de ses propres objets à protéger. Elle doit mettre en œuvre et respecter la présente directive, et contrôler sa mise en œuvre et son respect.

[3] L'UA responsable doit documenter de manière compréhensible la mise en œuvre et le respect de la présente directive (par ex. sur la base de [Si001-Hi01]). Cette documentation doit être contrôlée et signée au moins par:

a) le responsable de l'objet à protéger (selon ch. 2, al. 1);
b) le délégué à la sécurité informatique de l'UA responsable (DSIO);
c) le mandant (d'un projet), et
d) le responsable du processus d'affaires.

En outre, les signataires confirment que, selon leur évaluation, tous les fournisseurs de prestations (FP) participant à l'exploitation de l'objet à protéger répondent aux exigences les concernant.

[4] L'UA responsable doit également documenter de manière compréhensible le contrôle de la mise en œuvre et du respect de la présente directive. La façon dont ce contrôle est exécuté dépend de l'objet à protéger et de son besoin de protection. Elle doit être convenue et documentée avec le DSIO. Si un objet à protéger est exploité par un ou plusieurs FP internes sur mandat de l'UA responsable, le contrôle est réputé réalisé lorsque les FP correspondants ont cosigné le document «Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale».

1.2 Champ d'application et cadre juridique

[1] Le champ d'application de la présente directive est régi par l'art. 2 OPCy.

[2] Le cadre juridique découle également de:

a) l'ordonnance concernant la protection des informations (OPrI) et des directives concernant les prescriptions de traitement détaillées relatives à la protection des informations (directives de traitement);
b) la loi fédérale sur la protection des données (LPD), pour ce qui est de la gestion des données personnelles;
c) la loi fédérale sur l'archivage (LAr), pour ce qui est de l'archivage des données.

1.3 Dérogations

[1] Lorsqu'une UA ne peut pas remplir une ou plusieurs exigences de la présente directive pour un objet à protéger, elle doit demander une dérogation visée à l'art. 11, al. 1, let. f, OPCy selon l'une des trois méthodes exposées aux al. 2 à 4 ci-après.

[2] Les exigences signalées par un astérisque (*) au ch. 4 comportent moins de risques du

point de vue de la sécurité informatique de l'administration fédérale. Elles peuvent faire l'objet de dérogations si celles-ci sont justifiées et consignées dans le document «Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale» ou dans le concept de sécurité de l'information et de protection des données (SIPD). La dérogation est alors réputée approuvée par les responsables énoncés au ch. 1.1, al. 3.

[3] Un délégué à la sécurité informatique du département (DSID) peut approuver une demande formelle de dérogation ou déléguer cette compétence au DSIO de l'UA responsable lorsque les conditions suivantes sont réunies (cumulativement):

a) Le DSID est tellement impliqué dans le processus d'octroi d'une dérogation qu'il peut assumer cette responsabilité.
b) La dérogation porte exclusivement sur l'utilisation d'informations de l'UA responsable ou sur d'autres objets à protéger qui n'ont aucun besoin de protection accru ou qui présentent un tel besoin en raison des seules exigences relatives à la protection des données.
c) La dérogation ne concerne ni des services informatiques standard ni une autre UA.
e) Toutes les personnes énoncées au ch. 1.1, al. 3, et le responsable de l'UA ou un membre de sa direction sont manifestement d'accord avec la dérogation.
d) Le DSID tient à jour un registre des dérogations accordées et le communique au Centre national pour la cybersécurité (NCSC) à sa demande.

[4] Toutes les autres demandes de dérogation peuvent être soumises au NCSC conformément à la gestion des exigences et des directives concernant l'informatique de l'administration fédérale (P035). Elles doivent justifier les dérogations à la protection informatique de base et présenter de manière détaillée les mesures éventuelles et prévues pour réduire les risques.

[5] Les dérogations visées à l'al. 4 sont toujours limitées dans le temps (en général, deux ans).

2 Définitions

[1] L'expression «**objet informatique à protéger (objet à protéger)**» est définie dans l'OPCy. Un objet à protéger est utilisé au sein ou sur mandat de l'administration fédérale; il doit être protégé conformément à son besoin de protection et fait l'objet de la présente directive[1]. Un responsable doit être désigné pour chaque objet à protéger. Pour les applications, il s'agit du responsable d'application, conformément à la description des rôles des processus informatiques de l'administration fédérale[2]. Le terme «responsable de l'objet à protéger» se réfère toutefois à tous les objets à protéger et constitue dès lors une généralisation.

[2] De plus, les définitions suivantes s'appliquent dans la présente directive:

a) **Analyse des besoins de protection:** méthode structurée visant à déterminer le besoin de protection d'un objet à protéger. Ce faisant, on opère une distinction entre une protection de base et un besoin de protection accru.
b) **Concept de sécurité de l'information et de protection des données (SIPD):** description structurée des exigences de sécurité d'un objet à protéger, des mesures de sécurité prévues et mises en œuvre ainsi que des risques résiduels.

[1] Plusieurs moyens informatiques peuvent être regroupés en un objet à protéger s'ils sont étroitement liés du point de vue du contenu et présentent le même besoin de protection.
[2] https://intranet.dti.bk.admin.ch/isb_kp/fr/home/ikt-vorgaben/prozesse-methoden/p000-informatikprozesse_in_der_bundesverwaltung.html

c) **Informations:** données enregistrées, traitées ou transmises par voie électronique[3]. Si les données se réfèrent à une personne identifiée ou identifiable, il s'agit alors de **données personnelles** au sens de la LPD.

d) **Système informatique (système):** système technique d'information qui est exploité comme un logiciel (système) sur un matériel dédié ou virtualisé, ou une machine virtuelle[4]. Dans le deuxième cas, on parle de système informatique virtualisé.

e) Un système informatique est[5]:

- un **système serveur** lorsqu'il fournit avant tout des prestations informatiques;
- un **système client** lorsqu'il bénéficie avant tout de prestations informatiques;
- un **ordinateur client de l'administration fédérale** lorsqu'il est un système client géré au sein du service standard Bureautique. Il peut s'agir soit d'un système de poste de travail (SPT), soit d'un système client virtualisé qui fonctionne sur un appareil électronique (*smart device*), dans une *sandbox* comportant une gestion des appareils mobiles (*mobile device management*, MDM) selon [E021] (système MDM);
- un **périphérique** lorsqu'il étend les fonctions d'autres systèmes informatiques et doit, pour ce faire, être intégré ou installé (pilote; par ex. imprimantes, appareils multifonctions ou systèmes de présentation dans les salles de conférence);
- un **appareil de mesure** lorsque sa tâche principale consiste à transmettre à un autre système informatique les valeurs de mesure[6] d'un capteur situé sur le lieu de mesurage par l'intermédiaire d'une connexion dédiée qui n'est pas utilisable à d'autres fins. Le système informatique de destination peut soit se contenter de collecter les valeurs et de les compiler, soit les analyser et les traiter. La communication peut être bilatérale et aussi permettre, par exemple, de transmettre des commandes à l'appareil de mesure. Les appareils de mesure sont surtout utilisés dans les applications de l'Internet des objets (IdO);
- un **élément du réseau** lorsqu'il sert principalement à transporter des données entre des systèmes informatiques tels que des commutateurs, des routeurs ou des filtres de paquets statiques simples (pare-feu IP). Dans le modèle de référence OSI (*open systems interconnection*), les éléments du réseau évoluent jusqu'à la couche 5 (couche session), y compris celle-ci;
- un **point d'application des règles ou *policy enforcement point* (PEP)** lorsqu'il sert principalement à mettre en œuvre des règles (provenant de politiques). Exemples: filtres de paquets dynamiques, gateway (passerelles) pour protocoles d'application, serveurs proxy et proxy inverse. Dans le modèle de référence OSI, les PEP évoluent jusqu'à la couche 7 (couche application), y compris celle-ci, et vérifient dès lors également le(s) protocole(s) de communication transmis.

[3] D'après le message concernant la nouvelle LPD, le terme «informations» est employé de manière générique pour désigner les «informations et données». On parle de données uniquement lorsqu'il s'agit des données personnelles au sens de la protection des données.

[4] Le système informatique qui met à disposition le matériel virtualisé ou la machine virtuelle (hyperviseur) est lui aussi un logiciel et constitue donc un système informatique autonome.

[5] La distinction entre un système client et un système serveur est floue, car un système informatique peut être à la fois un système client et un système serveur.

[6] Ces valeurs de mesure peuvent également être des signaux acoustiques et/ou optiques.

f) **Application:** logiciel d'application utilisé sur les systèmes informatiques d'une ou de plusieurs UA pour exécuter des processus d'affaires. Les applications de l'IdO se distinguent des autres applications principalement par le fait que les informations utilisées proviennent surtout d'appareils de mesure.

g) **Réseau:** dispositif technique (composé principalement d'éléments du réseau et de connexions) servant à échanger des données entre des systèmes informatiques.

h) **Segment de réseau (segment):** partie d'un réseau qui – pour des raisons d'équilibrage de charges et/ou de sécurité – est généralement séparée du reste du réseau au moyen d'éléments du réseau.

i) **Zone:** regroupement logique de systèmes informatiques qui présentent des exigences de sécurité similaires et sont soumis à la même réglementation (*policy*) de zone. En particulier, une zone n'est pas limitée à un périmètre précis (par ex. un centre de calcul). Le raccordement au niveau réseau des éléments d'une zone est réalisé grâce aux éléments du réseau, tandis que l'application de la réglementation de zone relève des PEP.

j) **Sous-zone:** une zone peut être subdivisée en sous-zones si la réglementation correspondante le prévoit. Chaque sous-zone constitue une zone. En particulier, toute sous-zone doit avoir une réglementation qui peut uniquement préciser celle de la zone supérieure; en d'autres termes, la réglementation de la sous-zone ne peut contenir que des exigences ou prescriptions supplémentaires (tout assouplissement est proscrit). Une sous-zone peut être subdivisée en sous-zones supplémentaires, mais uniquement en cas d'absolue nécessité.

k) **Réglementation de zone:** elle décrit de manière structurée les exigences et les prescriptions relatives
   - aux systèmes informatiques exploités dans la zone,
   - à la zone elle-même (par ex. peut-elle être segmentée sur le réseau et, si oui, comment?),
   - à l'authentification des personnes et des processus automatisés qui accèdent aux applications et aux systèmes informatiques exploités dans la zone, et
   - à la communication interne (pouvant dépasser le cadre du segment) et externe (pouvant dépasser le cadre de la zone d'application des règles [*policy enforcement zone*, PEZ]) autorisée pour la zone, c'est-à-dire les communications entrantes et sortantes admises[7].Une communication entre deux ou plusieurs zones similaires[8] est considérée comme interne si les interfaces entre les zones sont conformes aux réglementations (*policy*) correspondantes et sont contrôlées par la PEZ commune.

l) **Modèle de zones de la Confédération:** modèle générique pour la création de zones dans l'administration fédérale (cf. annexe A).

[7] Une communication est sortante lorsque l'échange de données correspondant est initié par un système informatique de la zone en question. Dès lors, elle est entrante lorsque l'échange de données a certes été initié par un système informatique situé hors de la zone, mais s'adresse à un système informatique se trouvant dans cette dernière. Dans les deux cas, les données peuvent être échangées dans les deux directions.

[8] Ces zones peuvent également avoir des propriétaires différents.

3 Principes

[1] **Forme de la fourniture de prestations:** la protection informatique de base s'applique à tous les objets à protéger, indépendamment de la forme de la fourniture de prestations. En d'autres termes, les exigences et mesures de sécurité relatives au FP doivent être mises en œuvre par les FP tant internes qu'externes. En cas de FP externes, il faut en particulier veiller au respect des directives relatives à la sécurité informatique[9] et à l'obtention de l'autorisation correspondante de l'autorité supérieure, conformément aux processus spécifiques à un office ou à un département (cf. [Si001-Hi04]).

[2] **Virtualisation:** la protection informatique de base s'applique indépendamment du fait qu'un objet à protéger soit exploité sur du matériel dédié ou de manière virtualisée sur du matériel utilisé conjointement. Concernant le besoin de protection accru, l'usage d'éventuelles technologies et solutions de virtualisation doit être justifié et documenté dans le concept SIPD.

[3] **Principe «Zero Trust»:** dans la mesure du possible, le dispositif de sécurité d'un objet à protéger devrait être conçu de manière à ce que les exigences de sécurité énoncées au ch. 4 puissent être satisfaites en toute autonomie et à ce que l'objet soit isolé de son environnement, de sorte qu'il faille faire le moins d'hypothèses possibles sur la sécurité de ce dernier. Sont exclus du principe «Zero Trust» les services ayant un caractère général (par ex. services Single Sign-On [SSO] dans le cadre du service informatique standard Gestion des identités et des accès). Dans ce cas, les risques doivent être clairement identifiés et gérés dans le cadre d'une gestion globale des risques.

[4] **Principe «Defense in Depth»:** lorsque cela est possible et économiquement justifiable, un objet à protéger doit être sécurisé par plusieurs mesures de sécurité additionnelles qui se complètent mutuellement afin que le respect des exigences de sécurité soit redondant. Ces mesures de sécurité doivent avoir globalement un effet préventif, détecteur et réactif.

[5] **État de la technique:** toutes les mesures de sécurité (préventives, détectrices et/ou réactives) utilisées doivent correspondre à l'état de la technique[10], être standardisées dans l'idéal et avoir fait leurs preuves sur le plan opérationnel. Les mesures obsolètes ou dont on connaît les vulnérabilités ou les faiblesses doivent être améliorées ou remplacées rapidement et indépendamment du cycle de vie.

[6] **Principe «Least Privilege» ou «Need to Know»:** l'octroi de droits d'accès et de privilèges doit se limiter au strict minimum. Cela s'applique par exemple aux utilisateurs des systèmes informatiques et des applications[11], aux services et aux fonctionnalités complémentaires (*features*) qui sont activés dans ces systèmes et applications, ainsi qu'aux communications autorisées dans le cadre des réglementations (*policies*) de zone[12].

[8] **Principe «Security by Design»:** la sécurité doit être prise en compte dès le début du développement des composants matériels et logiciels ou de leur utilisation dans des systèmes informatiques et des applications. Elle doit être mise à jour afin que ces systèmes et applications ne présentent, dans la mesure du possible, aucune vulnérabilité ou faiblesse et que les possibilités d'attaque demeurent à un faible niveau.

---

9 Par exemple, le respect des directives relatives à la sécurité informatique peut être défini contractuellement et/ou garanti par des examens et certificats correspondants.

10 Concernant la cryptographie, la considération technologique « Recommandations de sécurité informatique pour la protection de base - Procédés cryptographiques: algorithmes et protocoles» de la Base d'aide au commandement (BAC) COE CRYPT fournit des renseignements sur l'état de la technique.

11 Dans l'idéal, un concept de rôles sera élaboré pour l'octroi des droits d'accès aux utilisateurs (dans le cadre d'un contrôle des accès fondés sur les rôles).

12 Les protocoles de communication sont admis uniquement s'ils sont nécessaires à l'exploitation.

[9] **Principe «Security by Default»:** les objets à protéger doivent être développés, configurés et exploités de telle sorte que toutes les mesures de sécurité judicieuses dans un environnement spécifique soient activées par défaut et puissent déployer leurs effets sans que les utilisateurs n'aient à s'en occuper.

[10] **Neutralité par rapport au produit:** les directives et recommandations du NCSC sont neutres par rapport au produit. Des déclarations favorables ou défavorables à l'usage de certains produits sont formulées uniquement lorsqu'elles concernent un service informatique standard[13] ou lorsqu'il existe d'autres motifs impérieux pour la sécurité informatique.

4 Exigences en matière de sécurité

[1] Les principes énoncés au ch. 3 doivent être pris en compte pour chaque objet à protéger et les exigences en matière de sécurité visées à l'al. 2, respectées. Ces exigences sont en partie reprises de la norme ISO/IEC 27002:2013 et structurées selon la norme ISO/IEC DIS 27002[14].

[2] Les exigences en matière de sécurité qui concernent l'organisation (O), le personnel (P), la technique (T) et les informations (I) doivent toujours être respectées, tandis que les exigences relatives aux systèmes informatiques (S), aux applications (A) et aux zones (Z) doivent l'être uniquement lorsque des objets à protéger correspondants sont utilisés.

Organisation	
O1	Responsabilité Une personne (au sein de l'UA responsable) doit être nommée responsable de l'objet à protéger. Compétente pour mettre en œuvre la présente directive, elle doit avoir conscience de ses responsabilités et disposer de connaissances techniques suffisantes pour les assumer.
O2	Documentation O2.1 Une documentation à jour, harmonisée avec celle des FP participants, doit être disponible pour l'objet à protéger. Elle doit couvrir toute la durée de vie (cycle de vie) de l'objet, et notamment: a) la chaîne d'approvisionnement (*supply chain*); b) les mesures de protection physiques, la nécessité de mesures techniques et architecturales pour protéger physiquement les systèmes informatiques devant être définie aux endroits requis avec l'Office fédéral des constructions et de la logistique (OFCL), armasuisse ou le Service fédéral de sécurité; c) les éléments, les fonctions et les paramètres importants pour la sécurité;

[13] Par exemple, dans le domaine de la cryptographie asymétrique, on utilisera de préférence des certificats émis par la Swiss Government PKI (SG-PKI) et, pour le cryptage des fichiers classés CONFIDENTIEL sur les SPT, le logiciel de chiffrement de l'administration fédérale (couche 1).

[14] Contrairement à la norme ISO/IEC 27002:2013, le présent document opère une distinction entre les contrôles organisationnels (section 5), personnels (section 6), physiques (section 7) et techniques (section 8). La correspondance entre les contrôles issus de la norme ISO/IEC DIS 27002 et ceux provenant de la norme ISO/IEC 27002:2013 est récapitulée à l'annexe B de la norme ISO/IEC DIS 27002.

	d) la gestion des clés lors de l'emploi de procédés cryptographiques; e) les modalités et les processus en cas de modification (dans le cadre de la gestion des changements), de réparation, d'élimination et de perte; f) les accords contractuels, et g) les processus et activités d'audit[15] destinés à contrôler la mise en œuvre et le respect de la présente directive. O2.2 Lorsque l'objet à protéger (système informatique ou application) n'est pas exploité dans une zone de l'administration fédérale (par ex. sur un nuage public), la documentation doit préciser: a) comment le besoin de protection de l'objet peut être satisfait dans cet environnement, et b) les mesures de sécurité complémentaires garantissant que cette situation n'engendre ni menace ni risque supplémentaires pour les autres objets à protéger de l'administration fédérale.
O3	Continuité de l'activité Concernant l'objet à protéger, la continuité de l'activité doit être garantie et documentée dans le cadre d'un processus de gestion de la continuité des services informatiques (IT Service Continuity Management, ITSCM) ou de gestion de la continuité de l'activité (Business Continuity Management, BCM), conformément au besoin identifié lors de l'analyse des besoins de protection.
O4	Cyberincidents L'objet à protéger doit faire partie du processus de gestion des cyberincidents[16]. En cas d'incidents majeurs, les travaux sont coordonnés par le NCSC.
Personnel	
P1	Sensibilisation et formation P1.1 Tous les utilisateurs de l'objet à protéger doivent être formés et sensibilisés à la sécurité informatique selon leur niveau de responsabilité et leur fonction. P1.2 Tous les utilisateurs de l'objet à protéger doivent connaître les directives d'application importantes pour celui-ci et s'engager à les respecter[17].
P2	Obligation d'annonce Tous les utilisateurs de l'objet à protéger doivent signaler aussi rapidement que possible au service compétent (par ex. Service Desk du FP) les événements

[15] Les processus et activités d'audit doivent être exécutés par un organe indépendant et conçus de telle sorte que la disponibilité des objets à protéger soit affectée le moins possible (en d'autres termes, les dysfonctionnements et les interruptions d'exploitation doivent être aussi limités que possible).

[16] https://intranet.ncsc.admin.ch/dam/ncscintra/de/dokumente/partner/20210217-Bewaeltigung_Cybervorfaelle.pdf.download.pdf/20210217-Bewaeltigung_Cybervorfaelle.pdf

[17] Cela s'applique en particulier à l'utilisation de systèmes MDM et/ou de périphériques privés lors du travail mobile. Une liste des directives d'application est disponible à l'adresse: https://intranet.dti.bk.admin.ch/isb_kp/fr/home/ikt-vorgaben/einsatzrichtlinien.html.

	critiques en matière de sécurité tels qu'un comportement anormal ou douteux du système ou une perte physique.
Technique	
T1	Exploitation L'objet à protéger doit être exploité conformément à l'état de la technique, en tenant compte des directives et recommandations de sécurité usuelles de la branche (meilleures pratiques).
T2	Configuration et paramétrage T2.1 Avant sa première mise en service, l'objet à protéger doit être configuré et paramétré de façon à: a) être protégé contre un accès non autorisé; b) être renforcé, si cela est techniquement possible, et être exploité dans une configuration minimale nécessaire à l'accomplissement des tâches qui ne peut pas être modifiée par un utilisateur (en d'autres termes, les interfaces, modules et fonctions non utilisés doivent être désactivés), et c) permettre un enregistrement et une évaluation rapide des activités et événements importants pour la sécurité (avec horodatage). T2.2 L'activation, la modification, la désactivation et la désinstallation des configurations et des paramètres de sécurité requièrent une autorisation.
T3	Environnement de production L'environnement de production de l'objet à protéger doit être séparé des autres environnements éventuels (par ex. destinés au développement et/ou aux tests). En cas de séparation logique, les dispositifs et mesures de sécurité correspondants doivent être justifiés et documentés.
T4	Faiblesses et vulnérabilités Il faut rechercher régulièrement et, de préférence, automatiquement (par ex. avec un scanneur de sécurité) les faiblesses et les vulnérabilités de l'objet à protéger avant sa mise en service et, en fonction de son besoin de protection et de son exposition à Internet, pendant l'exploitation également. On fera appel au NCSC pour les faiblesses et vulnérabilités critiques.
T5	Authentification et autorisation T5.1 Tout accès à un objet à protéger doit être authentifié[18] conformément au besoin de protection de ce dernier et autorisé selon le principe «Least Privilege» ou «Need to Know». T5.2 Tous les droits d'accès à l'objet à protéger doivent être gérés dans le cadre d'un processus[19] défini et documenté et être tenus à jour en tout temps. En particulier, la nécessité et l'exactitude des droits seront

[18] L'authentification peut être réalisée localement ou à l'aide d'une ou de plusieurs connexions réseau. Dans le second cas, elle est considérée dans son intégralité (c.-à-d. authentification locale sur un terminal et authentifications éventuelles sur des serveurs proxy).

[19] Dans le cadre de ce processus, la séparation des pouvoirs entre l'autorisation et l'attribution de droits d'accès doit être prise en compte lorsque cela est possible et judicieux, et documentée.

	examinées au moins une fois par an, les droits (ou comptes) qui ne sont plus nécessaires étant supprimés. T5.3 Seuls des moyens d'authentification et de vérification d'identité gérés dans le cadre d'un processus défini et documenté peuvent être utilisés pour l'objet à protéger. Ce processus doit couvrir l'ensemble du cycle de vie du support (y c. les possibilités d'accès en cas d'urgence, le blocage, la réinitialisation, la révocation et l'élimination).
T6	Authentification de l'utilisateur T6.1 L'utilisateur d'un SPT ou d'un système serveur doit être authentifié par un moyen d'authentification et de vérification d'identité présentant au moins le niveau de sécurité «moyen» selon l'annexe B ou grâce à une authentification à deux facteurs[20]. T6.2 L'utilisateur d'un système MDM doit être authentifié par une procédure compatible avec le système d'exploitation en question, telle qu'un numéro d'identification personnel (NIP)[21] ou une authentification biométrique (par ex. Touch ID ou Face ID pour les appareils iOS). Le NIP doit comporter au moins six caractères et ne pas être trop simple. T6.3 L'utilisateur d'un élément du réseau doit être authentifié par un moyen d'authentification et de vérification d'identité présentant au moins le niveau de sécurité «élevé» selon l'annexe B.
T7	Mots de passe Les exigences suivantes s'appliquent à l'authentification de l'utilisateur au moyen d'un mot de passe. T7.1* Le mot de passe a) doit être personnel[22]; b) doit être unique[23]; c) ne doit pas être communiqué à un tiers; d) ne doit pas être écrit ou doit être consigné de manière sécurisée ou être géré par un programme de chiffrement des mots de passe[24]; e) doit comporter au moins dix caractères (18 caractères pour les utilisateurs ayant des droits élevés), au moins trois des quatre catégories suivantes devant être présentes: majuscules, minuscules, chiffres et caractères spéciaux; f) ne doit pas être ordinaire ni se référer à l'utilisateur (par ex. aucun attribut tel que l'identifiant de l'utilisateur, son nom, son prénom ou sa date de naissance).

[20] La nécessité d'une authentification à deux facteurs découle d'une décision prise par le Conseil fédéral le 4 juin 2010. Pour les collaborateurs de la Confédération, on utilise des certificats de classe B de la SG-PKI. En cas de système serveur, l'authentification de l'utilisateur se réfère au niveau du système d'exploitation.

[21] La différence conceptuelle entre un mot de passe et un NIP est expliquée dans la considération technologique «Passwörter vs. PINs» du 29 juin 2012. Par conséquent, les exigences minimales des NIP indiquées ici ne s'appliquent que de manière limitée.

[22] Les comptes impersonnels ne peuvent être octroyés que dans des cas particuliers dûment justifiés (cf. [Si002-Hi01]). Ils ne peuvent être utilisés que pour accéder à des objets à protéger ne présentant pas un besoin de protection accru (protection de base).

[23] Il est notamment interdit d'utiliser le même mot de passe pour s'authentifier dans plusieurs systèmes informatiques et applications.

[24] Sur le SPT, il faut utiliser l'outil de gestion personnelle des mots de passe (couche 1).

	T7.2* Un mot de passe initial attribué de manière administrative doit être modifié dès sa première utilisation. T7.3* Lorsque le mot de passe est changé, il faut s'assurer que le nouveau ne correspond pas à l'un des dix mots de passe utilisés précédemment. T7.4* Après cinq tentatives erronées au plus, le mot de passe doit être bloqué. Il ne peut être débloqué que dans le cadre d'un processus défini. T7.5 Le mot de passe doit être changé sans délai si l'on soupçonne que des personnes non autorisées en ont connaissance ou qu'il y a un abus. T7.6* Au niveau du serveur, il faut veiller à ce que le mot de passe ne puisse pas être lu en texte clair ni être compromis facilement dans le cadre d'une autre attaque.
T8	Accès administratifs et accès à distance T8.1 Les accès administratifs à l'objet à protéger doivent être exécutés de manière documentée et contrôlée. En particulier, ils doivent bénéficier d'une sécurisation cryptographique tout en étant enregistrés et évalués de façon compréhensible. T8.2 Les systèmes informatiques utilisés pour les accès administratifs doivent être dédiés à cette tâche et, de préférence, exploités dans une zone de gestion. L'utilisation des comptes (privilégiés) correspondants doit pouvoir être attribuée à une personne. De plus, les comptes ne peuvent disposer que des droits d'accès minimaux requis, dont la durée de vie sera aussi courte que possible[25]. Ils doivent être affectés à l'une des couches d'un modèle de couches[26] et ne peuvent servir qu'à l'administration au sein de cette couche (pour éviter une escalade des privilèges). En particulier, les comptes ne peuvent pas être employés pour des accès non administratifs à Internet. T8.3 Un accès direct à distance est autorisé pour un prestataire externe si: a) le propriétaire de l'objet est d'accord et consent à d'éventuelles violations du secret de fonction conformément aux procédures spécifiques à l'office ou au département (cf. [Si001-Hi03], [Si001-Hi04]); b) l'accès est réalisé via un compte dédié et l'utilisateur est authentifié par un moyen d'authentification et de vérification d'identité présentant au moins le niveau «moyen» selon l'annexe B; c) l'utilisation de ce compte est limitée dans le temps et surveillée; d) lorsque cela est techniquement possible, l'accès est exécuté via un *jump host*; e) le raccordement technique du compte au réseau bénéficie d'une sécurisation cryptographique (par ex. avec SSH), et f) la possibilité d'auditer les processus externalisés est garantie en tout temps.

[25] Idéalement, les comptes sont gérés dans le cadre d'une solution Privileged Access Management (PAM) et ne sont valables que pour la durée d'une activité administrative précise.

[26] Ce modèle de couches est défini, par exemple, dans le cadre de la directive E033 en cours d'élaboration.

Informations (données)	
I1*	Admissibilité des systèmes informatiques Les informations importantes pour les affaires peuvent être enregistrées et traitées sur des systèmes informatiques uniquement lorsqu'ils appartiennent à une UA de l'administration fédérale ou lorsque le respect des exigences techniques de sécurité énoncées dans le présent document est défini contractuellement pour ces systèmes (par ex. dans le cadre d'une solution en nuage).
I2	Confidentialité et intégrité I2.1 La confidentialité et l'intégrité des informations importantes pour les affaires doivent être protégées à tout moment par des procédés cryptographiques, conformément à leur besoin de protection et en tenant compte des particularités physiques[27] (cela vaut également pour les données de test et les données de production utilisées à des fins de test). Lorsque les informations sont cryptées, les clés utilisées à cet effet doivent être gérées de telle sorte qu'une récupération et, partant, un décryptage des informations soient possibles à tout moment. En général, cela requiert une administration complexe des clés (avec un mécanisme de récupération des clés) et un test régulier de la récupération. I2.2 Les systèmes informatiques utilisés doivent être appropriés pour garantir la protection de la confidentialité et de l'intégrité des informations[28].
I3	Disponibilité I3.1 La disponibilité des informations importantes pour les affaires doit être garantie à tout moment, conformément au besoin de protection. I3.2 Les UA responsables des informations doivent disposer d'une stratégie de sauvegarde[29] et la mettre en œuvre. Cette stratégie doit prévoir un principe multigénérationnel et un stockage hors ligne des principaux jeux de données afin que celles-ci puissent être récupérées même en cas de maliciels chiffrant les informations (rançongiciel).
I4	Supports de données Les supports de données sur lesquels sont enregistrées les informations importantes pour les affaires doivent à tout moment être protégés conformément au besoin de protection de ces informations. Des processus appropriés doivent être définis et mis en œuvre pour la réparation et l'élimination de ces supports[30].

[27] En particulier, les informations ayant un besoin de protection accru qui sont enregistrées sur les disques durs de systèmes serveurs physiques sans protection particulière doivent être sécurisées grâce à un chiffrement du disque dur.

[28] Par exemple l'enregistrement et le traitement d'informations classées CONFIDENTIEL, de données sensibles ou de profils de la personnalité sur des systèmes MDM ne sont pas autorisés ou ne le sont que dans le cadre d'une communication vocale chiffrée [E027].

[29] Lorsque l'UA responsable est un bénéficiaire de prestations (BP), la stratégie de sauvegarde peut également provenir du FP. Elle doit cependant être vérifiée et considérée comme appropriée par le BP. Des exercices réguliers concernant cette stratégie revêtent alors une importance primordiale: la possibilité de récupérer les données après une perte doit être contrôlée régulièrement et confirmée par le BP.

[30] Lors de l'élimination des supports de données, il faut en particulier veiller à ce que leur contenu ou les

Systèmes informatiques	
S1	Affectation à une zone Le système informatique doit être affecté à une zone et exploité conformément à la réglementation de cette zone[31].
S2	Mises à jour et correctifs Il faut s'assurer que le(s) fabricant(s) du système informatique propose(nt) pendant toute sa durée de vie des mises à jour et des correctifs (patchs) qui peuvent être vérifiés et installés rapidement[32], ou que le système informatique est exploité dans une zone dédiée et aussi hermétique que possible (par ex. zone technique), des mesures de sécurité complémentaires garantissant que cette situation n'engendre ni menace ni risque supplémentaires pour les autres objets à protéger de l'administration fédérale. Si un remplacement est prévu, le système informatique peut encore être exploité pendant deux ans au plus, à condition que la poursuite de l'exploitation soit exposée dans un concept SIPD.
S3	Comptes de service S3.1 Les comptes utilisés par les services système (comptes de service) doivent être spécifiques[33] et posséder uniquement les droits minimums requis pour fournir les services. S3.2* Les comptes de service doivent être gérés automatiquement et requérir une authentification cryptographique forte. Idéalement, celle-ci s'appuiera sur une cryptographie asymétrique, les clés privées utilisées à cet effet devant être consignées de manière sûre. Si l'authentification repose sur des mots de passe, ils doivent être sensiblement plus forts (et plus longs) que pour l'authentification de l'utilisateur.
S4	Protection de l'intégrité et protection contre les maliciels S4.1 L'intégrité des composantes logicielles utilisées sur le système informatique doit être garantie (par ex. à l'aide de signatures numériques). En particulier, l'intégrité de chaque système serveur ayant un besoin de protection accru doit être contrôlée régulièrement[34]. S4.2 Lorsqu'une perte d'intégrité est détectée, le système informatique doit être immédiatement coupé du réseau, sécurisé et examiné. Si sa compromission est confirmée, il doit être intégralement supprimé et reconfiguré. S4.3 Le système informatique doit être intégré dans un concept de protection contre les maliciels basé sur [SB003], qui définit en particulier la marche à suivre lorsqu'un maliciel est identifié, les services à informer et la manière de le faire.

données enregistrées ne puissent pas être reconstitués.

31 Un système informatique qui ne peut être affecté à aucune autre zone fait partie d'Internet. Il n'existe alors aucune réglementation de zone. De plus, il se peut que des éléments du réseau ne soient attribués ni à une zone ni à Internet. Ils doivent être documentés.

32 Pour les SPT qui ne sont pas connectés en permanence au réseau, il faut s'assurer que des mises à jour et des correctifs sont installés au moins une fois par mois.

33 Un compte de service est réputé spécifique lorsqu'il n'est utilisé que pour un service.

34 Décision du Conseil fédéral du 16 décembre 2009

S5	Ordinateurs clients de l'administration fédérale S5.1 Les supports de données internes non volatils (par ex. disques durs) doivent être visiblement cryptés sur un ordinateur client de l'administration fédérale. En cas de système MDM, il faut prévoir en plus une possibilité de réinitialiser à distance ses paramètres de base et de supprimer toutes les informations enregistrées localement. S5.2 En l'absence d'activité de l'utilisateur, l'accès à l'ordinateur client de l'administration fédérale doit être bloqué automatiquement (au bout de 15 min. au plus pour les SPT et de 3 min. au plus pour les systèmes MDM). Une activation manuelle des blocages d'accès au système doit aussi être possible. Si un tel blocage n'est pas possible pour des raisons techniques, l'accès aux ordinateurs clients de l'administration fédérale non surveillés doit être protégé physiquement (par ex. par verrouillage de la pièce). S5.3 La fonction de démarrage automatique en cas de raccordement de supports de données externes (par ex. clés USB) doit être désactivée sur un ordinateur client de l'administration fédérale. S5.4 Les utilisateurs d'un SPT ne peuvent avoir aucun droit d'administrateur local. S5.5 Un accès administratif au SPT à des fins d'assistance n'est autorisé qu'avec l'autorisation explicite préalable de l'utilisateur.
S6	Périphériques S6.1 Un périphérique peut être utilisé lorsque a) il a été acquis auprès d'un service d'achat de la Confédération, et b) son intégrabilité[35] et sa sécurité élémentaire sont dûment confirmées par le FP. S6.2 Le périphérique doit être configuré de manière minimale par le FP et protégé contre les modifications non autorisées (de la configuration). S6.3 Lorsque l'appareil est utilisé pour imprimer des documents classifiés: a) il doit être exploité localement ou doit permettre d'authentifier l'utilisateur, et b) les supports de données internes non volatils (par ex. disques durs) doivent pouvoir être écrasés conformément aux recommandations en vigueur[36], cet écrasement pouvant être déclenché manuellement par l'utilisateur ou automatiquement. S6.4 L'utilisation de périphériques privés lors du travail mobile doit respecter la directive d'application [E026].
Applications	
A1	Achat / développement

[35] L'intégrabilité signifie, par exemple, que l'appareil peut être relié aux registres des collaborateurs de l'administration fédérale pour des fonctions comme ScanToMail.

[36] B.B. DoD 5220.22-M ou NIST SP 800-88

	A1.1 L'application doit être achetée ou développée dans le cadre d'un processus méthodique (de préférence HERMES[37]), en tenant compte précocement des directives et recommandations en vigueur en matière de sécurité[38] (meilleures pratiques). A1.2 Lors du développement de logiciels d'application, il faut notamment veiller à a) conserver le code source de manière sûre; b) réglementer clairement et contrôler de manière compréhensible l'accès aux référentiels correspondants; c) surveiller les processus Build et n'exécuter les modifications dans la Build Pipeline que sous supervision; d) tester régulièrement les logiciels, et e) garantir à tout moment leur intégrité (par ex. à l'aide de signatures numériques).
A2	Entretien et maintenance Un entretien et une maintenance professionnels doivent être garantis pour l'application et ses composantes (par ex. bibliothèques logicielles) pendant toute la durée de vie. Cela englobe en particulier l'installation de mises à jour et de correctifs (patchs) réguliers qui sont techniquement nécessaires à l'exploitation ou à la sécurité.
Zones	
Z1	Conformité Z1.1 La zone doit être conforme au modèle de zones de la Confédération et avoir un propriétaire, un nom unique[39], une réglementation (*policy*) de zone et un exploitant[40] (cela ne s'applique ni à Internet ni à la zone Internet). Si elle comprend des systèmes informatiques et des applications qui sont exploités en dehors de l'administration fédérale (par ex. sur un nuage public), le raccordement au réseau doit être défini dans la réglementation de zone. Z1.2 L'exploitant doit veiller à ce que seules les communications admises par la réglementation de zone soient exécutées depuis et vers la zone et, grâce à des mesures de sécurité complémentaires appropriées (par ex. isolement et segmentation), à ce qu'elles n'engendrent ni menace ni risque supplémentaires pour les autres systèmes informatiques et applications au sein et hors de la zone.

37 https://www.hermes.admin.ch

38 Pour le développement d'applications Web, il faut, par exemple, prendre en considération les directives et les recommandations de l'Open Web Application Security Project (OWASP), qui couvrent également la gestion sûre du code du programme.

39 L'unicité peut découler, par exemple, de l'indication du propriétaire comme suffixe dans le nom de la zone (par ex. SZ-BAC pour une zone de serveurs exploitée par la BAC). Si un propriétaire met plusieurs fois en œuvre une zone, les noms correspondants doivent être clairement différenciés.

40 L'exploitant est un FP qui gère la zone au niveau de la technique du réseau sur mandat du propriétaire. Si le propriétaire de la zone est un FP, le propriétaire et l'exploitant peuvent être identiques. Lorsque le propriétaire modifie la réglementation d'une (sous-)zone, un délai raisonnable de mise en œuvre doit être accordé à l'exploitant.

	Z1.3 La zone doit être intégrée au registre que le DSID tient et met à la disposition du NCSC. Le DSID est compétent lorsqu'une UA du département agit en tant que propriétaire ou exploitant de la zone.
Z2	Accès Z2.1 Un accès restreint[41] à une zone est autorisé uniquement pour les personnes et les processus automatisés qui ont été authentifiés par un moyen d'authentification et de vérification d'identité présentant au moins le niveau «moyen» (le niveau «faible» suffit pour les appareils de mesure). Les dérogations suivantes sont admises: a) accès anonymes et personnalisés créés dans le cadre des applications de cyberadministration utilisables par une large partie de la population dans une zone de serveurs. Les pages Web correspondantes doivent être sécurisées avec TLS (HTTPS) et protégées contre les attaques automatisées grâce à des formulaires (par ex. Captcha); b) accès temporaires pour charger des données sur un système serveur[42]; c) accès automatisés effectués avec le consentement d'un propriétaire de zone dans le cadre des contrôles de sécurité des sites Internet (*scans*). En cas d'accès à une zone présentant un besoin de protection accru (par ex. SZ+), le moyen d'authentification et de vérification d'identité doit avoir au moins le niveau «élevé» selon l'annexe B. Les dérogations a) et b) susmentionnées ne sont alors pas autorisées. Z2.2 Un accès illimité à une zone n'est admis que pour les personnes qui se connectent via un ordinateur client de l'administration fédérale, sont authentifiées par un moyen d'authentification et de vérification d'identité présentant au moins le niveau «élevé» selon l'annexe B et utilisent une connexion cryptographique sécurisée (par ex. avec SSH).
Z3	Communication interzone Toute communication interzone doit passer par une PEZ[43]. Celle-ci doit s'assurer que la communication est conforme à la réglementation des zones concernées. Pour ce faire, les modèles et relations de communication autorisés doivent être définis aussi précisément que possible dans les réglementations des zones (dans l'idéal sur la couche applicative et sous la forme d'une *allow list*). Si un test de conformité dans une PEZ n'est pas possible (par ex. dans le cas d'une communication cryptée de bout en bout), il peut également être effectué par les systèmes informatiques dans les zones elles-mêmes (au sens d'un PEP). Toutefois, des mesures complémentaires d'atténuation des risques

41 Un accès est dit restreint lorsque des mesures techniques (par ex. filtrage de paquets IP) sont mises en place pour le limiter à un seul ou à quelques systèmes informatiques ou applications définis et aux protocoles indispensables pour l'accès. Dans tous les autres cas, l'accès est réputé illimité.

42 Dans ce cas, la délimitation des systèmes serveurs correspondants par rapport aux autres systèmes informatiques de la même zone doit être documentée soit dans la réglementation de zone, soit – conjointement avec toutes les mesures de sécurité complémentaires visant à minimiser les risques – dans la documentation de sécurité de l'application. Bien entendu, le propriétaire de la zone doit également donner son accord à l'exploitation des systèmes serveurs.

43 Bien que cela s'applique en principe également à la communication d'une sous-zone vers sa zone supérieure, il est possible d'y renoncer dans des cas justifiés documentés dans les réglementations des sous-zones correspondantes.

	doivent alors être prévues et documentées.

Z4	PEZ Z4.1 Les PEP exploités dans une PEZ ne peuvent être gérés de manière virtualisée qu'au sein de la zone. En d'autres termes, aucun système informatique des autres zones ne peut être exploité sur le matériel utilisé en commun. Z4.2 Le propriétaire d'une PEZ ou d'une infrastructure proxy Web doit définir la manière dont l'accès aux ressources sur Internet est réalisé et quels accès sont autorisés. Il peut le faire dans la réglementation de zone de la PEZ ou dans une directive distincte. Le NCSC peut compléter les ensembles de règles correspondants. Dans le champ d'application du service informatique standard Communication de données, la réglementation est édictée dans le cadre de [Si004]. Z4.3 La connexion d'une PEZ à Internet doit être hautement disponible, voire redondante. En outre, l'exploitant doit s'assurer grâce à des mesures appropriées que les systèmes informatiques séparés d'Internet par la PEZ sont dûment protégés contre des attaques de déni de service (*denial of service*, DoS) ou de déni de service distribué (*distributed DoS*, DDoS).
Z5	Surveillance Z5.1 La communication au sein d'une zone doit être surveillée de telle sorte que les attaques puissent être identifiées de manière aussi fiable que possible (par ex. grâce à des systèmes de détection ou de prévention d'intrusion [*intrusion detection system*, IDS; *intrusion prevention system,* IPS]) et que l'exploitant puisse réagir rapidement et adéquatement en cas de besoin. Z5.2 Les informations collectées lors de la surveillance doivent être conservées et protégées contre des manipulations ultérieures, conformément aux dispositions légales (en particulier, la législation sur la protection des données et l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération). En cas de besoin, elles doivent être mises à la disposition du NCSC.

5 Entrée en vigueur et dispositions transitoires

[1] La directive entre en vigueur le 1er mars 2022.

[2] Les objets à protéger mis en service avant l'entrée en vigueur de la présente directive sont soumis aux dispositions qui s'appliquaient au moment de leur mise en service (c.-à-d. au moins [Si001], version 4.4, et [Si003], version 3.1). Ils doivent cependant être adaptés aux nouvelles prescriptions dans le cadre de leur cycle de vie, mais au plus tard dans les cinq ans suivant l'approbation de la documentation de sécurité.

[3] Les dérogations relèvent du ch. 1.3. Toutes celles qui ont été octroyées précédemment restent valables.

[4] Tant que la propriété du domaine de réseau bleu n'a pas été clarifiée et que les directives correspondantes n'ont pas été publiées, la réglementation de zone de l'annexe C avec l'ensemble des dérogations et accords[44] et la matrice d'accès de l'annexe D[45] s'appliquent.

[5] Le NCSC vérifie régulièrement le caractère actuel de la présente directive.

Abréviations

BA	Bureautique
BAC	Base d'aide au commandement
BCM	Gestion de la continuité de l'activité (*Business Continuity Management*)
BP	Bénéficiaire de prestations
CA	Autorité de certification (*Certification Authority*)
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CDF	Contrôle fédéral des finances
CF	Ordinateur client de l'administration fédérale (client fédéral)
ChF	Chancellerie fédérale
CVC	Communication vocale chiffrée
CZ	Client Zone
DAKO	Transmission de données (*Datenkommunikation*)
DDoS	Déni de service distribué (*Distributed DoS*)
DIS	Draft International Standard, projet de norme internationale
DNS	Système de noms de domaine (*Domain Name System*)
DoS	Déni de service (*Denial of Service*)
DSID	Délégué à la sécurité informatique du département
DSIO	Délégué à la sécurité informatique de l'unité administrative
EAL	Niveau d'évaluation (*Evaluation Assurance Level*)
FIDO	Fast ID Online
FP	Fournisseur de prestations
IAM	Gestion des identités et des accès (*Identity and Access Management*)
ID	Identifiant
IdO	Internet des objets
IDS	Système de détection d'intrusion (*intrusion detection system*)
IEC	Commission électrotechnique internationale (International Electrotechnical Commission)
IKE	Internet Key Exchange
IP	Protocole Internet (*Internet Protocol*)

[44] En l'occurrence, il s'agit d'une convention avec les Services du Parlement.
[45] Toute décision à cet égard sera soumise au NCSC par le secteur TNI.

IPS	système de prévention d'intrusion (*intrusion prevention system*)
IPsec	IP security, sécurité du protocole Internet
ISO	Organisation internationale de normalisation
IT	Technologies de l'information
ITSCM	Gestion de la continuité des services informatiques (*IT Service Continuity Management*)
JSON	JavaScript Object Notation
JWT	JSON Web Token
LoA	Niveau d'assurance (*Level of Assurance*)
LSI	Loi sur la sécurité de l'information
MDM	Gestion des appareils mobiles (*Mobile Device Management*)
NCSC	Centre national pour la cybersécurité
NIP	Numéro d'identification personnel (*Personal Identification Number, PIN*)
NW	Accès illimité au réseau (*Network Full Access*)
OFCL	Office fédéral des constructions et de la logistique
OPCy	Ordonnance sur les cyberrisques
OPrI	Ordonnance concernant la protection des informations
OSI	Open Systems Interconnection
OTP	Mot de passe à usage unique (*one-time password*)
OWASP	Open Web Application Security Project
PAM	Gestion des accès privilégiés (Privileged Access Management)
PEP	Point d'application des règles (*policy enforcement point*)
PEZ	Zone d'application des règles (*policy enforcement zone*)
PKI	Infrastructure à clés publiques (*Public Key Infrastructure*)
RA	Accès restreint au réseau (*Restricted Access*)
SAML	Security Assertion Markup Language
SG-PKI	Swiss Government PKI
SIPD	Sécurité de l'information et protection des données
SMS	Short Message Service
SPT	Système de poste de travail
SS	Service standard
SSH	Secure Shell
SSO	Single Sign-On
SSZ	Zone de services partagés (*Shared Service Zone*)
SZ	Zone de serveurs (*Server Zone*)
SZ+	Zone de serveurs avec besoin de protection accru
TCP	Transmission Control Protocol
TIC	Technologies de l'information et de la communication
TLS	Transport Layer Security
TNI	Transformation numérique et gouvernance de l'informatique (secteur de la ChF)
TPM	Trusted Platform Module
TT	Terminal de tiers
UA	Unité administrative

Références

[E021] TNI, E021 - Directive d’application pour la synchronisation des smartphones et tablettes, version 2.1 du 9 juin 2020

[E026] TNI, E026 - Directive d’application sur le système de poste de travail, version 1.0 du 11 juin 2019 (sera remaniée et adaptée au travail mobile)

[E027] TNI, E027 - Directive d’application Communication vocale chiffrée (CVC), version 1.1 du 1er octobre 2021

[OPCy] Ordonnance du 27 mai 2020 sur les cyberrisques

[OPrI] Ordonnance du 4 juillet 2007 concernant la protection des informations

[SB003] NCSC, Malwareschutz Strategie in der Bundesverwaltung, 2021

[Si001-Hi01] Mise en œuvre des mesures de protection informatique de base dans l’administration fédérale, version 4.6 du 31 mars 2021

[Si001-Hi03] Exigences liées aux risques de violation du secret de fonction dans l’administration fédérale 2021, version 1.4 du 31 mars 2021

[Si001-Hi04] Recommandation concernant la mise en œuvre opérationnelle de la procédure de consentement, 15 décembre 2020

[Si002-Hi01] Demande pour l’obtention de comptes impersonnels (comptes E et F), 15 décembre 2020

[Si004] Réglementation de l’accès aux ressources sur Internet. Directive de l’administration fédérale relative aux proxys web, version 1.3 du 4 octobre 2016 (état: 1er avril 2019)

Annexe A: Modèle de zones de la Confédération

Le modèle de zones de la Confédération (cf. illustration A.1) est un modèle générique destiné à la création de zones dans l'administration fédérale. Il définit comment les systèmes informatiques et les réseaux de cette dernière doivent être organisés et gérés en zones et en sous-zones.

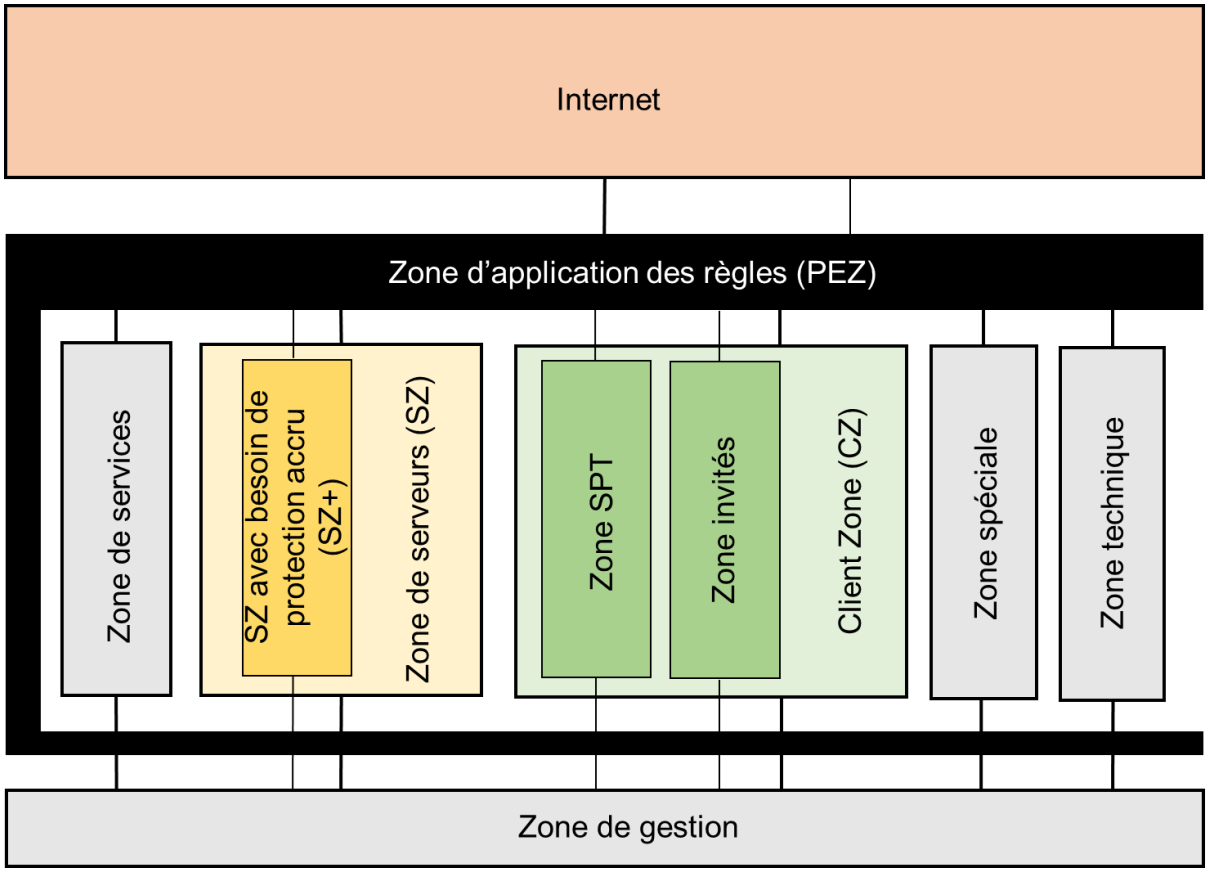

Illustration A.1: Modèle de zones de la Confédération

Dans le modèle de zones de la Confédération, on distingue les zones et sous-zones suivantes:

a) **Internet:** zone qui ne correspond à aucun critère des autres zones et pour laquelle aucune exigence (de sécurité) ne peut être définie.
b) **Zone d'application des règles *(Policy Enforcement Zone*, PEZ):** zone pour les PEP nécessaires à l'application des règles de communication externe avec d'autres zones.
c) **Zone de services (*Service Zone*):** zone destinée aux systèmes serveurs nécessaires à la fourniture de services d'infrastructure (par ex. serveurs DNS et serveur de temps).
d) **Zone de serveurs (*Server Zone*, SZ):** zone destinée aux systèmes serveurs sur lesquels sont gérées des applications qui ne présentent pas un besoin de protection accru selon l'analyse des besoins de protection.

e) **Zone de serveurs avec besoin de protection accru (SZ+):** sous-zone de la SZ destinée aux systèmes serveurs sur lesquels sont gérées des applications ayant un besoin de protection accru selon l'analyse des besoins de protection[46].
f) **Client Zone (CZ):** zone destinée aux systèmes clients. L'exploitation de systèmes serveurs dans la CZ ou une sous-zone est autorisée si la réglementation (*policy*) correspondante le prévoit et si ces systèmes serveurs sont utilisés principalement par les systèmes clients de la même (sous-)zone (par ex. serveur local de bureautique ou d'impression).
g) **Zone SPT:** sous-zone de la CZ destinée aux systèmes clients qui fonctionnent comme des systèmes de poste de travail (SPT) et sont utilisés exclusivement pour le service standard Bureautique / UCC.
h) **Zone invités:** sous-zone de la CZ destinée aux systèmes clients qui ne sont pas gérés par une unité administrative de la Confédération, tels que les appareils utilisés par des collaborateurs externes ou des employés de l'administration fédérale dans le cadre de la politique «Bring Your Own Device».
i) **Zone spéciale:** zone destinée aux systèmes informatiques de l'administration fédérale qui présentent des caractéristiques particulières et des exigences correspondantes (par ex. exploitation autosuffisante ou connexion réseau à faible bande) et qui peuvent être administrés depuis la zone de gestion (par ex. réseau de transport assorti d'exigences spécifiques).
j) **Zone technique:** zone particulière destinée aux systèmes informatiques et aux systèmes de l'IdO, tels que les systèmes de domotique ou de *facility management*, les systèmes d'enregistrement du temps de travail, les systèmes de mesure et les systèmes de télédiagnostic.
k) **Zone de gestion:** zone particulière destinée aux systèmes informatiques qui sont utilisés exclusivement pour administrer les systèmes informatiques des autres zones.

Toute (sous-)zone du modèle de zones de la Confédération peut être mise en œuvre plusieurs fois.

[46] Lorsque l'exploitation d'une application ayant un besoin de protection accru nécessite plusieurs systèmes serveurs, la répartition des différents systèmes entre la SZ et la SZ+ doit être documentée et justifiée dans un concept SIPD.

Annexe B: Niveaux de sécurité des moyens d'authentification et de vérification d'identité

Les moyens d'authentification et de vérification d'identité actuellement disponibles ou utilisés avec les protocoles de fédération correspondants sont répartis selon les quatre niveaux de sécurité suivants (faible, moyen, élevé et élevé+)[47]:

a) **Faible:** les informations d'authentification transmises par le réseau étant statiques et identiques pour chaque authentification, elles peuvent être exploitées par un intrus et utilisées à mauvais escient, par exemple pour une attaque par rejeu suivie d'une usurpation d'identité. Le nom d'utilisateur et le mot de passe sont des exemples typiques de ce type d'informations d'authentification. Si celles-ci sont utilisées en tant que jeton de fédération au sens de la norme I050, il suffit de les protéger à un niveau faible contre les attaques visant leur intégrité et de les relier au contexte de l'utilisateur. À titre d'exemple, on peut citer divers «jetons au porteur» tels que les cookies.

b) **Moyen:** les informations d'authentification sont systématiquement modifiées à chaque connexion et ne peuvent donc pas être utilisées à mauvais escient pour une attaque de rejeu suivie d'une usurpation d'identité. Font partie de cette catégorie, par exemple, les noms d'utilisateur et les mots de passe avec code de vérification envoyé par SMS ou la restriction à un appareil, les solutions logicielles utilisant des mots de passe à usage unique (*one-time password* [OTP], par ex. Google Authenticator) ainsi que les certificats logiciels délivrés par la SG-PKI (classe C, D ou E). Si les informations d'authentification sont utilisées comme un jeton de fédération, elles doivent être protégées contre les attaques visant leur intégrité et liées au contexte de l'utilisateur d'une manière correspondant à l'état de la technique. On peut citer comme exemples les tickets Kerberos des forêts de ressources de la norme standard Bureautique et les jetons au porteur tels que JWT transmis via SAML ou OIDC/OAuth.

c) **Élevé:** les informations d'authentification sont dynamiques et dépendent d'une clé cryptographique qui est stockée dans un module matériel dédié et qui ne peut pas, en déployant un effort raisonnable, être déchiffrée à l'aide de ce module. Si le moyen d'authentification et de vérification d'identité est personnel, l'enregistrement de la personne ou la remise du moyen de vérification à celle-ci doivent être basés sur un document d'identité officiel (passeport ou carte d'identité, par ex.). Si la vérification de l'identité de la personne et l'enregistrement ont lieu conjointement, les moyens d'identification doivent être remis par courrier recommandé. La remise peut également être protégée par un code secret (mot de passe ou NIP, par ex.) ou par des caractéristiques biométriques (Touch ID ou Face ID avec Apple, Hello avec Windows, par ex.). Cette catégorie comprend notamment les jetons OTP, les solutions OTP basées sur un TPM, les jetons FIDO2, Swisscom Mobile ID et la SuisseID. Si les informations d'authentification sont utilisées en tant que jeton de fédération, elles doivent être protégées contre les attaques visant leur intégrité et liées au contexte de l'utilisateur d'une manière correspondant à l'état de la technique. Globalement, le protocole de fédération doit correspondre à un profil de protection comparable au CC EAL4+. Il s'agit par exemple de l'identité SSO/la fédération SSO

[47] La norme informatique I050 définit quatre niveaux de confiance (*Level of Assurance*, LoA), qui peuvent servir à fixer les exigences minimales de sécurité à imposer aux moyens d'authentification et de preuve d'identité qui seront utilisés. Cependant, comme il n'existe pas de classification selon les LoA des moyens d'authentification et de preuve d'identité actuellement disponibles et en usage, on utilisera ici, à titre transitoire, une classification simple qui met l'accent sur quelques aspects de sécurité techniques.

du portail SSO et des tickets Kerberos des forêts utilisateurs, si ceux-ci ont été émis sur la base d'une authentification de l'utilisateur avec un certificat de classe B délivré par la SG-PKI.

d) **Élevé+:** les moyens d'authentification et de vérification d'identité répondent aux exigences du niveau «élevé» (y c. les exigences applicables au protocole de fédération). En outre, le NCSC doit approuver tant le module matériel que le processus d'enregistrement sous-jacent avant leur utilisation par l'administration fédérale. Cette catégorie ne comprend que les certificats de classe B délivrés par la SG-PKI sur des cartes à puce.

Les exemples cités dans le texte et figurant sous forme de résumé dans le tableau B.1 ne constituent pas une liste exhaustive.

Niveau de sécurité	Exemples de moyens d'authentification et de vérification d'identité
Faible	• Nom d'utilisateur et mot de passe • «jeton au porteur» (par ex. cookies)
Moyen	• Nom d'utilisateur et mot de passe avec code de vérification envoyé par SMS[48] • Nom d'utilisateur et mot de passe liés à un appareil • Solution logicielle OTP (par ex. Google Authenticator) • Certificat logiciel délivré par la SG-PKI (classe C, D ou E) • Tickets Kerberos de la forêt de ressources du service informatique standard Bureautique • «Jeton au porteur» tel que JWT transmis par SAML ou OIDC/OAuth
Élevé	• Jeton (token) OTP (par ex. RSA, Vasco, etc.) • Solution OTP basée sur un TPM • Jeton FIDO2 • Swisscom Mobile ID • SuisseID (tant que ce moyen est fourni officiellement) • Identité SSO/fédération SSO du portail SSO • Jeton SAML émis dans le cadre de l'eIAM • Tickets Kerberos des forêts utilisateurs (SG-PKI)
Très élevé	• Certificat sur carte à puce délivré par la SG-PKI (classe B)

Tableau B.1: Niveaux de sécurité de quelques moyens d'authentification et de preuve d'identité

Fondamentalement, un niveau de sécurité ne peut pas être amélioré en cumulant plusieurs moyens d'authentification et de vérification d'identité de même niveau. Ainsi, un certificat logiciel délivré par la SG-PKI reste, par exemple, au niveau de sécurité «moyen» même s'il

[48] En principe, les procédures d'authentification basées sur l'envoi d'un SMS ne devraient être utilisées qu'en l'absence d'une meilleure solution.

est combiné avec un nom d'utilisateur et un mot de passe avec code de vérification envoyé par SMS.

Annexe C: Réglementation de zone «Domaine de réseau bleu»

C.1 Exigences et prescriptions relatives aux systèmes informatiques

[1] Un système informatique peut être géré dans le domaine de réseau bleu s'il remplit les exigences visées au chapitre 3*a* OPCy, à savoir les exigences relatives à l'analyse des besoins de protection, à la protection informatique de base et au concept SIPD.

C.2 Exigences et prescriptions relatives au domaine de réseau bleu

[1] Le domaine de réseau bleu peut être segmenté.

[2] Une subdivision en sous-zone au sens du ch. 2, al. 2, let. j, est possible.

C.3 Exigences et prescriptions relatives à la communication autorisée

C3.1 Communication interne

[1] La communication interne peut être réalisée directement. Elle n'est soumise à aucune restriction allant au-delà d'une segmentation réseau.

C.3.2 Communication externe

[1] La communication externe ne doit pas être réalisée directement, mais doit passer par un ou plusieurs PEP (par ex. dans une PEZ).

[2] Il faut s'assurer qu'un système informatique du domaine de réseau bleu ne peut pas entretenir simultanément plusieurs communications externes avec des systèmes informatiques d'autres zones.

[3] Les exigences et prescriptions suivantes s'appliquent aux communications entrantes:

a) Seuls des protocoles qui sont publiés et standardisés ou pour lesquels il existe un serveur reverse proxy digne de confiance peuvent être utilisés en tant que tels. Les protocoles et formats de données SOAP/XML, REST/XML et/ou REST/JSON doivent être employés pour les services web.

b) La communication est réalisée grâce à un serveur reverse proxy qui (i) authentifie la personne initiant la communication, (ii) protège le trafic des données et (iii) enregistre et évalue rapidement les données secondaires correspondantes. Dans le cas des services web, une authentification des processus (consommateurs et fournisseur de ces services) sur la base de certificats SSL/TLS reconnus suffit, et la protection du trafic des données doit être exécutée grâce à une vérification du contenu des

messages[49] ainsi qu'à une authentification et un cryptage transparents des données reposant sur HTTPS.

c) Un accès illimité au réseau est uniquement possible à partir d'un système informatique exploité par une unité organisationnelle de l'administration fédérale.

[4] La directive de l'administration fédérale relative aux proxys web [Si004] s'applique aux communications sortantes.

[49] Si un cryptage de bout en bout entre le consommateur et le fournisseur du service web est nécessaire et si le pare-feu de ce service ne peut dès lors pas vérifier directement le contenu des messages, des mesures complémentaires devront être mises en œuvre pour garantir cette vérification au moins indirectement.

Annexe D: Matrice d'accès du domaine de réseau bleu et de la SSZ

Les tableaux suivants sont repris de la version 4.0 de la matrice d'accès (anciennement [Si002]) et s'appliquent respectivement à l'authentification des personnes se connectant au domaine de réseau bleu et à la zone de services partagés (Shared Service Zone, SSZ) (tableau D.1) et à l'authentification des systèmes partenaires et des processus (tableau D.2). Les dérogations relatives aux applications de cyberadministration (exigence Z2.1 a) continuent de s'appliquer.

	Niveau de protection	**Base (NP0)**				**1 (NP1)**				**2 (NP2)**			
	Terminal d'utilisateur	CF	CF	TT	TT	CF	CF	TT	TT	CF	CF	TT	TT
	Méthode d'accès	NW	RA	NW	RA	NW	RA	NW	RA	NW	RA	NW	RA
Domaine de réseau bleu	Hard crypto token	o	o	n	o	o	o	n	o	o	o	n	o
	OTP	o	o	n	o	o	o	n	o	o	o	n	o
	OTP sans appareil	n	o	n	o	n	o	n	o	n	n	n	n
	Soft crypto token	n	n	n	n	n	n	n	n	n	n	n	n
	Mot de passe ou NIP	n	n	n	n	n	n	n	n	n	n	n	n
SSZ	Hard crypto token	o[50]	o	n	o	o[50]	o	n	o	o[50]	o	n	o
	OTP	o[50]	o	n	o	o[50]	o	n	o	o[50]	o[50]	n	o
	OTP sans appareil	n	o	n	o	n	o	n	o	n	n	n	n
	Soft crypto token	n	o	n	o	n	o	n	o	n	n	n	n
	Mot de passe ou NIP	n	o	n	o	n	o	n	o	n	n	n	n

Tableau D.1: Authentification de personnes se connectant au domaine de réseau bleu ou la SSZ

	Niveau de protection	**Base (NP0)**		**1 (NP1)**		**2 (NP2)**	
	Méthode d'accès	NW	RA	NW	RA	NW	RA
Domaine de réseau bleu / SSZ	Hard crypto token	n	o	n	o	n	o
	OTP / OTP sans appareil	Aucune application pratique					
	Soft crypto token	n	o	n	o	n	o[51]
	Mot de passe ou NIP	n	o[52]	n	n	n	n

Tableau D.2: Authentification de systèmes partenaires et des processus correspondants

50 Seul cas d'application: administration de systèmes via Admin-LAN (zone de gestion FP).
51 Autorisé uniquement pour l'accès à Sedex et à d'autres applications par l'intermédiaire desquelles seuls des messages standardisés peuvent être échangés et/ou des processus définis peuvent être suivis.
52 Admis uniquement pour les données télémétriques (instruments de mesure).

Annexe E: Modifications par rapport à la version 4.6 (état au 1er janvier 2021)

Les informations ci-après indiquent comment les exigences de la version 4.6 (colonne de gauche) ont été intégrées dans la version 5.0. Elles se limitent aux exigences qui n'étaient pas encore abrogées dans la version 4.6 et qui y figuraient explicitement.

Ch. 2.1.1: La restriction selon laquelle seuls des systèmes MDM pouvaient communiquer avec les systèmes de l'administration fédérale semble désormais trop limitative, d'autant que le modèle de zones comprend également des zones spéciales et une zone invités. Sur le fond, on opère une distinction entre les systèmes MDM (qui sont également des ordinateurs clients de l'administration fédérale) et les autres appareils électroniques (*smart devices*). D'après I1*, I2.2 et la note de bas de page correspondante, l'enregistrement et le traitement de données importantes pour les affaires (jusqu'au niveau de classification INTERNE compris) ne sont autorisés que sur les systèmes MDM. Ce point est pris en compte. Les dérogations mentionnées sont reprises par analogie au dans Z2.1, let. a) (avec d'autres).

Ch. 2.1.2: Découle de I2.2 et de la note de bas de page correspondante. Le traitement d'informations classées SECRET est interdit sur tous les types d'appareils électroniques (*smart devices*).

Ch. 2.1.6: Cette exigence est reprise sous une forme plus générale dans 02.1, let. e), et, pour les systèmes MDM, dans S5.1. On renonce à l'exigence supplémentaire selon laquelle «cette réglementation doit être communiquée aux unités administratives sous une forme appropriée». La présente exigence vaut pour toutes les réglementations.

Ch. 2.1.8: Cette exigence est reprise dans T6.2 et S5.2.

Ch. 3.1.1: Cette exigence est reprise dans P1.1.

Ch. 3.1.2: Concernant les droits d'accès, cette exigence est reprise dans T5.1 et T5.2. Les droits d'entrée et d'accès font partie des mesures de protection physiques; ils relèvent d'O2.1, let. b).

Ch. 3.1.3: Cette exigence s'applique indépendamment de la protection de base. Elle ne doit donc pas être réglementée dans cette dernière (concerne la LSI et sa mise en œuvre).

Ch. 4.1.2/3: Ces exigences sont reprises par analogie dans I1*. Le besoin de protection doit toujours être pris en compte (et pas uniquement lors de l'utilisation de moyens informatiques privés).

Ch. 5.1: La teneur de cette exigence est reprise dans I4.

Ch. 6.1: Cette exigence est reprise dans S5.1.

Ch. 6.2: Cette exigence est citée comme exemple dans P2 (avec d'autres événements critiques pour la sécurité).

Ch. 7.1.1: Cette exigence est reprise dans T5.1 et Z2 (pour les zones).

Ch. 7.1.4: Cette exigence est reprise dans T5.1 et T5.2.

Ch. 7.1.5: Cette exigence est reprise dans S5.4 et étendue dans T8.2 au sens d'une solution PAM (ou dans T8.1 pour les entrées de journaux).

Ch. 7.1.6: Cette exigence est reprise sous une forme atténuée dans T5.2 et la note de bas de page correspondante. Cette atténuation concerne la «séparation des pouvoirs entre l'autorisation et l'attribution de droits d'accès», qui doit être respectée uniquement lorsque cela est possible et judicieux. Une documentation est requise dans tous les cas.

Ch. 7.1.7: Cette exigence est reprise dans T6.1 (authentification à deux facteurs). La possibilité de comptes E et F impersonnels est conservée dans T7.1* et dans la note de bas de page correspondante. Ceux-ci peuvent être demandés conformément à [Si002-Hi01].

Ch. 7.1.8: Cette exigence est reprise et précisée dans T8.3.

Ch. 7.1.9: Cette exigence est reprise dans Z2.2 (dernier point).

Ch. 7.1.10: Cette exigence est reprise dans S5.5.

Ch. 7.1.11: Cette exigence est reprise dans S3.1.

Ch. 8.1: Reprise sous une forme simplifiée, cette exigence fait partie des dispositions concernant la gestion des mots de passe sur les serveurs dans T7.

Ch. 8.2: Cette exigence est reprise dans T7.1*, let. a), et dans la note de bas de page correspondante.

Ch. 8.3: Cette exigence est reprise par analogie, mais sous une forme très simplifiée dans S3.2*.

Ch. 8.4: Cette exigence est reprise dans T5.3. L'argumentation porte toutefois sur l'admissibilité des moyens d'authentification et de vérification d'identité à utiliser.

Ch. 9.1: Cette exigence est reprise dans T8.1 et T8.2.

Ch. 9.2: Cette exigence est reprise sous la notion de zone de gestion dans le modèle de zones de la Confédération. L'interdiction de principe d'accéder à Internet et aux outils bureautiques semble toutefois trop restrictive et peu pratique. Ces possibilités d'accès doivent être clarifiées dans la réglementation de la zone de gestion. L'exigence d'une authentification à deux facteurs est reprise dans T6.1. Les autres exigences relatives à l'administration relèvent de T8.1 et T8.2.

Ch. 9.3: Cette exigence ne semble plus judicieuse. Chaque procédure d'authentification utilisée limite de toute façon le temps à disposition.

Ch. 9.4: Cette exigence est reprise dans S5.2, mais uniquement pour les ordinateurs clients de l'administration fédérale. Elle apparaît trop radicale et peu conviviale pour les serveurs et les applications. Dans un cas particulier, une limite temporelle peut bien évidemment être opportune et être fixée en conséquence.

Ch. 10.1.1: Cette exigence est reprise sous une forme plus générale en tant que principe 5 (état de la technique). Elle renvoie au même document.

Ch. 10.1.3: On continue de se référer à la SG-PKI pour l'authentification à deux facteurs basée sur des certificats (note de bas de page relative à T6.1). Il n'est pas utile de préciser que chaque FP utilise uniquement des certificats de l'une des autorités de certification qu'il accepte.

Ch. 10.1.4: Cette exigence est reprise dans I2.1

Ch. 10.1.5/6: Ces exigences n'ont pas vraiment été mises en œuvre par le passé et n'ont vraisemblablement que des avantages limités. Elles ne sont donc pas reprises et ne figurent pas parmi les points relatifs aux mesures de protection qui doivent correspondre à l'état de la technique. L'obligation de documentation est intégrée à la gestion des clés.

Ch. 11.1.1/2: Ces exigences sont reprises dans O2.1, let. b).

Ch. 12.1.1: L'obligation de documentation est reprise sous une forme légèrement différente dans O2.

Ch. 12.1.2/3: Ces exigences ne sont pas directement applicables sous cette forme ou découlent de l'exploitation courante. Elles ne sont donc pas reprises et font plutôt l'objet d'un plan d'exploitation.

Ch. 12.1.4: Cette exigence est reprise dans T3. Toutefois, tous les objets à protéger ne disposent pas d'environnement de production (notamment dans le domaine du développement agile).

Ch. 12.2.1/2: Ces exigences sont reprises dans S4.3 (l'obligation d'informer résulte de P2).

Ch. 12.2.3: Cette exigence est reprise dans S2 et dans une note de bas de page correspondante.

Ch. 12.2.4: Cette exigence est reprise dans S5.3.

Ch. 12.3.1/2: Cette exigence est reprise par analogie dans I3.

Ch. 12.4.1: Cette exigence est reprise sous une forme simplifiée et résumée dans T2.1, let. c), et dans Z5 (pour les zones).

Ch. 12.4.2: Cette exigence n'est plus nécessaire sous cette forme (l'heure est synchronisée presque partout).

Ch. 12.4.3: Voir les remarques concernant le ch. 12.4.1.

Ch. 12.4.4: Cette exigence est reprise par analogie dans S4 (en particulier, S4.1 et S4.2).

Ch. 12.5.1: Cette exigence est reprise dans S4.1 (pour les systèmes informatiques) et dans A1.2, let. e) (pour les applications).

Ch. 12.6.1: Cette exigence est reprise dans S2 (pour les systèmes informatiques) et dans A2 (pour les applications).

Ch. 12.6.2: Cette exigence est reprise dans T4. Le renvoi à l'OWASP figure dans A1.1 et dans la note de bas de page correspondante.

Ch. 12.7.1/2: Cette exigence est reprise dans O2.1, let. g), et dans la note de bas de page correspondante.

Ch. 13.1.1: L'obligation de documentation relative aux réseaux s'applique conformément à O2. De plus, ceux-ci font partie d'une zone et doivent répondre aux prescriptions du modèle de zones selon Z1, qui englobent une telle obligation.

Ch. 13.1.2: La question de la virtualisation est clarifiée dans le principe 2 éponyme.

Ch. 13.1.3: Les éléments du réseau constituent également des systèmes informatiques. Cette exigence est donc reprise implicitement.

Ch. 13.1.4: Les principaux points de cette exigence sont repris dans T6.3 (authentification de l’utilisateur) et T8.3 (accès à distance). Les autres points figurent implicitement dans d’autres exigences.

Ch. 13.1.5: Eu égard à l’intégration de [Si003], cette exigence est implicitement reprise.

Ch. 13.1.6: Cette exigence est reprise et précisée dans Z5.2.

Ch. 13.1.7: Cette exigence est reprise dans I2 (les données d’authentification sont importantes pour les affaires et ont un besoin de protection accru).

Ch. 13.1.10: Cette exigence est reprise dans Z2.1, let. a).

Ch. 14.1.1: Cette exigence est reprise dans S6.1 et S6.4 (y c. [E026]).

Ch. 14.1.2: Cette exigence est reprise dans T2.1 et T7.2*.

Ch. 14.1.3: Cette exigence est reprise dans T2.2.

Ch. 14.1.4: Cette exigence est reprise dans T2.1, let. b).

Ch. 14.2.1: Cette exigence est reprise dans I2, qui précise que les données de test doivent être traitées comme des données de production.

Ch. 15.1.1: Cette exigence est reprise dans le principe 1 (forme de la fourniture de prestations) ainsi que dans O2.1, let. f), et dans I1*.

Ch. 15.2.1: Il va de soi que «la révélation de secrets de fonction à des FP informatiques externes doit être minimisée»; il ne faut donc pas le préciser ici. Sinon, l’exigence est reprise dans une large mesure dans T8.3.

Ch. 16.1/2: Ces exigences relèvent du processus de gestion des cyberincidents selon O4.

Ch. 17.1.1: Cette exigence est reprise dans O3 pour l’ITSCM et le BCM.