Federal Information Security Policy Guideline

Aperçu global
de la sécurité de l'information
au niveau fédéral

21/11/2019

FISPDOC08 V1.1

Remarque importante : Le présent document est un guide qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures présentées sont considérées comme des mesures minimales applicables raisonnablement de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales et des bonnes pratiques en matière de sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont requises pour un service fédéral pour des raisons réglementaires ou autres raisons formelles et impérieuses, on peut supposer que ces mesures sont prioritaires sur les mesures prévues dans le présent guide.

FISP

Groupe de travail

.be

Table des matières

Contenu de ce document

Orientation du document

Ce document fait partie intégrante de la méthodologie relative à la sécurité de l'information au sein de l'administration fédérale (projet FISP).

Objectif de sécurité du document

Le présent document décrit la politique de sécurité de l'information.

Champ d'application

Cette politique de sécurité de l'information est applicable à toutes les informations qui circulent dans les organisations fédérales.

Confidentialité du document

Distribution publique

Clause de non-responsabilité

Ces informations ne peuvent pas être utilisées individuellement comme documentation de référence. Ce document ne peut pas servir de substitut à la législation ou à des normes, mais vise à guider le lecteur dans la prise de mesures de sécurité appropriées.

Responsabilités

Ce document est destiné au conseiller en sécurité de l'information et au délégué à la protection des données (DPO) des institutions publiques fédérales, aux sous-traitants de l'information (y compris les sous-traitants de systèmes d'information) ainsi qu'aux autres intervenants dans des domaines connexes (ex. le gestionnaire de documents).

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

FISP

FISP (Federal Information Security Policy) est un guide en matière de sécurité de l'information qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures présentées sont considérées comme des mesures minimales applicables raisonnablement de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales, des bonnes pratiques dans le domaine de la sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP. Les conseils contenus dans ce guide sont rédigés de manière à offrir un soutien suffisant et à pouvoir être facilement appliqués par les instances fédérales.

L'objectif de cette politique consiste à garantir la disponibilité, l'intégrité et la confidentialité des informations au moyen de plusieurs guides de conseils. Ces guides accordent également l'attention nécessaire à l'identification, l'authentification et l'autorisation concernant l'accès à l'information.

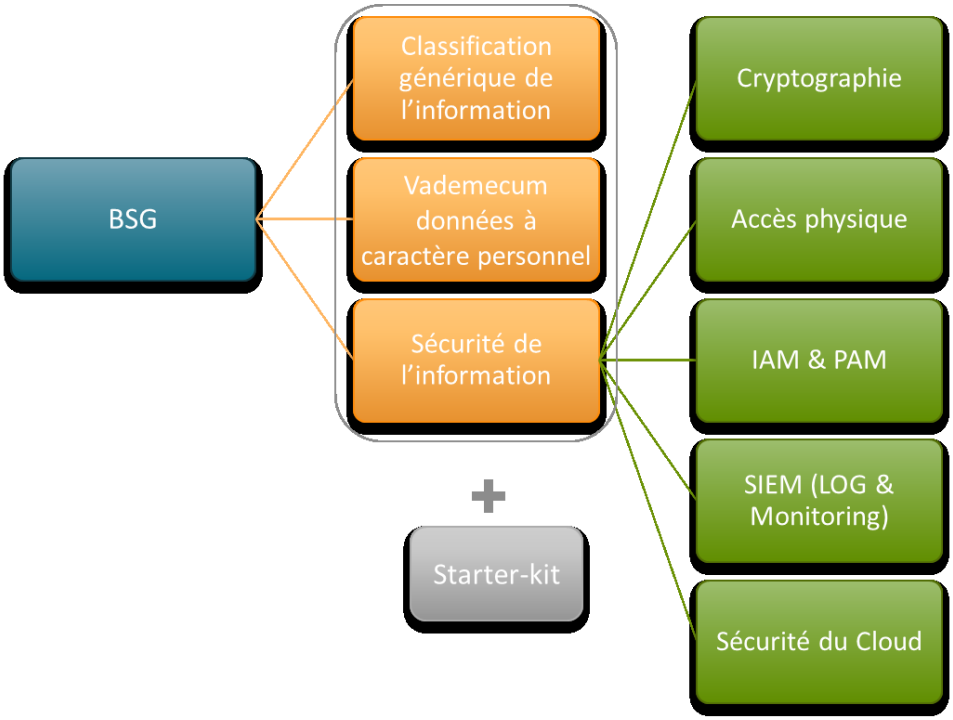
Ensuite, la politique de sécurité de l'information consiste en une classification générique de l'information, liée à des mesures spécifiques pour chacun de ces niveaux de classification. Il y a en outre un vade-mecum sur la protection des données à caractère personnel ainsi qu'un kit de démarrage reprenant quelques astuces pratiques globales pour l'utilisation du FISP.

La politique de sécurité de l'information est un complément aux BSG (Baseline information Security Guidelines) fournies par le Centre pour la Cybersécurité Belgique (CCB) et tient également compte des normes ISO 2700X existantes. Le paquet de mesures proposées en matière de sécurité de l'information n'est toutefois pas complet, étant donné qu'il y a des objectifs de sécurité qui ne sont pas encore traités de manière détaillée dans cette première version du FISP, par comparaison aux BSG. Il est recommandé de traiter les autres objectifs de sécurité lors des prochaines versions du FISP.

À noter également que cette politique de sécurité de l'information recommandée nécessite le soutien du management pour sa mise en œuvre dans leur organisation fédérale spécifique. La sécurité de l'information fait en effet partie intégrante d'une bonne gestion de l'organisation. L'implication du management favorise en outre le développement d'une culture de la sécurité et la mise en œuvre des mesures de sécurité proposées.

Si des mesures plus strictes sont nécessaires à un service fédéral pour des raisons réglementaires ou pour d'autres raisons formelles et contraignantes, il va de soi que ces mesures prévalent sur celles décrites dans le présent guide.

Organigramme des documents



Description des documents

Nom	*Réf. FISP*	*Contenu*
Aperçu général pour la sécurité de l'information au niveau fédéral	FISPDOC08	Il s'agit d'un document global qui fait référence à toutes les mesures de sécurité qui ont trait à la sécurité de l'information au niveau fédéral.
Guide pour la catégorisation des informations	FISPDOC01	Ce document décrit la manière dont les organisations fédérales, selon la sensibilité de l'information, doivent protéger l'information suivant une méthodologie afin de maîtriser et limiter les risques à certains niveaux de protection. Ces niveaux de protection s'expriment en niveaux de catégorisation.
Guide pour le contrôle et la sécurité des accès physiques	FISPDOC02	Ce document décrit les mesures recommandées en vue d'empêcher tout accès physique, dommage et interférence non autorisés aux informations et aux systèmes de traitement des informations des organisations fédérales.
Guide pour la cryptographie	FISPDOC03	Ce document décrit les mesures recommandées en matière de cryptographie. Il contient des informations suffisantes pour poser des choix (stratégiques) appropriés et créer une prise de conscience. Les mesures proposées sont liées à la proposition de catégorisation de l'information de FISP et aux différents contextes de données.

Guide pour le logging et le monitoring	FISPDOC04	Ce document décrit les mesures recommandées en matière de journalisation. Les mesures proposées sont liées à la catégorisation de l'information proposée par FISP. Le document comprend également des conseils pour les mesures à prendre pour la gestion du journal, des indications sur la rétention et la sécurité des enregistrements d'audit, sur la manière de gérer les erreurs dans les enregistrements d'audit et sur le suivi, l'analyse et le rapportage des audits.
Guide pour la sécurisation et la gestion des identités et des accès de base (IAM), et des accès privilégiés (PAM)	FISPDOC05	Dans ce document, les mesures générales IAM sont organisées selon la catégorisation de l'information proposée par le groupe de travail FISP. Ce document fait également référence au "Privileged Access Management" (PAM).
Guide pour un usage sécurisé du cloud	FISPDOC06	Ce document décrit les menaces, les risques technologiques et les mesures de sécurité pour les environnements Cloud.
Guide pour la protection des données à caractère personnel	FISPDOC07	Ce document décrit les exigences en matière de sécurité de l'information telles que définies par le règlement général sur la protection des données (RGPD). Il contient également une catégorisation standardisée basée sur l'interprétation du groupe de travail FISP.
Starter-kit • **Guide de démarrage** • **Glossaire** • **Tableau des rôles et responsabilités (RASCI**	• FISPDOC09 • FISPDOC10 • FISPDOC11	Ce document est un guide pratique pour les différentes autorités fédérales, avec des conseils d'ordre général pour l'application et la mise en œuvre de FISP.

Gestion du document

Historique

Date	*Auteur*	*Version*	*Description des modifications*
22/10/2019	BOSA	V.01	Première ébauche
04/11/2019	BOSA	V02	Mise à jour sur la base des commentaires formulés durant la réunion FISP
21/11/2019	FISP workgroup	V1.1	Distribution publique

Approbations

Date	*Approbateur(s)*	*Version*
21/11/2019	FISP FISP workgroup	V.1.1

Sources

Ce document a été rédigé à l'aide des sources suivantes :

- ISO/CEI 27001

Lien avec une autre politique

Dépendance de documents internes

Réf.	*Version*	*Titre*
		néant

Positionnement de la politique par rapport à la norme ISO 27001

Section	*Objectifs et mesures de référence*	*En relation (X = Oui)*
4	*Contexte de l'organisation*	
5	*Leadership*	*X*
6	*Planification*	
7	*Support*	
8	*Fonctionnement*	
9	*Évaluation des performances*	
10	*Améliorations*	

Positionnement de la politique par rapport à la norme ISO 27002

Section	*Objectifs et mesures de référence*	*En relation (X = Oui)*	*Objectifs/Mesures (Détail)*
A5	*Politique de sécurité de l'information*		
A6	*Organisation de la sécurité de l'information*		
A7	*Sécurité des ressources humaines*		
A8	*Gestion des actifs*		
A9	*Contrôle d'accès*		
A10	*Cryptographie*		
A11	*Sécurité physique et environnementale*		
A12	*Sécurité liée à l'exploitation*		
A13	*Sécurité des communications*		
A14	*Acquisition, développement et maintenance des systèmes d'information*		
A15	*Relations avec les fournisseurs*		
A16	*Gestion des incidents liés à la sécurité de l'information*		
A17	*Sécurité de l'information dans la gestion de la continuité de l'activité*		
A18	*Conformité*		