Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale
de la sécurité des systèmes d'information

Le guide PSSI

Élaboration de politiques de sécurité des systèmes d'information

Le guide PSSI constitue la référence nationale pour la rédaction des politiques de sécurité des systèmes d'information.

Il est largement utilisé au sein des administrations et du secteur privé. Sa diffusion est gratuite sur le site de la DCSSI (http://www.ssi.gouv.fr).

Les principes fondateurs

En 2002, le Conseil de l'OCDE a adopté une nouvelle version des "lignes directrices régissant la sécurité des systèmes et réseaux d'information – vers une culture de la sécurité"[1].

Elles insistent sur la nécessité d'un cadre général pour la sécurité des systèmes d'information (SSI).

Elles prennent en compte les évolutions du contexte de la SSI tels que l'accroissement de l'interconnexion des réseaux et l'évolution des données en terme de type, volume, sensibilité, ainsi que les nouveaux enjeux liés par exemple aux projets gouvernementaux et de commerce électronique.

Elles introduisent les notions de "culture de sécurité" et de continuité de la gestion des risques SSI.

Ces nouvelles lignes directrices décrivent les neuf principes suivants, à l'origine du guide PSSI :

1. Sensibilisation
2. Responsabilité
3. Réaction
4. Éthique
5. Démocratie
6. Évaluation des risques
7. Conception et mise en œuvre de la sécurité
8. Gestion de la sécurité
9. Réévaluation

[1] Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information – vers une culture de la sécurité, 29 juillet 2002, Organisation de Coopération et de Développement Économiques (OCDE).

Le socle de la SSI

La PSSI constitue le principal document de référence en matière de SSI. Elle en est un élément fondateur, au même titre qu'un schéma directeur, qui lui, définit les objectifs à atteindre et les moyens accordés pour y parvenir.

Ces documents sont établis en fonction de la culture et du référentiel existant.

Les orientations stratégiques

Une PSSI reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration…) en matière de SSI. Elle traduit la reconnaissance officielle de l'importance accordée par la direction à la SSI.

Elle informe la maîtrise d'ouvrage et la maîtrise d'œuvre des enjeux, des choix en terme de gestion des risques et suscite la confiance des utilisateurs et partenaires.

Un facteur d'économie

D'une PSSI globale, il est possible de décliner des PSSI techniques par métier, activités ou systèmes. Elle servira également de base de cohérence entre ces PSSI et entre toutes les études SSI.

Un instrument de sensibilisation et de communication

Après validation, la PSSI doit être diffusée à l'ensemble des acteurs du SI (utilisateurs, sous-traitants, prestataires…). Elle constitue alors un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir.

Un document évolutif

La PSSI est un document vivant qui doit évoluer afin de prendre en compte les transformations du contexte de l'organisme (changement d'organisation, de missions...) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux).

Une démarche basée sur l'analyse des risques SSI

Le guide propose une démarche d'élaboration de la PSSI décomposée en 4 phases :

- ✓ organisation du projet PSSI et constitution du référentiel,
- ✓ recueil des éléments stratégiques,
- ✓ choix des principes et déclinaison en règles adaptées au contexte (graduation des moyens),
- ✓ finalisation et validation de la PSSI et de son plan d'action.

La réalisation préalable d'une analyse des risques SSI (pour cela, la DCSSI préconise la méthode EBIOS) facilite l'élaboration d'une PSSI notamment pour :

- ✓ déterminer les éléments stratégiques,
- ✓ choisir les principes à développer,
- ✓ guider l'élaboration des règles,
- ✓ assurer la cohérence avec les objectifs de sécurité identifiés pour l'organisme.

Organisation en projet PSSI

La démarche du guide d'élaboration de PSSI prévoit une organisation sous la forme d'un véritable projet :

- ✓ un chef de projet désigné,
- ✓ des groupes de travail constitués,
- ✓ des ressources allouées,
- ✓ un calendrier fonction des étapes de la méthode,
- ✓ des livrables identifiés (notes de cadrage et de stratégie, synthèses des règles et impacts, PSSI, plan d'action).

Cette organisation facilite l'élaboration, les validations et l'implication des acteurs. Elle permet ainsi de trouver le meilleur compromis entre décideurs, responsable SSI, MOA, MOE, utilisateurs, financiers, ressources humaines dans la gestion des risques SSI…

Un référentiel de principes de sécurité

Le guide décrit plus de 160 principes de sécurité organisés en 16 domaines :

1. politique de sécurité,
2. organisation de la sécurité,
3. gestion des risques SSI,
4. sécurité et cycle de vie,
5. assurance et certification,
6. aspects humains,
7. planification de la continuité des activités,
8. gestion des incidents,
9. sensibilisation et formation,
10. exploitation,
11. aspects physiques et environnementaux,
12. identification / authentification,
13. contrôle d'accès logique,
14. journalisation,
15. infrastructures de gestion des clés cryptographiques,
16. signaux compromettants.

Ces principes de sécurité couvrent les normes ISO/IEC 13335, 15408 et 17799.

Les références SSI

Les références SSI du guide PSSI permettent de disposer de pistes de réflexion et de ne rien omettre quant aux évolutions récentes de la réglementation et des normes :

- ✓ les réglementations nationales et internationales (atteinte aux personnes, atteinte aux biens, atteinte aux intérêts fondamentaux de la nation, terrorisme et atteinte à la confiance publique, atteintes à la propriété intellectuelle, cryptologie, signature électronique…),
- ✓ les lignes directrices de l'OCDE (SSI, cryptographie…),
- ✓ les codes d'éthique,
- ✓ les critères communs d'évaluation (ISO/IEC 15408),
- ✓ les guides méthodologiques.

Tous ces avantages font du guide PSSI l'outil indispensable pour élaborer des politiques SSI.

Toutes les remarques et contributions peuvent être adressées à la DCSSI par courrier électronique (conseil.dcssi@sgdn.pm.gouv.fr).