Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Élaboration de politiques de sécurité des systèmes d'information

PSSI

MÉMENTO

Version du 3 mars 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Introduction

Dès 1992, les lignes directrices[1] de l'OCDE insistaient sur la nécessité d'un cadre général pour la sécurité des systèmes d'information (SSI). En effet, ce cadre permet de promouvoir la coopération entre différentes organisations en terme de sécurité, d'améliorer la sensibilisation aux risques SSI et de renforcer la confiance envers le système d'information.

C'est la raison pour laquelle le guide pour l'élaboration d'une Politique de Sécurité Interne (PSI)[2] a été créé et publié par le SCSSI[3] en 1994. Il présentait les fondements de la politique de sécurité interne, des principes de sécurité organisés par domaines et des références réglementaires et documentaires. Il permettait ainsi de justifier l'élaboration de politiques de sécurité et d'aider le responsable SSI à réfléchir sur l'ensemble des thèmes à aborder.

Le guide PSI a rencontré un grand succès dans le secteur public et privé en tant que guide de référence (il est en effet parmi les 7 documents les plus téléchargés sur le site Internet de la DCSSI depuis 1999).

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"[4] afin de prendre en compte les évolutions du contexte de la SSI : 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.

Les nouvelles lignes directrices introduisent les notions de "culture de sécurité" et de processus continu de gestion des risques SSI.

Les nouvelles lignes directrices de l'OCDE décrivent les neuf principes issus de la recommandation[5] adoptée le 25 juillet 2002 :

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] Recommandation du Conseil et annexe (lignes directrices régissant la sécurité des systèmes d'information), 26 novembre 1992, Organisation de Coopération et de Développement Économiques (OCDE).

[2] Guide pour l'élaboration d'une Politique de Sécurité Interne (PSI) à l'usage du responsable de la sécurité du système d'information, version 1.1, 15 septembre 1994, Service Central de la Sécurité des Systèmes d'Information (SCSSI).

[3] Héritière du Service central de la sécurité des systèmes d'information (SCSSI), la Direction centrale de la sécurité des systèmes d'information (DCSSI) a été instituée par décret (décret n°2001-693 du 31 juillet 2001 créant au Secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information).

[4] 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).

[5] http://www.oecd.org/pdf/M00033000/M00033183.pdf

Afin de maintenir la cohérence avec ces lignes directrices, la DCSSI a mis à jour le guide PSI de 1994, qui est devenu le guide d'élaboration de Politiques de Sécurité des Systèmes d'Information (PSSI) en 2003.

La révision a consisté à :

- ✓ développer l'approche méthodologique d'élaboration de PSSI,
- ✓ réorganiser et enrichir les principes de sécurité,
- ✓ étendre le champ d'application de la PSSI (politique globale déclinée en politiques spécifiques),
- ✓ mettre à jour les références.

Un mémento présente ces principes sur le site web de la DCSSI (http://www.ssi.gouv.fr/OCDE-lignesdir.pdf).

Qu'est-ce qu'une PSSI ?

La formulation des orientations stratégiques

La Politique de Sécurité des Systèmes d'Information (PSSI) reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration…) en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI.
Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme.

La validation de la PSSI par la direction traduit la reconnaissance officielle accordée à la sécurité de son système d'information.
La PSSI vise à informer la maîtrise d'ouvrage et la maîtrise d'œuvre des enjeux tout en l'éclairant sur ses choix en terme de gestion des risques et à susciter la confiance des utilisateurs et partenaires envers le système d'information.

Un socle fondateur de la SSI

D'une manière générale, il convient de disposer d'un socle fondateur de la SSI pour l'organisme. Celui-ci sera établi en fonction de sa culture et du référentiel existant. La PSSI constitue l'un de ces documents fondateurs et un élément de la culture de sécurité.

La PSSI s'inscrit dans le système de management de l'organisme, donc de la sécurité des informations et processus, puis enfin de la SSI. Elle constitue en effet le premier document à formaliser dans l'étape de planification et sera suivie des étapes de mise en œuvre, de vérification et d'amélioration du système de management de la SSI.

Dans le cas où il existe un schéma directeur du système d'information comportant un volet SSI ou un schéma directeur SSI, le rôle de la PSSI est de le traduire en règles de sécurité applicables et de contrôler que le schéma directeur SSI est conforme avec les objectifs et contraintes de l'organisme. La PSSI peut aussi servir de base à l'élaboration d'un volet SSI du schéma directeur du système d'information ou bien d'un schéma directeur SSI, décrivant alors comment devront être mises en œuvre les règles de sécurité.

Un facteur d'économie

Une PSSI globale peut être déclinée en PSSI techniques par application ou métier, en procédures à mettre en œuvre et en chartes de sécurité.

Elle servira aussi de base à la factorisation des études de sécurité portant sur le même périmètre que la PSSI afin de garantir une cohérence globale.

La PSSI permet ainsi de réaliser des économies pour tous les travaux relatifs à la SSI puisque son contenu peut être réutilisé par les maîtrises d'ouvrage et les maîtrises d'œuvre en y ajoutant les effets d'une mutualisation des mécanismes mis en place. À titre d'exemple, les analyses de risques intégreront les éléments stratégiques de la PSSI et les règles de sécurité devant être respectées. Le référentiel des audits sera également élaboré à partir de la PSSI afin de vérifier la conformité de celle-ci vis-à-vis de la réalité.

Un instrument de sensibilisation

Après validation, la PSSI doit être largement communiquée à l'ensemble des acteurs du SI, qu'ils soient utilisateurs internes, sous-traitants, prestataires ou stagiaires. La PSSI constitue alors un véritable outil de sensibilisation aux risques SSI, aux moyens disponibles pour s'en prémunir et à l'organisation SSI. Par ailleurs, elle aide l'ensemble des acteurs à prendre conscience de leurs responsabilités et participe à l'amélioration de la culture de sécurité.

Un document évolutif

La PSSI doit être régulièrement révisée afin de prendre en compte les évolutions du contexte (modifications des processus, du système d'information, des personnels, de l'organisation) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux).
Cette adaptation peut être faite systématiquement ou bien déclenchée par une évolution majeure du contexte ou la survenance d'une agression et des leçons que l'on peut en tirer.

Les 5 atouts du guide PSSI

1 - Une démarche basée sur l'analyse des risques

La réalisation préalable d'une analyse des risques SSI (par exemple à l'aide la méthode EBIOS®) facilite l'élaboration d'une PSSI. Elle a pour effet de déterminer plus facilement les éléments stratégiques, de déterminer les critères de sélection des principes de sécurité à développer et de guider l'élaboration des règles de sécurité.

Les principes de sécurité sont l'expression des orientations de sécurité nécessaires et des caractéristiques importantes de la sécurité. Ils constituent une base de réflexion pour l'élaboration d'une politique et en particulier des règles de sécurité la composant.
Les règles de sécurité définissent des exigences de sécurité pour la mise en place des moyens techniques et organisationnels, et sur les comportements par déclinaison des principes retenus. Elles sont construites par déclinaison des principes dans un environnement et un contexte donnés.

La cohérence avec les objectifs de sécurité identifiés pour l'organisme est ainsi assurée.

2 - 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 est désigné,
- ✓ des groupes de travail sont constitués (utilisation, technique, pilotage, exploitation),
- ✓ des ressources sont allouées (budget, hommes…),
- ✓ un calendrier est conçu en fonction des étapes de la méthode (préalables, élaboration des éléments stratégiques, sélection des principes et rédaction des règles, finalisation),
- ✓ des livrables sont identifiés (note de cadrage, note de stratégie, synthèse des règles de sécurité, synthèse des impacts, PSSI, plan d'action).

Cette organisation facilite l'élaboration, les validations et l'implication des acteurs. Elle permet aussi d'ouvrir les discussions afin de trouver un compromis entre décideurs, RSSI, maîtrises d'ouvrage, maîtrises d'œuvre, utilisateurs, financiers, ressources humaines…

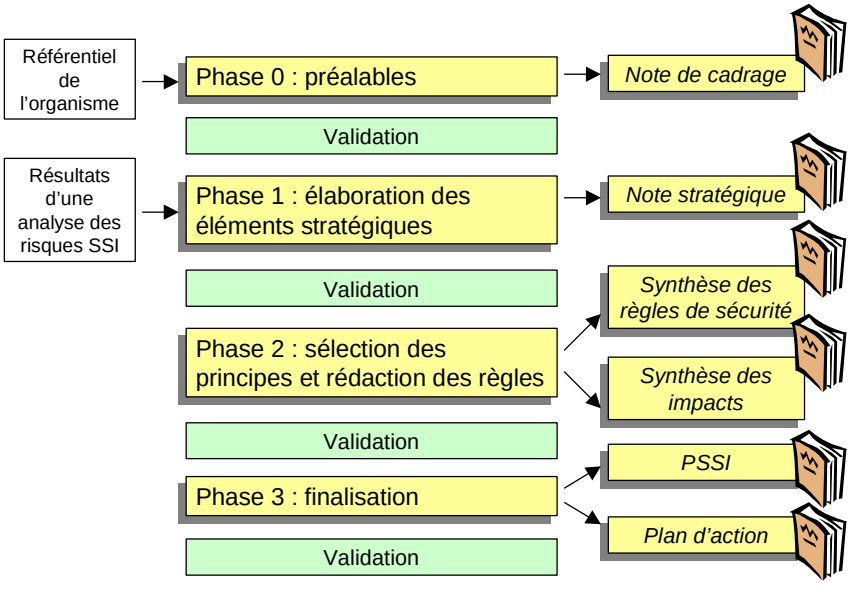
3 - La méthodologie

L'élaboration d'une PSSI requiert une approche globale, considérant non seulement les domaines techniques tels que la sécurité logique, la sécurité des matériels informatiques et la sécurité des réseaux, mais aussi les domaines non techniques tels que la sécurité physique, la sécurité liée aux aspects humains et la sécurité organisationnelle.
Les règles de sécurité seront alors réalistes et cohérentes pour un périmètre généralement large et un champ d'application étendu.

Conduire un projet PSSI, c'est avant tout faire naître ou renforcer une culture de sécurité. C'est par la démarche proposée dans le guide que les équipes en charge de la rédaction d'une PSSI assureront la cohérence des objectifs de sécurité de l'organisme et contribueront à la sensibilisation et l'implication des personnels.

Le guide propose en outre un plan type pour les PSSI, ce qui améliore l'homogénéité des PSSI en interne (PSSI globale et PSSI spécifiques) et en externe (comparaisons avec d'autres organismes), garantissant l'exhaustivité du contenu (éléments stratégiques, règles de sécurité organisées par domaine).

La démarche d'élaboration de PSSI de la DCSSI est décomposée en quatre phases successives :



- ✓ La phase 0 est un préalable à la démarche d'élaboration. Elle consiste à organiser le projet PSSI (chef de projet, comité de pilotage, calendrier, disponibilité d'un budget et d'objectifs de sécurité…) et à constituer le référentiel (du système d'information, de la SSI, des aspects déontologique et contractuels). Une note de cadrage formalise les informations nécessaires pour cette phase.

- ✓ La phase 1 permet de recueillir l'ensemble des éléments stratégiques nécessaires à la rédaction d'une note de stratégie de sécurité qui servira de base à l'élaboration de la PSSI et à toute autre étude de sécurité.
  Ces éléments stratégiques forment le périmètre que doit couvrir la PSSI. Ils sont constitués des enjeux et des orientations stratégiques en matière de SSI, de la prise en compte des aspects légaux et réglementaires, de l'élaboration d'une échelle de besoins, de l'expression des besoins de sécurité généraux, de l'identification des éléments menaçants et de leurs méthodes d'attaque.

- ✓ La phase 2 consiste à choisir les principes de sécurité à prendre en compte dans le référentiel du guide et à les décliner en règles de sécurité sur la base des éléments stratégiques.
  Des synthèses des règles de sécurité (adressée au comité de pilotage) et des impacts organisationnels et financiers (adressés à la Direction générale) doivent être rédigées.

- ✓ La phase 3 permet de finaliser et de valider la PSSI ainsi que son plan d'action.

4 - Le référentiel de principes de sécurité

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

- ✓ principes organisationnels :
  1. politique de sécurité,
  2. organisation de la sécurité,
  3. gestion des risques SSI,
  4. sécurité et cycle de vie,
  5. assurance et certification ;
- ✓ principes de mise en œuvre :
  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 ;
- ✓ principes techniques :
  12. identification / authentification,
  13. contrôle d'accès logique,
  14. journalisation,
  15. infrastructures de gestion des clés cryptographiques,
  16. signaux compromettants.

Ces principes de sécurité permettent de couvrir l'ensemble des sections de l'ISO/IEC 13335 (GMITS), ainsi que l'ensemble des domaines de l'ISO/IEC 17799 et d'assurer la compatibilité avec l'ISO/IEC 15408 (critères communs d'évaluation).
La démarche permet de décliner les principes en règles de sécurité cohérentes et adaptées au contexte (graduation des moyens).

5 - Les références SSI

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

- ✓ réglementation nationale et internationale (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…),
- ✓ lignes directrices de l'OCDE,
- ✓ code d'éthique,
- ✓ critères communs d'évaluation,
- ✓ guides méthodologiques.

Ces pistes de réflexion pourront être mises à jour indépendamment de la méthodologie, ce qui offre la possibilité de suivre l'actualité et d'améliorer ainsi la couverture.

Conclusion

Le nouveau guide PSSI est disponible gratuitement sur le site web de la DCSSI (http://www.ssi.gouv.fr).

Les principales améliorations ont consisté à mettre à jour les références et les principes de sécurité, à étendre le domaine d'application de la PSSI et à développer une véritable démarche d'élaboration de PSSI.

Elles font du guide PSSI un outil méthodologique indispensable dans le cadre de la gestion de la SSI au sein de l'État et des entreprises.