

P R E M I E R M I N I S T R E

Secrétariat général
de la défense
nationale

*Direction centrale de la
sécurité des systèmes
d'information*

Mise en œuvre en France des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information adoptées le 25 juillet 2002

1. Dissémination des nouvelles lignes directrices de l'OCDE

Depuis septembre 2002, le Secrétariat général de la défense nationale (SGDN), et plus particulièrement la Direction centrale de la sécurité des systèmes d'information (DCSSI) publie un [mémento](#) relatif à ces nouvelles lignes directrices sur son site web.

2. Mise en œuvre des nouvelles lignes directrices

La France a déjà mis en œuvre un grand nombre de mesures visant à promouvoir la culture de sécurité. Elles s'inscrivent parfaitement dans les actions répertoriées dans le plan d'application des lignes directrices de l'OCDE. La plupart des informations et des outils disponibles pour le public est regroupée sur un [serveur thématique sur la sécurité des systèmes d'information](#).

2.1. Politique nationale visant la sécurité de l'information

La France a mis en place et tient à jour un cadre juridique visant à garantir la sécurité des systèmes d'information et prenant en compte l'évolution de la société de l'information.

Dès 1988, la loi « Godfrain » avait complété le dispositif pénal existant en sanctionnant les actes de vandalisme appliqués aux systèmes d'information, permettant ainsi de lutter contre des formes de criminalité informatique telles que les virus, les bombes logiques ou les « chevaux de Troie » (logiciels espions ayant pour but de surveiller un site ou un système informatique, voire de le contrôler à distance).

D'autre part, un [projet de loi récent pour la confiance dans l'économie numérique](#), en cours d'examen au Parlement, prévoit de renforcer cet arsenal juridique et d'aggraver les peines sanctionnant le fait d'accéder ou de se maintenir frauduleusement dans toute ou partie d'un système de traitement automatisé de données, d'en entraver ou d'en fausser le fonctionnement, et d'y introduire ou d'y supprimer frauduleusement des données.

Cet arsenal juridique est conforme à la Convention sur la cybercriminalité du Conseil de l'Europe, signée par la France en 2001 et [en cours de ratification](#), et au projet européen de décision cadre relatif aux attaques visant des systèmes d'information, en cours de discussion au Conseil de l'Union européenne et au Parlement européen.

2.2. Coopération transfrontière

La France est l'un des premiers pays à avoir appartenu au réseau 24/7 mis en place par le G8 à l'origine et qui relie actuellement 29 pays. Ce réseau transfrontière que les pays membres peuvent activer à tout moment doit permettre de faciliter les contacts en cas d'urgence. L'idée de ce réseau a d'ailleurs été reprise dans la Convention sur la cybercriminalité du Conseil de l'Europe.

2.3. Diffusion des alertes et notes d'information

Le [CERTA](#) est une structure d'alerte et d'assistance sur l'Internet, chargée d'une mission de veille et de réponse aux attaques informatiques. Les deux principaux objectifs du CERTA sont d'assurer la détection des vulnérabilités et la résolution d'incidents concernant la sécurité des systèmes d'information (SSI) ainsi que l'aide à la mise en place de moyens permettant de se prémunir contre de futurs incidents.

Pour ce faire, le CERTA met à disposition du public sur son site web :

- des alertes destinées à prévenir un danger immédiat,
- des avis faisant état de vulnérabilités et de moyens de s'en prémunir,
- des notes d'information faisant état de phénomènes à porter générale,
- de recommandations.

En effet, si le CERTA a été mis en place pour renforcer et coordonner la lutte contre les systèmes informatiques de l'Etat, il informe également le public avec quelques jours de retard.

2.4. Sensibilisation et mise à disposition de méthodes de sécurisation des systèmes informatiques

Les travaux du bureau conseil de la DCSSI appliquent les principes contenus dans les nouvelles lignes directrices de l'OCDE. On peut citer entre autres :

- la mise à jour d'un [guide d'élaboration de politique de sécurité des systèmes d'information](#) (PSSI), qui propose une démarche pour élaborer des PSSI et présente un catalogue de principes de sécurité à implémenter en règles de sécurité selon le contexte. Ce guide est compatible avec les nouvelles lignes directrices (l'ancien reposait sur les lignes directrices de 1992),
- la diffusion de la méthode d'analyse des risques [EBIOS](#) (expression des besoins et d'identification des objectifs de sécurité), qui est largement diffusée et employée dans les secteurs publics et privés et pour laquelle des formations sont assurées par le centre de formation de la DCSSI :
 - o elle contribue à la gestion des risques, l'un des principes des lignes directrices, et à la réévaluation des risques, un autre principe,
 - o les réflexions sur le processus continu de gestion des risques SSI sont compatibles avec les nouvelles lignes directrices,
- la communication au sujet de la SSI sous la forme de sensibilisations, d'information, de formation, de mémentos ou de bonnes pratiques qui contribuent au principe de sensibilisation.

2.5. Sensibilisation des agents de l'Etat aux questions de sécurité

Le [centre de formation à la sécurité des systèmes d'information](#) (CFSSI), créé en 1986 et rattaché à la DCSSI, est l'acteur central d'un réseau de sensibilisation aux problèmes de la sécurité des systèmes d'information et le lieu de formation d'experts hautement qualifiés aux différents métiers de la discipline.

Le CFSSI propose des stages allant de la journée de sensibilisation à deux ans pour la préparation d'un brevet d'études supérieures de la sécurité des systèmes d'information. Les stages et journées de sensibilisation sont réservées à la formation et à l'information des agents de l'Etat dont les fonctions justifient cette formation.