

## La sécurité des systèmes d'information : bibliographie réalisée par l'Infothèque pour le Symposium HEG 2008

### *Définition de la sécurité des systèmes d'information*

Ensemble de mesures de sécurité physiques, logiques, administratives, et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer la protection de ses biens informatiques, la confidentialité des données de son système d'information et la continuité de service.

La sécurité [des systèmes d'information] comporte trois aspects : la protection physique des installations, la protection des données contre la consultation, la modification ou la dégradation, effectuées de façon volontaire ou accidentelle par des personnes non autorisées, et la protection de la fiabilité de ces données (c'est-à-dire la conservation de leur contenu au fil du temps ou lors de leur traitement).

La sécurité [des systèmes d'information] ne résulte pas d'une accumulation de moyens, mais est plutôt associée à une démarche méthodique d'analyse et de réduction des risques. Ainsi, de nombreuses techniques sont mises en oeuvre pour réduire la vulnérabilité vis-à-vis des risques informatiques ; elles concernent notamment l'organisation de l'entreprise, le contrôle des accès aux systèmes d'information, la protection des télécommunications, le plan de secours, les consignes de sécurité, la qualité des logiciels, les sauvegardes, le chiffrement, etc.

(Source : OFFICE QUEBECOIS DE LA LANGUE FRANCAISE. Sécurité informatique : définition. In : *BV – Lexiques et vocabulaires ... en toute sécurité informatique* [en ligne]. [http://www.olf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie\\_sec\\_informatique/securite\\_informatique.html](http://www.olf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/securite_informatique.html) (consulté le 21.07.2008)

### *Sécurité et entreprise*



►► LE GUYADER, Patrick. *Protection du patrimoine des entreprises et des institutions : menaces, risques, parades*. Paris : Hermès, 2006. 313 p.

#### **COTE HEG : 658.478 LEG**

Cet ouvrage présente un dispositif organisationnel à instaurer dans le cadre d'une démarche sécuritaire. Il décrit les actions principales à réaliser telles que l'audit de sécurité physique et logique, la rédaction d'une politique de sécurité en partenariat avec les principaux dirigeants et acteurs responsables de l'entreprise afin de respecter la loi, identifier les informations sensibles et les classer. Enfin, ce livre souligne l'importance de définir des solutions simples et flexibles. Il insiste sur la nécessité d'informer, de sensibiliser et de former les professionnels sur l'ensemble des dispositions de sécurité.

## Internet



►►BRAUX, Bertrand. Comment les entreprises françaises gèrent-elles leur sécurité ?. In : *01net* [en ligne]. 19.06.2008

<http://www.01net.com/editorial/382833/comment-les-entreprises-francaises-gerent-elles-leur-securite-/>

(consulté le 03.11.2008)

Le Club de la sécurité de l'information français (Clusif) vient de publier les résultats de son enquête 2008 sur les pratiques de sécurité informatique auprès de 350 entreprises françaises.



►►CLUSIF. *CLUSIF : bienvenue* [en ligne]. 2008.

<http://www.clusif.asso.fr/>

(consulté le 03.11.2008)

Le CLUSIF est un club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité. Il accueille des utilisateurs et des offreurs issus de tous les secteurs d'activité de l'économie. La finalité du CLUSIF est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques. Il entend ainsi sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion : management des risques, droit, intelligence économique ...



►►CLUSIS. *CLUSIS* [en ligne]. 2008.

<http://www.clusis.ch>

(consulté le 03.11.2008)

Le CLUSIS (Association suisse de la sécurité des systèmes d'information) a les mêmes objectifs que le CLUSIF décrit ci-dessus. Toute personne intéressée par le domaine peut devenir membre et à ce titre accéder à l'espace réservé qui contient de nombreux articles, les supports des conférences et séminaires organisés par le CLUSIS, mais aussi une newsletter et des liens utiles.



►►CSO. *CSO Online : security and risk* [en ligne]. 11.08.2008

<http://www.csoonline.com/>

(consulté le 03.11.2008)

Spécialisé dans la sécurité informatique, ce site (en anglais) propose différents outils destinés au directeur du service informatique (CSO = Chief Security Officer). Des articles sur l'actualité du domaine sont mis à disposition régulièrement, ainsi qu'un vaste choix de newsletters. Des guides thématiques (White papers) sont également téléchargeables gratuitement.



►►DCSSI. *Portail officiel de la sécurité informatique – DCSSI – République française* [en ligne]. 31.07.2008

<http://www.securite-informatique.gouv.fr/>

(consulté le 03.11.2008)

La sécurité informatique désigne un ensemble de techniques et de bonnes pratiques pour protéger les ordinateurs et les données qui y sont stockées. Si elles sont élaborées par des spécialistes, les plus simples doivent être connues et mises en œuvre par tous les utilisateurs. C'est l'objectif de ce portail d'information qui propose des fiches pratiques et des conseils destinés à tous les publics (particuliers, professionnels, PME). Il comporte également des actualités et avertit de menaces nouvellement rencontrées qui appellent une action rapide des utilisateurs pour en limiter les effets.

## Prendre conscience des risques

### Hackers et virus ne sont pas les seuls à menacer vos informations



►► LAFITTE, Michel. *Sécurité des systèmes d'information et maîtrise des risques*. Paris : Revue Banque, 2003. 127 p. (Les essentiels de la banque)

**COTE HEG : 658.478 LAF**

Le XXI<sup>e</sup> siècle sera le siècle des réseaux de télécommunications, du nomadisme et de la virtualité. L'interconnexion généralisée entre les organisations deviendra progressivement la règle. Dans le cadre de ce nouveau paradigme organisationnel, les préoccupations sécuritaires constitueront progressivement un enjeu stratégique majeur pour les entreprises, notamment celles du secteur financier qui gèrent des flux immatériels. À partir des caractéristiques de ce nouveau paysage technologique, cet ouvrage montre la diversité et la complexité des problèmes sécuritaires liés à l'émergence des réseaux ouverts. Il dresse ensuite un panorama des techniques sécuritaires, de leurs forces et de leurs faiblesses, puis propose une typologie des risques encourus par les organisations. Il explicite enfin, à partir d'une vision assurancière des risques, les fondements d'une politique sécuritaire d'entreprise.



►► BLOCH, Laurent, WOLFHUGEL, Christophe. *Sécurité informatique : principes et méthodes*. Paris : Eyrolles, 2007. 261 p.

**COTE HEG : 005.8 BLO**

Comprendre les menaces informatiques pour les juguler : l'administrateur et le responsable informatique affrontent une insécurité informatique protéiforme et envahissante, qui menace tant les données que les applications de l'entreprise virus, attaques par le réseau, tromperie sur le web, etc. Bien des outils sont proposés pour y faire face, mais encore faut-il comprendre leur rôle et leur mode opératoire et les replacer dans le cadre d'une politique de sécurité efficace. On devra pour cela garder en tête les principes qui animent tout système d'information et chasser de dangereuses idées reçues. Une approche systématique de la sécurité informatique : écrit par le responsable de la sécurité des systèmes d'information de l'INSERM, ce livre expose les causes des risques inhérents à tout système informatique - et les moyens de s'en protéger.

#### Internet



►► BISEUL, Xavier et al. Les usages issus du web 2.0 mettent les DSI sous pression. In : *01 net* [en ligne]. 29.07.2008  
<http://www.01net.com/editorial/387522/les-usages-issus-du-web-2.0-mettent-les-dsi-sous-pression/>  
(consulté le 03.11.2008)

Le périmètre de l'entreprise étendue voit ses frontières remises en cause par les usages du web 2.0. Plutôt que de lutter à contre-courant d'un phénomène massif et planétaire, les DSI se doivent d'accompagner le mouvement.

## Méthode simple pour analyser les risques de votre PME, organisation ou service

### Internet



►► La méthode EBIOS. In : *SecuriteInfo.com* [en ligne]. 20.07.2007  
<http://www.securiteinfo.com/conseils/ebios.shtml>  
(consulté le 03.11.2008)

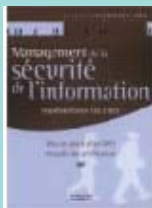
EBIOS signifie : Expression des Besoins et Identification des Objectifs de Sécurité. Cette méthode a été mise en place par la Direction centrale de la sécurité des systèmes d'information. Méthode reconnue par les différentes administrations françaises, la méthode EBIOS consiste à formaliser les besoins de sécurité et les menaces, et permet de déterminer les risques pesant sur les périmètres à auditer.



►► SAINSON, Véronique. Stratégie de sécurité dans les PME-PMI et collectivités. In : *SecuriteInfo.com* [en ligne]. 16.08.2007  
[http://www.securiteinfo.com/conseils/strategie\\_securite\\_informatique\\_pme\\_pmi.shtml](http://www.securiteinfo.com/conseils/strategie_securite_informatique_pme_pmi.shtml)  
(consulté le 03.11.2008)

Les PME-PMI, les collectivités ou les associations employant du personnel prennent rarement le temps de formaliser une véritable stratégie de sécurité. Par manque de temps, par manque de moyens ou de ressources, elles pensent pouvoir faire l'économie de cette réflexion qui pourtant est indispensable en cas de crise informatique. Une stratégie ou politique de sécurité doit servir à limiter un certain nombre de risques ou en cas de crise permettre de limiter au maximum les conséquences sur l'activité.

## Bien gérer la sécurité des systèmes d'Information grâce aux « bonnes pratiques » extraites des normes ISO 27001 et 27002



►► FERNANDEZ-TORO, Alexandre. *Management de la sécurité de l'information : Implémentation ISO 27001, mise en place d'un SMSI et audit de certification*. Paris : Eyrolles, 2007. 255 p.

### COTE HEG : 658.478 FER

En dépit d'une panoplie d'outils et de techniques de sécurité toujours plus efficaces en informatique, bien des sociétés sont encore victimes d'actes de malveillance. Et pour cause ! Les mesures de sécurité sont souvent déployées au jour le jour, sans orchestration ni attachement aux besoins réels de l'entreprise. C'est pourquoi il devient nécessaire de mettre en place un système de management de la sécurité de l'information (SMSI). Cet ouvrage apporte des éléments indispensables à la compréhension et à l'application de la norme ISO 27001, qui s'est imposée comme référence pour les SMSI, en s'appuyant notamment sur les recommandations de la norme ISO 27002 qui lui est associée. A la lumière de sa longue expérience, l'auteur explique la démarche à suivre pour mettre en place un SMSI, en insistant sur les pièges à éviter, et offre un guide précieux dans la préparation de l'audit de certification ISO 27001 d'un système de management de la sécurité du système d'information.



►► LINLAUD, Daniel. *Sécurité de l'information : élaboration et gestion de la politique de l'entreprise suivant l'ISO 17799*. Saint-Denis La Plaine : AFNOR, 2003. 249 p.

**COTE HEG : 658.478 LIN**

Conçu de façon pédagogique et pragmatique, cet ouvrage apporte un éclairage précieux sur toutes les étapes de la définition d'un système de gestion de l'information, de nombreux conseils pratiques et des outils (questionnaires, exemples, tableaux et modèles d'application) pour élaborer et gérer la politique de sécurité de l'information de l'entreprise. Il offre une méthodologie qui permet à tous ceux qui le souhaitent, dirigeants ou responsables des systèmes d'information, d'optimiser leur système de gestion de l'information, de suivre le processus de sécurisation de l'information et d'en mesurer l'efficacité. Il donne en plus des recommandations indispensables pour préparer la certification selon la norme BS7799-2.

### Normes



►► AFNOR. *Sécurité informatique : manager et assurer*. Saint-Denis La Plaine : AFNOR, 2008. 3e éd. Recueil de normes. Informatique

**COTE HEG : REF. 658.478 ASS**

Les systèmes d'information et de communication sont impliqués dans pratiquement toutes les activités de l'entreprise, que ce soit des activités tournées vers l'extérieur (vente, achat, promotion...) ou des activités internes (gestion des ressources humaines, comptabilité...). De plus se connecter à Internet ouvre de vastes horizons, mais expose également l'utilisateur ou l'entreprise à toutes sortes de menaces et désagréments : hackers, virus, spam. Par ailleurs, les obligations légales (loi informatique et libertés) sont fortes dans le domaine de la sécurité informatique. Face à un marché en forte croissance, les responsables ont besoin de réponses managériales et de référentiels communs ainsi que de guides de bonnes pratiques. *Sécurité informatique* propose donc aux directeurs et responsables informatique, directeurs des systèmes d'information et aux responsables de la sécurité des systèmes d'information, les normes et standards français, et internationaux (ISO) les plus récents (notamment la norme ISO/CEI 17799 et ISO/IEC 27001), faisant référence dans le domaine de la sécurité informatique et traitant de l'identification des besoins, du management et de la gestion ainsi que des bonnes pratiques en matière de sécurité informatique.



►► *Technologie de l'information – techniques de sécurité – systèmes de gestion de la sécurité de l'information - exigences*. Genève : ISO, 2005. Norme internationale ISO/CEI 27001

**COTE HEG : REF. 658.478 TEC**

L'ISO/CEI 27001:2005 couvre tous les types d'organismes (par exemple entreprises commerciales, organismes publics, organismes à but non lucratif). L'ISO/CEI 27001:2005 spécifie les exigences relatives à l'établissement, à la mise en œuvre, au fonctionnement, à la surveillance et au réexamen, à la mise à jour et à l'amélioration d'un SMSI documenté dans le contexte des risques globaux liés à l'activité de l'organisme. Le présent document spécifie les exigences relatives à la mise en œuvre des mesures de sécurité adaptées aux besoins de chaque organisme ou à leurs parties constitutives. L'ISO/CEI 27001:2005 est destiné à assurer le choix de mesures de sécurité adéquates et proportionnées qui protègent les actifs et donnent confiance aux parties intéressées.



►► *Technologie de l'information – techniques de sécurité – code de bonne pratique pour la gestion de la sécurité de l'information*. Genève : ISO, 2005. 1<sup>re</sup> éd. 2005-06-15. Norme internationale ISO/CEI 27002

**COTE HEG : REF. 658.478 TECa**

L'ISO/CEI 27002:2005 établit des lignes directrices et des principes généraux pour préparer, mettre en oeuvre, entretenir et améliorer la gestion de la sécurité de l'information au sein d'un organisme. Les objectifs esquissés fournissent une orientation générale sur les buts acceptés communément dans la gestion de la sécurité de l'information. L'ISO/CEI 27002:2005 est un code de bonne pratique pour les objectifs et mesures, dans les catégories suivantes de la gestion de la sécurité de l'information : politique de sécurité, organisation de la sécurité de l'information, gestion des biens, sécurité liée aux ressources humaines, sécurité physique et environnementale, gestion opérationnelle et gestion de la communication, contrôle d'accès, acquisition, développement et maintenance des systèmes d'information, gestion des incidents liés à la sécurité de l'information, gestion de la continuité de l'activité, conformité.



►► *Information technology – security techniques – Information security risk management*. Genève : ISO, 2008. 1<sup>re</sup> éd. 2008-06-15. Norme internationale ISO/CEI 27005

**COTE HEG : REF. 658.478 INFc**

La norme ISO/CEI 27005 étaye les concepts généraux spécifiés dans l'ISO/CEI 27001:2005. La nouvelle norme a pour but d'aider à mettre en oeuvre l'ISO/CEI 27001, la norme relative aux systèmes de management de la sécurité de l'information (SMSI), qui est fondée sur une approche de gestion du risque. Pour comprendre cette norme internationale, il est important de connaître les concepts, modèles, processus et termes exposés dans l'ISO/CEI 27001 et l'ISO/CEI 27002: 2005

**Internet**



►► BLOCH, Laurent. Le management de la sécurité de l'information. In : *Sécurité informatique* [en ligne]. 12.2006, p.4,5  
[http://www.cermav.cnrs.fr/media/secu\\_info\\_58.pdf](http://www.cermav.cnrs.fr/media/secu_info_58.pdf)  
(consulté le 03.11.2008)

Le domaine de la sécurité informatique voit depuis quelques années éclore des normes comme champignons après une pluie d'été : nous nous intéresserons plus particulièrement ici à la norme ISO 27001, consacrée aux systèmes de management de la sécurité de l'information (SMSI).



►► ISO 27000. An Introduction to ISO 27001 (ISO27001). In : *ISO 27000 – ISO 27001 and ISO 27002 Standards* [en ligne]. 2008  
<http://www.27000.org/iso-27001.htm>  
(consulté le 03.11.2008)

La norme ISO 27001 a été publiée en 2005, pour remplacer l'ancienne BS7799-2. Elle est orientée vers les systèmes de gestion de la sécurité informatique.



►► ISO 27000. Introduction to ISO 27002 (ISO27002). In : *ISO 27000 – ISO 27001 and ISO 27002 Standards* [en ligne]. 2008  
<http://www.27000.org/iso-27002.htm>  
 (consulté le 03.11.2008)

La norme ISO 17799, renommée ISO 27002, est un guide de bonnes pratiques pour la sécurité informatique.

## Les risques sont-ils plus élevés pour les organisations et entreprises dotées de logiciels libres ?

### Internet



►► DUPONT ELISE, Christophe. Sécurité : verrouiller sans enfermer. In : *01net* [en ligne]. 21.01.2005  
<http://www.01net.com/article/264279.html>  
 (consulté le 03.11.2008)

Détection d'intrusions, pare-feu, filtrage des mails et PKI : le logiciel libre ne cesse de marquer des points dans l'univers de la sécurité.



►► JACQUES, Arnaud. La sécurité et l'Open Source. In : *Société de sécurité informatique – Audit Firewall Appliance* [en ligne]. 2008  
<http://www.securiteinfo.com/conseils/opensourcesecurity.shtml>  
 (consulté le 03.11.2008)

Depuis Linus Torvalds et son système Linux, l'Open Source s'est considérablement développé. Mais qu'est-ce que l'Open Source ? C'est le fait de rendre public le code source d'un logiciel. Les plus grandes entreprises emboîtent actuellement le pas des développeurs indépendants et proposent à leur tour des logiciels de qualité professionnelle en Open Source. Mais derrière cette effervescence intellectuelle, quelles sont les conséquences, en matière de sécurité, pour les projets Open Source ?



►► RICHARD, Philippe. La menace informatique innove. In : *01net* [en ligne]. 04.06.2007  
<http://www.01net.com/editorial/350273/la-menace-informatique-innove/>  
 (consulté le 03.11.2008)

Applications Web, noyaux Linux, OpenOffice... Durant trois jours en 2007, les meilleurs spécialistes français de la sécurité réunis à Rennes, ont pointé du doigt les nouvelles attaques.

## Maîtriser les risques

### Mise en place d'une politique pragmatique de sécurité



►► BENNASAR, Mathieu, et al. *Manager la sécurité du SI : planifier, déployer, contrôler, améliorer*. Paris : Dunod, 2007. 258 p.

#### COTE HEG : 658.478 MAN

Cet ouvrage s'adresse aux décideurs de l'entreprise qui jouent un rôle décisif dans les problématiques de sécurité ainsi qu'aux risk managers, aux responsables de la sécurité du système d'information (RSSI) et aux directeurs des systèmes d'information (DSI). Ce livre affirme la place stratégique du management de la sécurité dans l'entreprise et aborde les aspects pratiques de la mise en œuvre d'une stratégie de sécurité du SI : les grands principes et quelques conseils (l'exposé des rôles et des responsabilités ainsi que des schémas d'organisation, une présentation de l'environnement juridique, une approche du calcul de retour sur investissement), une méthodologie pour développer le programme de management de la sécurité (les piliers, la stratégie de mise en œuvre, le suivi et le contrôle, l'organisation), ainsi que trois études de cas pour illustrer et mettre en relief les éléments présentés dans les deux premières parties. La diversité des expériences professionnelles des quatre auteurs a permis de condenser une somme d'expériences concrètes, de conseils et de savoir-faire qui vous permettront de vous préparer à l'imprévu.

#### Internet

►► CLUSIF. Menaces informatiques et pratiques de sécurité en France. In : *CLUSIF : bienvenue*. 2008  
<https://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008.pdf>  
(consulté le 03.11.2008)

Le CLUSIF souhaitait, pour l'édition 2008 de cette enquête, interroger exactement le même échantillon d'entreprises interrogé en 2006, afin de pouvoir comparer les progrès ou les éventuelles régressions. Ainsi, la cible est-elle constituée des entreprises de plus de 200 salariés, de différents secteurs d'activité.

►► Comment ça marche. Mise en place d'une politique de sécurité. In : *Comment ça marche – Communauté informatique* [en ligne]. 12.08.2008  
<http://www.commentcamarche.net/secu/secuintro.php3#politique-securite>  
(consulté le 03.11.2008)

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés. Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend.



►► ISIQ. Politique de sécurité. In : *ISIQ : Institut de la sécurité informatique du Québec* [en ligne]. 2008

[https://www.isiq.ca/fr/outils/politique\\_securite/](https://www.isiq.ca/fr/outils/politique_securite/)  
(consulté le 03.11.2008)

Dans cette section, vous trouverez : un modèle (gabarit) de politique de sécurité, un guide de rédaction d'une telle politique, un guide de plan de diffusion (communication) pour la mise en place d'une politique de sécurité et assurer le suivi. Ce modèle de politique de sécurité et le guide de rédaction qui s'y rattache ont été adaptés par l'ISIQ du modèle fourni par le Ministère l'économie du Grand-Duché de Luxembourg dans le cadre d'une entente de collaboration entre les deux organismes.



►► WIKIPEDIA. Politique de sécurité du système d'information. In : *Wikipédia* [en ligne]. 06.04.2008

[http://fr.wikipedia.org/wiki/Politique\\_de\\_s%C3%A9curit%C3%A9\\_du\\_syst%C3%A8me\\_d%27information](http://fr.wikipedia.org/wiki/Politique_de_s%C3%A9curit%C3%A9_du_syst%C3%A8me_d%27information)  
(consulté le 03.11.2008)

La politique de sécurité des systèmes d'information (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration, État, unions d'États...) en matière de sécurité des systèmes d'information (SSI).

### Limites légales de la surveillance et de la protection de la sphère privée



►► CALÉ, Stéphane, TOUITOU, Philippe. *La sécurité informatique : réponses techniques, organisationnelles et juridiques*. Paris : Hermès Science, 2007. 282 p. (Management et informatique)

#### COTE HEG : 005.8 CAL

La sécurité informatique comprend tout à la fois la protection technique et juridique du système, des informations et des œuvres qui y sont stockées, ainsi que celle des individus dont les données personnelles sont traitées. Elle est un droit et une obligation pour l'entreprise qui pourrait voir sa responsabilité recherchée en cas de manquement, en plus des préjudices inhérents à tout sinistre informatique. En assurant la protection du système d'information, les chefs d'entreprises et les membres du service informatique contribuent donc à la sécurité de l'entreprise, mais aussi à la leur, dans la mesure où ils sont susceptibles de répondre de leurs fautes d'imprudence ou de négligence. Trop souvent cantonnée à sa dimension strictement technologique, la sécurité informatique est considérée à tort comme le domaine réservé de quelques initiés. Cette conception réductrice conduit malheureusement les entreprises à construire une ligne Maginot autour de leur système d'information. Cet ouvrage adopte au contraire une approche globale résolument novatrice de la sécurité informatique, proposant des solutions éprouvées prenant en compte aussi bien les technologies les plus récentes (comme la TOIP et le Wi-Fi), que les dernières dispositions légales et jurisprudentielles, ainsi qu'une méthodologie organisationnelle internationalement reconnue (norme ISO 27001).

## Internet



►► Confédération suisse. 235.1 Loi fédérale sur la protection des données (LPD). In : *admin.ch – Page d'accueil* [en ligne]. 01.01.2008  
[http://www.admin.ch/ch/fr/rs/235\\_1/](http://www.admin.ch/ch/fr/rs/235_1/)  
(consulté le 03.11.2008)

La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données.



►► Confédération suisse. *PFPDT – Le préposé fédéral à la protection des données et à la transparence (PFPDT)* [en ligne]. 23.07.2008  
<http://www.edoeb.admin.ch/index.html?lang=fr>  
(consulté le 03.11.2008)

Le préposé fédéral à la protection des données et à la transparence (PFPDT) accomplit notamment les tâches suivantes : surveillance des organes fédéraux, surveillance des personnes privées, conseil aux personnes privées, soutien et conseil aux organes fédéraux et cantonaux, avis sur les projets législatifs de la Confédération, collaboration avec les organes de protection des données nationaux et internationaux, information du public, tenue et publication du registre des fichiers. Pour s'acquitter de ses tâches, le PFPDT établit les faits d'office ou à la demande de tiers. Sur la base de ses constatations, il peut ensuite émettre des recommandations.

## Comment inciter vos collaborateurs à devenir les premiers garants de votre système de sécurité informatique



►► ISIQ. Sécurité de l'information et sensibilisation des utilisateurs. In : *Bulletins ISIQ* [en ligne]. No 8, 07-08.2006  
[https://www.isiq.ca/fr/bulletin/2006/bulletinISIQ\\_07-0806.htm](https://www.isiq.ca/fr/bulletin/2006/bulletinISIQ_07-0806.htm)  
(consulté le 03.11.2008)

Le comportement des utilisateurs est la clé de la sécurité dans un monde en réseau. Dans son nouvel ouvrage sur la sécurité informatique, Bruce Schneier souligne que le maillon faible face aux nouveaux types d'attaques qui combinent la technologie et la naïveté humaine, ce sont les utilisateurs. Les attaques provenant de l'intérieur des organisations sont passées de 60 % à 80 % en moins de deux ans et 75 % des attaques provenant de l'extérieur résultent de renseignements divulgués de l'intérieur.



►► GUILLEMIN, Christophe. Sécurité des systèmes d'information: les employés montrés du doigt. In : *Business et technologies – ZDNet.fr* [en ligne]. 22.12.2004  
<http://www.zdnet.fr/actualites/informatique/0,39040745,39194612,00.htm>  
(consulté le 03.11.2008)

Les responsables de la sécurité informatique des entreprises françaises se plaignent de ne pouvoir faire respecter leur politique en la matière. En cause, la faible prise de conscience des utilisateurs due à leur manque de formation.

## A qui confier la responsabilité de la sécurité des systèmes d'information



►► BOULET, Patrick. *Management de la sécurité du SI*. Paris : Hermès Science, 2007. 246 p. (Collection management et informatique)

**COTE HEG : 658.478 BOU**

Afin de résoudre les problèmes de sécurité informatique toujours croissants, cet ouvrage démontre la nécessité de redéfinir la politique de sécurité des entreprises et de donner au RSSI (responsable de la sécurité du système d'information) un plus grand pouvoir sur l'ensemble du système informatique. Après une analyse des différentes menaces pesant sur le SI et de leurs conséquences sur l'entreprise, *Management de la sécurité du SI* détaille les contraintes réglementaires à prendre en compte et présente les normes de sécurité et les méthodes d'analyse des risques à la disposition du RSSI. Cet ouvrage expose ensuite les moyens et outils indispensables ou envisageables à la sécurisation des différentes briques du SI (infrastructures, données, applications, accès, échanges). Les actions courantes et quotidiennes du RSSI sont également traitées ainsi que la mise en oeuvre du plan de secours auquel il doit être associé.



►► FORAY, Bernard. *La fonction RSSI : Guide des pratiques et retours d'expérience*. Paris : Dunod, 2006. 268 p. (InfoPro)

**COTE HEG : 658.403 801 1 FOR**

Cet ouvrage s'adresse aux responsables de la sécurité des systèmes d'information, qu'ils aient le titre de RSSI ou qu'ils soient chargés de cette fonction au sein d'une entreprise. Il intéressera également tous ceux qui dans leur métier ont la responsabilité de veiller à la sécurisation des applications et des données de l'entreprise. L'un des objectifs premiers de cet ouvrage est de changer l'image de la sécurité pour qu'elle ne soit plus vue comme une contrainte mais comme un service. Si tout le monde dans l'entreprise est convaincu que l'application de petits gestes quotidiens peut éviter de grands problèmes, alors le RSSI a accompli une partie de sa mission. Cet ouvrage est construit en quatre parties : la préparation qui définit le rôle du RSSI et ses moyens d'action (processus de sécurité, roadmap sécurité, externalisation...), les principes de base (qui présentent la définition du périmètre, la défense en profondeur des systèmes et des applications, les audits, les plans de corrections des vulnérabilités du SI), les expériences opérationnelles (qui expliquent comment faire face à quatre situations réelles auxquelles sont confrontés les RSSI : l'authentification forte, la mobilité, le Wi-Fi et enfin le spam) et les moyens de contrôle (tests intrusifs, tableaux de bord...) qui permettent de s'assurer de la robustesse des protections.

### Internet



►► BISEUL, Xavier. « En 2012, le DSI sera un DSI heureux ! ». In : *01net* [en ligne]. 29.07.2008  
<http://www.01net.com/editorial/387531/-en-2012-le-dsi-sera-un-dsi-heureux-.-/>  
(consulté le 03.11.2008)

Quelle sera la vie du DSI en 2012 ? Louis Naugès s'est prêté au jeu de la prospective. Cloud computing, Saas, Paas et web 2.0... Pour le président du cabinet de conseil Revevol, un nouveau cycle de changements technologiques et organisationnels attend les DSI. Le premier chantier porte sur les infrastructures.



►► BOUCQ, Isabelle. Profession DSI. In : *01net* [en ligne]. 02.03.2005  
<http://www.01net.com/article/268094.html>

La mission du directeur des systèmes d'information : trouver des solutions informatiques aux besoins stratégiques de l'entreprise. Qualité d'écoute et compétences techniques exigées.

---

## Gérer la sécurité

---

### Choisir un audit informatique éthique et non intrusif

#### Internet



►► Association française de l'audit et du conseil informatiques. *AFAI – Accueil* [en ligne]. 2008  
<http://www.afai.fr/>  
(consulté le 03.11.2008)

Créée en 1982, l'AFAI a pour but de développer l'emploi des techniques et des méthodes visant la maîtrise des systèmes d'information. L'AFAI regroupe plus de 600 membres et organise des manifestations, des formations, anime des groupes de recherche et publie des résultats d'enquêtes et d'études, des ouvrages ainsi qu'une revue.



►► COHEN, Didier. Les outils de l'audit informatique : la nouvelle donne. In : *La Revue* [en ligne]. 05.2007, p. 23-25  
<http://www.afai.asso.fr/public/doc/371.pdf>  
(consulté le 03.11.2008)

Le 9 novembre 2006 a eu lieu la journée ACTI qui faisait office, pour l'AFAI, de séminaire de lancement du projet d'observatoire à lancer sur les outils d'audit informatique. Quelques constats ont permis de faire émerger ce projet : il n'existe pas à ce jour une base centralisée des outils d'audit existants sur le marché. Les besoins d'innovation autour de ces outils ne sont pas systématiquement formulés.



►► IFACI. Code de déontologie. In : *IFACI – Institut de l'audit interne* [en ligne]. [2000]  
<http://www.ifaci.com/fo/page.asp?id=94>  
(consulté le 03.11.2008)

Compte tenu de la confiance placée en l'audit interne pour donner une assurance objective sur les processus de management des risques, de contrôle et de gouvernement d'entreprise, il était nécessaire que la profession se dote d'un tel code. Le code de déontologie va au-delà de la définition de l'audit interne. Ce texte est une traduction du Code of Ethics adapté par le Conseil d'administration de l'IIA, le 17 juin 2000.



►► ISACA. *Willcomen bei ISACA Switzerland chapter* [en ligne].  
<http://www.isaca.ch/>  
(consulté le 03.11.2008)

ISACA Suisse est le chapitre suisse d'un organisme international regroupant plus de 60'000 membres dans plus de 140 pays. Depuis sa fondation en 1969, ISACA supporte le développement de la technologie de l'information (IT) en considérant, en particulier, les aspects liés à la sécurité et aux contrôles et offre l'accès à des connaissances et des formations dans le monde entier.

## Modélisation du système de gestion de la sécurité de l'information

### Livre



►►SCHUMACHER, Markus [et al.] *Security patterns: integrating security and systems engineering*. Chichester : John Wiley, 2006. 565 p.

Most security books are targeted at security engineers and specialists. Few show how build security into software. None breakdown the different concerns facing security at different levels of the system: the enterprise, architectural and operational layers. Security Patterns addresses the full spectrum of security in systems design, using best practice solutions to show how to integrate security in the broader engineering process.

- Essential for designers building large-scale systems who want best practice solutions to typical security problems
- Real world case studies illustrate how to use the patterns in specific domains

## Outils de gestion de la sécurité des Systèmes d'Information : les tableaux de bord



►►LLORENS Cédric. LEVIER Laurent, VALOIS Denis. *Tableaux de bord de la sécurité réseau*. Paris : Eyrolles, 2006. 559 p.

### COTE HEG : 005.8 LLO 2006

Destiné aux directeurs informatique, aux administrateurs réseau et aux responsables sécurité, cet ouvrage montre comment élaborer une véritable stratégie de sécurité réseau à l'échelle d'une entreprise. Après avoir répertorié les attaques auxquelles peut être confronté un réseau d'entreprise, il décrit les différentes étapes de la mise en place d'une politiques de sécurité : analyse des risques (description des méthodes) et expressions des besoins, définition de la politiques de sécurité réseau (recueil de règles), choix et déploiement des solutions techniques (accès réseau, gestion réseau, etc.), mise en place de procédures et d'outils de contrôle. L'ouvrage montre enfin comment élaborer des tableaux de bord synthétisant les événements réseau, les analyses des configurations réseau, etc.

### Internet



►►DCSSI. Élaboration de tableaux de bord SSI. In : *Portail officiel de la sécurité informatique – DCSSI – République française* [en ligne]. 23.03.2007  
[http://www.securite-informatique.gouv.fr/gp\\_rubrique16.html](http://www.securite-informatique.gouv.fr/gp_rubrique16.html)  
(consulté le 03.11.2008)

Un tableau de bord parfaitement adapté à chaque type de fonction de la "voie fonctionnelle SSI" est un atout pour améliorer la qualité des services de sécurité et maîtriser le niveau de sécurité global de sécurité des systèmes d'information. Il constitue en effet un outil de synthèse et de visualisation indispensable pour suivre toutes les actions liées à la SSI.



►► SSI Conseil. Tableau de bord SSI. In : *SSI-Conseil sécurité des systèmes d'information – Accueil SSI-Conseil* [en ligne].  
<http://www.ssi-conseil.com/content/view/96/122/>  
 (consulté le 03.11.2008)

Outil indispensable de pilotage de la sécurité, le tableau de bord SSI doit être assez synthétique. Il résulte du choix d'indicateurs pertinents, met en œuvre des processus automatiques ou manuels de collecte.

## Comment reprendre les activités après une catastrophe

### Internet



►► ISIQ. Gérer les incidents de sécurité. In : *ISIQ : Institut de la sécurité informatique du Québec* [en ligne]. 13.02.2007  
[https://www.isiq.ca/fr/Guides/PME/1211\\_incidents.html](https://www.isiq.ca/fr/Guides/PME/1211_incidents.html)  
 (consulté le 03.11.2008)

Un incident de sécurité est la concrétisation d'un risque qui menace la confidentialité, l'intégrité ou la disponibilité d'une ressource informationnelle et qui met en péril, selon sa sévérité, le déroulement des activités de votre organisation. Le processus de gestion des incidents est constitué de cinq activités : la prévention des incidents, la détection, la réaction aux incidents, l'activation de mesures de rétablissement, la rétroaction.



►► ISIQ. Prévoir la continuité des activités. In : *ISIQ : Institut de la sécurité informatique du Québec* [en ligne]. 13.02.2007  
[https://www.isiq.ca/fr/Guides/PME/1212\\_continuite.html](https://www.isiq.ca/fr/Guides/PME/1212_continuite.html)  
 (consulté le 03.11.2008)

Le plan de continuité des activités vise à réduire en cas d'incendie, d'inondation, d'accidents, de pannes de matériel ou d'actes délibérés l'impact sur votre organisation et à récupérer dans des délais raisonnables les ressources informationnelles endommagées ou détruites.



►► JACQUES, Arnaud. Que faire si vous êtes attaqué ?. In : *Société de sécurité informatique – Audit Firewall Appliance* [en ligne]. 2008  
<http://www.securiteinfo.com/conseils/quefaire.shtml>  
 (consulté le 03.11.2008)

Vous détectez une activité anormale, une déconnexion, un ralentissement système... Après vérification, vous en êtes sûr, vous êtes attaqué. Voici quelques règles qu'il faut appliquer rapidement. Ces règles dépendent de vous : vous ne réagirez pas de la même façon si vous êtes un particulier qui surfe sur le web, ou un administrateur réseau en entreprise.



►► WIKIPEDIA. Plan de continuité d'activité (informatique). In : *Wikipédia* [en ligne]. 01.08.2008  
[http://fr.wikipedia.org/wiki/Plan\\_de\\_continuit%C3%A9\\_d'activit%C3%A9\\_\(informatique\)](http://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9_d'activit%C3%A9_(informatique))  
 (consulté le 03.11.2008)

En informatique, un plan de continuité d'activité, parfois aussi appelé "plan de reprise d'activité", a pour but la reprise des activités après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise.

Crédits :

*Images et résumés : Amazon.com, Inc. ; ISO.com. Tous droits réservés*

*Résumés : infothèque HEG*