

VOLET N°3

Copyright PRONETIS

1

Copyright Société PRONETIS - 2011 - Droits d'utilisation ou de reproduction réservés.

Politiques de sécurité et normes

Définition d'une politique cadre et des politiques ciblées de sécurité

Exemples de politiques de sécurité

Mise en œuvre des politiques de sécurité au sein de l'entreprise

Normes et certifications de sécurité

Aspects réglementaires et légaux

Copyright PRONETIS

2

Copyright Société PRONETIS - 2011 - Droits d'utilisation ou de reproduction réservés.

Politique de sécurité

Politique de sécurité

- Définition formelle de la position d'une entreprise en matière de sécurité.

« Ensemble des règles formelles auxquelles doivent se conformer les personnes autorisées à accéder à l'information et aux ressources d'une organisation »
(RFC 2196)

Finalité d'une politique de sécurité ?

- « Réduire les risques »
- « Qu'est-ce qui est autorisé ? Qu'est-ce qui ne l'est pas ? »
- « Définir les règles du jeu »
- « Communiquer , faire accepter et faire respecter les règles du jeu »

3

Copyright Société PRONETIS - 2011 - Droits d'utilisation ou de reproduction réservés.

Politique de sécurité

Composantes d'une politique de sécurité

- Ensemble des principes juridiques, humains, organisationnels et techniques qu'il est recommandé de mettre en œuvre pour créer, gérer, protéger le système d'information

Réussite de mise en œuvre d'une politique de sécurité

- Implication forte de la direction
- En accord avec les directions fonctionnelles et les équipes techniques
- Analyse des risques pleinement étudiée

4

Copyright Société PRONETIS - 2011 - Droits d'utilisation ou de reproduction réservés.

Politique de sécurité

Les politiques de sécurité sont de trois types :

- Communication
- Informatique
- Organisation

5

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Politique de sécurité

Les politiques de communication prennent les formes suivantes :

- Sensibilisation (ex : guide de l'utilisateur, Page Intranet)
- Responsabilisation (ex : élaboration de charte de sécurité)
- Formations ciblées par métier

6

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Politique de sécurité

Les politiques touchant aux infrastructures informatiques s'articulent autour des thèmes suivants :

- Systèmes et réseaux sécurisés : organisation de la sécurité opérationnelle, architectures de sécurité, études de solutions techniques, mise en œuvre (intégration, administration, exploitation, supervision)
- Intégration de la sécurité dans la conduite de projets : définition méthode, actions menées sur tout le cycle conception – développement - intégration, clauses contractuelles avec les fournisseurs

Politique de sécurité

Les politiques touchant à l'organisation de la sécurité portent sur les aspects suivants :

- Structures, organigramme, comités
- Responsabilités, fonctions, fiches de mission
- Fonctionnement, référentiels, règles
- Management du changement
- Plan de continuité d'activités, Plan de secours, Gestion de crise
- PKI : Infrastructure à clé publique.

Exemples de politiques de sécurité ciblées

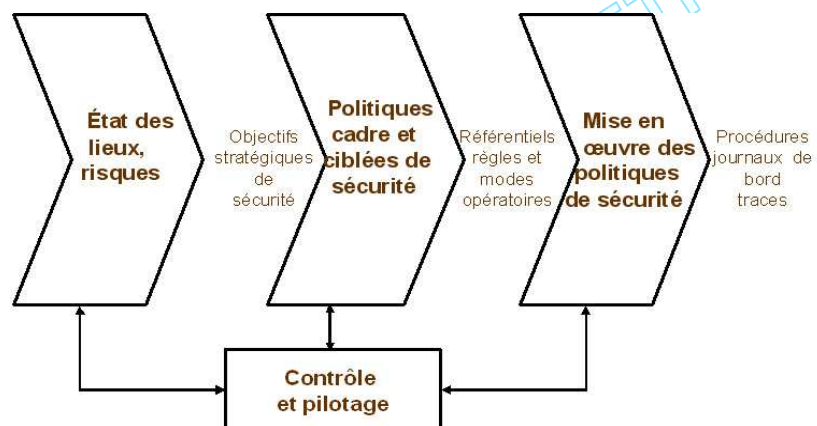
Politique d'authentification (gestion des comptes)
Politique d'autorisation (gestion des habilitations)
Politique de gestion de la continuité des services informatique
Politique d'exploitation des applications et de gestion du réseau
Politique d'acquisition, développement et maintenance des applications
Politique d'intervention par des tiers externes pour le personnel informatique
Politique de sécurité des ressources humaines
Politique de respect de la réglementation interne et externe

9

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Pilotage et mise en œuvre des politiques de sécurité

Démarche sécurité – PDCA – SMSI – ISO 27001



10

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Pilotage et mise en œuvre des politiques de sécurité

La mise en œuvre a pour but :

- la mise en œuvre des plans d'action sécurité
- L'implémentation des solutions
- la rédaction de documents opérationnels permettant la mise en œuvre des différentes politiques techniques définies au niveau informatique. Il s'agit principalement de :
 - Procédures
 - Journaux de bord
 - Traces

11

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Pilotage et mise en œuvre des politiques de sécurité

Le contrôle et le pilotage ont pour but de contrôler la conformité du dispositif de sécurité par rapport aux objectifs généraux de sécurité ainsi que son efficacité en regard de l'évolution des architectures techniques et des menaces.

Les principales actions relevant de cette étape sont les suivantes :

- Mission d'audit
- Tests intrusifs
- Définition du dispositif de contrôle de la sécurité
- Mise en place de référentiels et de procédures
- Elaboration et mise en place de tableaux de bord

12

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Mesures de sécurité

« Le cercle de la sécurité » du système d'information est construit autour de quatre phases :

- **La prévention** : l'ensemble des mesures à mettre en place par l'entreprise pour limiter la probabilité qu'un incident de sécurité se produise
- **La détection** : l'ensemble des mesures à mettre en place pour détecter un incident
- **La réaction** : l'ensemble des mesures à suivre lorsqu'un incident est survenu visant à minimiser son impact
- **La reprise** : l'ensemble des mesures à prendre pour remettre le SI dans l'état normal de fonctionnement avant que l'incident ne se produise.

Exemples de mesures de sécurité

- Prévention
 - Analyse de risques
 - Classifier les données
 - Formaliser des politiques de sécurité
 - Etablir un schéma directeur de sécurité
 - Dissuader les éventuelles tentatives
 - Sensibiliser le personnel
 - Définir des règles, normes et standards techniques à respecter
 - Sécuriser les architectures réseaux

Exemples de mesures de sécurité

- **Prévention**
 - Faire réaliser des audits techniques et organisationnels
 - Exécuter des tests de vulnérabilités et d'intrusion
 - Réaliser une veille en sécurité
 - Sécuriser le développement des applications
 - Définir une politique de maintenance de la sécurité
 - Sécuriser les processus métiers
 - Former les administrateurs systèmes aux techniques de sécurisation
 - Définir des indicateurs de sécurité
 - Définir et tester une stratégie de continuité d'activité

15

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Exemples de mesures de sécurité

- **Détection**
 - Corréler les enregistrements
 - Mettre en place des systèmes de détection d'intrusion
 - Surveiller ou télé-administrer 24/7
 - Installer des outils de traçage
 - Externaliser des services de sécurité
 - Mettre en place des systèmes de contrôle d'intégrité

16

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Exemples de mesures de sécurité

- Réaction
 - Filtrer les communications suspectes
 - Analyser les alertes
 - Analyser les incidents
 - Analyser les fichiers des enregistrements des accès
 - Réunir une cellule de crise

17

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Exemples de mesures de sécurité

- Reprise
 - Revoir les mesures de sécurité
 - Exécuter le plan de secours
 - Utiliser des moyens de restauration des données

18

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Normes et certifications de sécurité

Pourquoi s'inspirer des normes ou des recueils de meilleures pratiques en matière de sécurité ?

- Avoir une approche structurée face à la complexité de la tâche
 - s'assurer d'une certaine exhaustivité, cohérence et homogénéité dans sa démarche,
 - Avoir des éléments communs (vocabulaire, concepts, ...) avec tous les intervenants dans le projet : décideurs, utilisateurs, personnels de l'informatique, sous-traitants, fournisseurs, partenaires, etc.
- Bénéficier de l'expérience des meilleures pratiques (succès et erreurs du passé)
- Se comparer aux meilleures pratiques du moment
 - Référentiel de comparaison par rapport aux autres entreprises

Normes et certifications de sécurité

La famille des normes ISO 27000 :

- Norme ISO-27000 : Vocabulaire
- Norme ISO-27001 : Système de management de la sécurité de l'information (SMSI)
- Norme ISO-27002 : (ex. ISO-17799) Cadre général de bonnes pratiques et d'audit
- Norme ISO 27003 : Guide d'implémentation
- Norme ISO 27004 : Standard de métriques et de mesures d'un SMSI
- Norme ISO 27005 : Analyse de risques - en cours de rédaction
- Norme ISO 27006 : Audit du SMSI
- Norme ISO 27007 : Mesures PCA
- Norme ISO 27799 : équivalent 27002 pour le secteur de la santé (Etat Draft)

Autres normes ISO :

- Norme ISO-19011 : Guide pour mener un audit interne
- Norme ISO-13335 : Management de la sécurité des technologies de l'information et de la communication

Normes ISO 27001 et ISO 27002

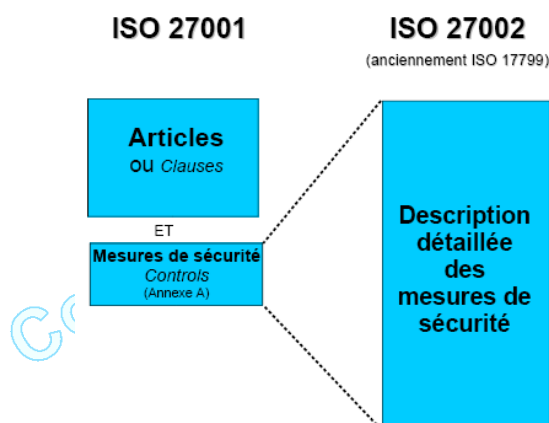
- ISO-27001 : SMSI
 - Cycle de gestion de la SI dit « PDCA » PLAN-DO,CHECK-ACT de la roue de Deming
 - Référentiel pouvant être utilisé pour auditer et certifier le système de management de la sécurité
- ISO-27002 (ex: ISO-17799) : « Code de pratiques pour la gestion de la sécurité de l'information »
 - propose des recommandations pour assurer la sécurité de l'information, sous la forme d'objectifs de contrôles ou de mesures de sécurité
 - 11 chapitres 133 mesures exhaustives basées sur les meilleures pratiques en sécurité de l'information.

21

Copyright Société PRONETIS 2011 – Droits d'utilisation ou de reproduction réservés.

Normes ISO 27001 et ISO 27002

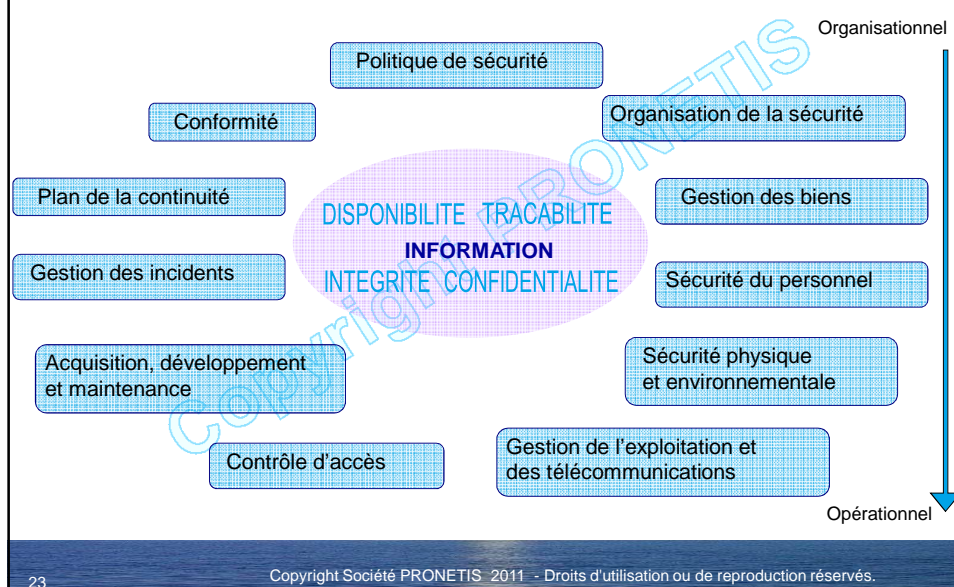
- « ISO-27001 explique comment appliquer ISO-27002 »



22

Copyright Société PRONETIS 2011 – Droits d'utilisation ou de reproduction réservés.

Norme ISO 27002



Norme ISO 27002

- Chapitre N°1 : Politique de sécurité
 - Exprimer formellement la stratégie de sécurité de l'organisation
 - Communiquer clairement son appui à l'implémentation.
- Chapitre N°2 : Organisation de la sécurité
 - Gérer efficacement la sécurité de l'information dans l'organisation
 - Maintenir la sécurité des moyens de traitement et des actifs accédés par des tiers ou des sous-traitants
 - Maintenir la sécurité des informations lorsque la responsabilité du traitement des informations est externalisée ou sous-traitée à une autre organisation

Norme ISO 27002

- Chapitre N°3 : Classification et contrôle des actifs
 - Maintenir le niveau de protection adapté à chaque actif d'information en accord avec la politique de sécurité.
 - Tout élément d'actif important doit être répertorié et alloué à un responsable nominatif.

- Chapitre N°4 : Sécurité liée aux ressources humaines
 - Réduire le risque d'erreur, de vol, de fraude ou de mauvais usage des moyens de traitement
 - S'assurer que les utilisateurs soient informés des risques et menaces concernant les informations.
 - S'assurer que les utilisateurs soient formés et équipés pour appliquer la politique de sécurité lors de leurs activités normales.
 - Minimiser les dommages en cas d'incident ou de mal-fonction
 - Apprendre de ces incidents

25

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Norme ISO 27002

- Chapitre N°5 : Sécurité physique et environnementale
 - Prévenir les accès physiques non autorisés, les dommages et les interférences sur les informations, les activités et les locaux de l'organisation.
 - Prévenir la compromission ou le vol d'information ou de moyens de traitement.

- Chapitre N°6 : Exploitation et réseaux
 - Assurer une exploitation correcte et sûre des moyens de traitement
 - Minimiser les risques de pannes et leur impact
 - Assurer l'intégrité et la disponibilité des informations, des traitements et des communications
 - Prévenir les dommages aux actifs et les interruptions de service
 - Prévenir les pertes, les modifications et les mauvaises utilisations d'informations échangées entre organisations.

26

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Norme ISO 27002

- Chapitre N°7 : Contrôle d'accès
 - Gérer et contrôler l'accès aux informations
 - Prévenir les accès non autorisés
 - Assurer la protection des systèmes en réseau
 - Détecter les activités non autorisées
 - Assurer la sécurité des informations lors des accès mobiles ou distants.

- La politique de contrôle d'accès comprend notamment:
 - L'enregistrement unique de chaque utilisateur,
 - Une procédure écrite de délivrance d'un processus d'authentification signée du responsable hiérarchique,
 - Des services de déconnexion automatique en cas d'inactivité,
 - Une politique de révision des mots de passe,
 - Une hiérarchisation du niveau d'accès en fonction du degré de confidentialité des données,...

27

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Norme ISO 27002

- Chapitre N°8 : Acquisition, Développement et maintenance des systèmes
 - Assurer que la sécurité est incluse dès la phase de design
 - Prévenir la perte, modification, mauvaise utilisation des informations dans le SI
 - Protéger la confidentialité, l'intégrité et la disponibilité des informations
 - Assurer que les projets et la maintenance sont conduits de manière sûre
 - Maintenir la sécurité des applications tant pour le logiciel que pour les données

- Chapitre N°9 : Gestion des incidents
 - Mettre en place un système permettant d'alerter, de tracer les incidents de sécurité
 - Surveiller les outils de traçage en place
 - Gérer l'amélioration continue des dispositifs de sécurité par l'exploitation régulière des journaux des incidents détectés.
 - Collecter les preuves de malveillance si nécessaire

28

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Norme ISO 27002

- Chapitre N°10 : Continuité de service
 - Développer la capacité à répondre rapidement aux interruptions des activités critiques de l'organisation, résultant de pannes, d'incident, de sinistre ou de catastrophe.
- Chapitre N°11 : Conformité
 - Respect des lois et réglementations: licences logiciels, propriété intellectuelle, règles de stockage des fichiers et l contenant des informations touchant la confidentialité des personnes,
 - Conformité avec les procédures et règles de la politique de sécurité,
 - Efficacité des dispositifs de traçabilité (logs, enregistrements de transaction....)

Certifications de sécurité pour un organisme – ISO 27001

- Intérêts de la certification
 - Sécurité – PDCA – maîtrise des risques
 - Communication aux parties prenantes - Savoir-faire de la profession, pratiques éprouvées - Référentiel qui améliore la confiance = business
 - Mutualisation des audits
 - Communication aux auditeurs hors SSI
 - Homogénéisation
 - Référentiel universel, international
 - Facilitation de la communication interne, des échanges d'expérience
 - Simplicité
 - Réduction des coûts (mutualisation audit, élimination des mesures inutiles)
 -

Certifications de sécurité pour un organisme – ISO 27001

- Rappels :
 - Certification d'un processus, pas d'un état ou d'un résultat
 - Certification du fait que le système de management fonctionne, pas du niveau de sécurité
 - Et auditeur de certification ne doit pas apporter de conseil

- Procédure de certification
 - Demande à un organisme certificateur
 - Audit de conformité
 - Décision d'attribution
 - Surveillance tous les 12 mois – Renouvellement tous les 3 ans
 - Coût dépendant de l'ampleur du site(s)

31

Copyright Société PRONETIS 2011 – Droits d'utilisation ou de reproduction réservés.

Certifications de sécurité – Certification ISO 27001

Japan	2999*	France	12	Oman	3
India	441	Iceland	12	Peru	3
UK	395	Pakistan	12	Portugal	3
Taiwan	248	Philippines	11	Vietnam	3
China	191	Singapore	11	Bangladesh	2
Germany	124	Russian Federation	10	Canada	2
Korea	89	Saudi Arabia	10	Isle of Man	2
USA	86	Slovenia	9	Kazakhstan	2
Czech Republic	71	Sweden	9	Morocco	2
Hungary	64	Slovakia	6	Ukraine	2
Italy	59	South Africa	6	Argentina	1
Poland	39	Switzerland	6	Armenia	1
Spain	35	Bahrain	5	Belgium	1
Hong Kong	31	Colombia	5	Kyrgyzstan	1
Austria	30	Croatia	5	Lebanon	1
Australia	29	Indonesia	5	Lithuania	1
Ireland	29	Kuwait	5	Luxembourg	1
Malaysia	26	Bulgaria	4	Macedonia	1
Brazil	21	Gibraltar	4	Belarus	1
Thailand	21	Norway	4	Mauritius	1
Mexico	20	Qatar	4	Moldova	1
UAE	18	Sri Lanka	4	New Zealand	1
Turkey	18	Chile	3	Uruguay	1
Greece	15	Egypt	3	Yemen	1
Romania	15	Iran	3	Relative Total	5333
Netherlands	13	Macau	3	Absolute Total	5314

32

Copyright Société PRONETIS 2011 – Droits d'utilisation ou de reproduction réservés.

Certifications de sécurité

Quelques certifications individuelles

- ISO27001 Lead Auditor (ISMS Lead Auditor)
 - destinée aux professionnels de l'informatique et amenés à conduire des audits dans le domaine de la gestion de services informatiques.
- ISO27001 Lead Implementer (ISMS Lead Implementer)
 - Elle est destinée aux professionnels de l'informatique ayant une connaissance de base dans la sécurité des systèmes d'information et désirant implémenter un SMSI.
- ISO 27005 Risk Manager (Information Security Risk Manager)
 - Destinée aux gestionnaires de risques en sécurité de l'information, donc à toute personne devant réaliser une appréciation des risques.
- CISSP (International Information Systems Security Certification Consortium)
 - Destinée aux responsables de la sécurité opérationnelle en interne
- Et les Certifications à profils techniques :
 - CEH (Certified Ethical Hacker), CHFI (Computer Hacking Forensics Investigator),

33

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Certifications de sécurité

Certification individuelle du responsable Sécurité : RSSI

- Certification CISSP
 - Certification de compétences de haut niveau dans le domaine SSI
 - Développé par L'(ISC)2
 - Certification internationale reconnue par les experts sécurité
- Objectif de la certification CISSP
 - Valider les connaissances des experts et d'assurer que les experts continuent leur formation en permanence.
 - Permet d'étalonner son niveau de compétence tant au niveau des connaissances techniques qu'au niveau analyse des risques et audit des systèmes dans une optique gouvernance des systèmes d'informations.

(ISC)2 - *International Information Systems Security Certification Consortium*
<http://www.isc2.org>

34

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Certifications de sécurité

Certification individuelle du RSSI

- Bénéfices à promouvoir pour cette certification
 - Établir la preuve du niveau de compétence atteint en sécurité du SI par un organisme tiers indépendant reconnu au niveau international.
 - Asseoir une crédibilité certaine vis à vis des fournisseurs, des différents partenaires et des clients
 - Renforce la crédibilité en interne en prouvant que le domaine de la sécurité du SI est couvert par un Responsable Sécurité compétent.

- Nb CISSP Monde = +65.000 -- Nb CISSP France > 650

35

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Certifications de sécurité

Les acteurs de la certification

- L'ISO (International Organization for Standardization)
 - Organisation internationale non gouvernementale - 157 pays.
 - Parmi les normes les plus connues, on peut citer l'ISO 9000 sur la qualité et l'ISO 14000 sur la protection de l'environnement. L'ISO 27000 est la famille de normes sur la gestion de la sécurité de l'information.

- Le COFRAC (association française)
 - Chargée de donner l'accréditation aux organismes certificateurs en France. Il garanti que ceux-ci sont compétents et impartiaux et que leurs prestations peuvent être reconnues internationalement. Le Cofrac s'appuie sur les normes européennes et internationales, notamment celles de l'ISO.

36

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

Certifications de sécurité

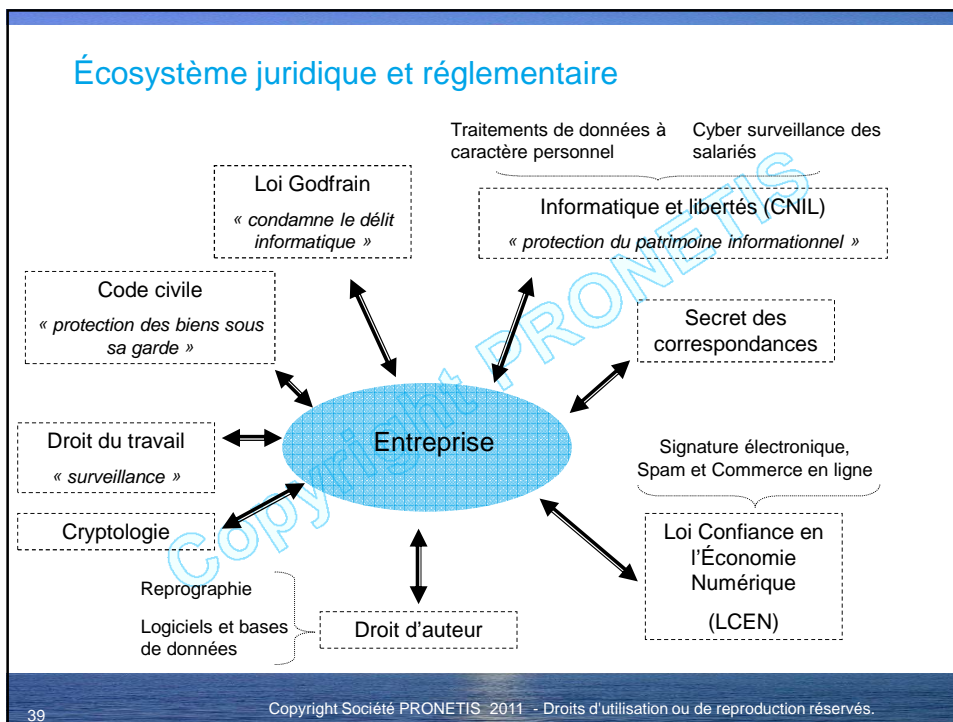
Les acteurs de la certification

- Le certificateur
 - Le certificateur est une entité accréditée en France par le Cofrac. Il est chargé des audits de certification et de la remise des certificats. Actuellement, l'unique certificateur accrédité par le Cofrac pour la norme ISO 27001 est la société LSTI.
- L'auditeur
 - Personnes physiques certifiés à titre individuel (lead auditor ISO 27001) qui peuvent intervenir au cours de l'audit de certification pour le compte du certificateur, ou qui peuvent intervenir en tant que conseil pour aider une entreprise ou un organisme à préparer la certification.

Aspects légaux et réglementaires

- Obligations de sécurité des données
- Protection des personnes
- Protection des biens immatériels
- Protection des données et des systèmes
- Droit des salariés et la cyber surveillance

Écosystème juridique et réglementaire



LA PROTECTION DES PERSONNES



■ Les contraintes légales – Nouvelle Loi Informatique et Libertés CNIL

- La loi du 6 août 2004 (modifie la loi du 6 janvier 1978) prend en compte les risques liés à l'utilisation des nouvelles technologies dans le cadre du traitement, de l'échange et de la circulation des données.
- La loi s'applique à l'ensemble des traitements de données à caractère personnel, c'est-à-dire à toute opération, quel que soit le procédé utilisé (la collecte, l'enregistrement, l'organisation, la conservation, l'utilisation, etc.) portant sur toute information relative à une personne physique identifiée ou pouvant être identifiée par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
- Trois points majeurs se dégagent de la loi du 6 août 2004 : la modification du régime de déclaration, la création d'un correspondant à la protection des données, les nouveaux pouvoirs attribués à la CNIL.
 - Les nouveaux pouvoirs de la CNIL
 - Pouvoir de sanctionner pécuniairement le responsable du traitement litigieux
 - Jusqu'à 150 000 euros pour le premier manquement, 300 000 euros en cas de récidive dans les 5 ans
 - Ce pouvoir de sanction ne s'étend pas aux traitements mis en œuvre par l'État.

LA PROTECTION DES PERSONNES



- Les contraintes légales – Protection des personnes dont les données sont conservées
 - Aider les responsables du traitement informatique à s'assurer que la collecte des informations n'est ni frauduleuse, ni déloyale, ni illicite et qu'elle s'accompagne d'une bonne information des personnes ;
 - Identité du responsable, finalité du traitement, modalités des droits d'accès, de rectification ou d'opposition, l'éventualité de transfert des données à des tiers,...
 - Les informations ne sont pas conservées au-delà de la durée prévue ;
 - Les informations ne sont pas communiquées à des personnes non autorisées ;
 - Le traitement ne fait pas l'objet d'un détournement de finalité ;
 - L'accès aux résultats des traitements et aux données collectées fait l'objet d'une sécurité optimale, afin qu'aucun détournement de la finalité ne puisse avoir lieu.

41

Copyright Société PRONETIS - 2011 - Droits d'utilisation ou de reproduction réservés.

Rapport d'activité 2008 de la CNIL

- Les temps forts : EDVIGE & HADOPI
 - **SUPPRESSION DU FICHIER EDVIGE** (Exploitation documentaire et valorisation de l'information générale) au **profit d'un nouveau fichier EDVIRSP** (Exploitation documentaire et valorisation de l'information relative à la sécurité publique) **avec des conditions de traitement largement révisées et plus strictement encadrées par rapport au fichier «EDVIGE»**.
 - **La suite, avant le 28/10/09** : Réponse du Conseil constitutionnel
 - <http://www.laquadrature.net/fr/HADOPI>

TÉLÉCHARGEMENT ET DROITS D'AUTEUR



42

Copyright Société PRONETIS - 2011 - Droits d'utilisation o

Rapport d'activité 2008 de la CNIL

- Les temps forts : EDVIGE & HADOPI
 - **HADOPI: décision historique du 10 juin 2009, le Conseil constitutionnel retire tout pouvoir de sanction à l'HADOPI.** Notant que le libre accès à Internet est devenu une **composante essentielle de la liberté d'expression et de communication** garantie par l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen, le Conseil estime que **seule l'autorité judiciaire, garante des libertés, peut prononcer des mesures y faisant obstacle.** Le projet de loi **HADOPI 2**, examiné au cours de l'été 2009, cherche à **contourner la censure du Conseil constitutionnel** en confiant ce pouvoir de sanction à un **juge unique**, généralisant au passage une **procédure judiciaire expéditive et irrespectueuse des droits fondamentaux.**

43

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

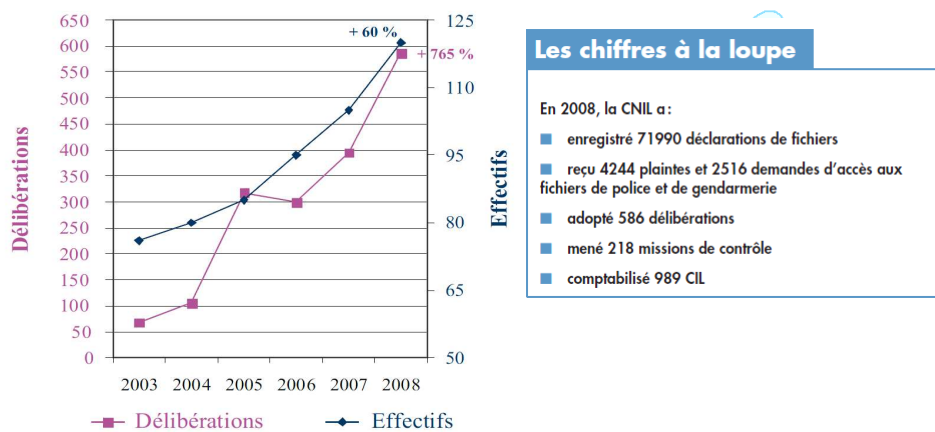
Rapport d'activité 2008 de la CNIL

- CNIL a reçu **4.244 plaintes pour non-respect** de la loi « informatique et libertés ».
 - **Commerce (25%), notamment pour demander la radiation de leurs coordonnées d'un fichier utilisé pour l'envoi de publicités (15 %) ;**
 - **Banque-crédit (25%), en particulier pour contester leur inscription au fichier des incidents de remboursement des crédits aux particuliers « FICP »**
 - **Travail (15%), principalement pour s'opposer à la mise en place de dispositifs de contrôle de leur activité professionnelle ;**
 - **Opérateurs télécoms (15%), notamment pour contester la gestion de leurs données par les opérateurs de téléphonie ou, plus largement, pour s'opposer à la diffusion de leurs données personnelles sur Internet ;**
 - **Education (10%), en particulier pour dénoncer les sites Internet de notation des professeurs ;**
 - **Divers (10%)**

44

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

La CNIL en quelques chiffres – Activité 2008



45

Copyright Société PRONETIS 2011 – Droits d'utilisation ou de reproduction réservés.

LES OBLIGATIONS DE SECURITE DES DONNEES

Code pénal, Section 5 : Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques

Art. 226-17

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300.000 € d'amende.

Article 34

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

46

Copyright Société PRONETIS 2011 – Droits d'utilisation ou de reproduction réservés.

LA PROTECTION DES BIENS IMMATERIELS

Attribuer des droits aux auteurs de logiciels en tant qu'œuvres originales
Protéger ces droits face à la contrefaçon

Art. L. 335-2. (modifié par L. n°94-102 du 5 fév. 1 994)

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon ; et toute contrefaçon est un délit :

- La contrefaçon en France d'ouvrages publics en France ou à l'étranger est punie de deux ans d'emprisonnement et de 152.450 € d'amende.
- Sont punis des mêmes peines l'exportation et l'importation des ouvrages contrefaits.

LA PROTECTION DES DONNEES & DES SYSTEMES

Loi Godfrain 5 Janvier 1988 Art. 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30.000 euros d'amende.

Lorsqu'il en est résulté, soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45.000 € d'amende.

Art. 323-2

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende

LA PROTECTION DES DONNEES & DES SYSTEMES

Art. 323-3

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende.

Art. 323-3-1

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

CYBER SURVEILLANCE - CONTRÔLE DE CONNEXION INTERNET

- **Le contrôle de l'utilisation d'Internet**
 - Aucune disposition légale n'interdit l'employeur de fixer les conditions et les limites d'utilisation d'Internet
 - Mise en place de dispositifs de filtrage de sites non autorisés associés au pare-feu peut constituer une mesure de prévention dont il y a lieu d'informer les salariés
 - Possibilité offerte aux salariés de se connecter à Internet à des fins non professionnelles peut s'accompagner de prescriptions légitimes (Chat, Web mail perso, téléchargement) dictées par l'exigence de sécurité de l'entreprise (politique de sécurité, charte utilisateur)
- **Le contrôle nominatif des connexions Internet des salariés**
 - Conformément à l'art. L432-2-1 du code du travail, ce contrôle doit faire l'objet de préalable d'une consultation du comité d'entreprise ou du comité technique paritaire ou toute instance équivalente et d'une information des utilisateurs
 - Faire une déclaration à la CNIL en précisant la finalité du traitement, la durée de conservation...

CYBER SURVEILLANCE - LE CONTRÔLE DE L'USAGE DE LA MESSAGERIE ÉLECTRONIQUE

- Un message émis ou reçu depuis le poste de travail de l'entreprise revêt un caractère professionnel :
 - Sauf indication manifeste dans l'objet du message ou dans le nom du répertoire dans lequel ce message a été archivé qu'il lui conférerait le caractère et la nature d'une correspondance privée protégée par le secret des correspondances
 - Avant d'accéder aux messages, l'employeur doit donc vérifier que l'objet du message ne lui confère pas un caractère manifestement personnel – **Exemple – Personnel dont l'objet du message**
- Un contrôle de l'encombrement du réseau peut conduire l'entreprise à
 - Mettre en place des quotas pour la taille des fichiers transmis en pièces jointes ou encore des outils d'archivage des messages échangés.
 - L'emploi de tels outils de contrôle et d'archivage doivent être portés à la connaissance des salariés ainsi que la durée de conservation des messages

51

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

CYBER SURVEILLANCE - LE CONTRÔLE DE L'USAGE DE LA MESSAGERIE ÉLECTRONIQUE

- Un contrôle individuel par poste du fonctionnement de la messagerie
 - Communication auprès des utilisateurs
 - Faire une déclaration à la CNIL en précisant la finalité du traitement, la durée de conservation...
- Cas des fichiers et des répertoires créés par un employé
 - Il a été jugé que les fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel (Cour de cassation, 18 octobre 2006). Tout fichier qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder hors la présence du salarié.
 - En revanche, si un fichier est identifié comme étant personnel, l'employeur ne peut y avoir accès « qu'en présence du salarié ou si celui-ci a été dûment appelé, ou en cas de risque ou événement particulier ».

Par exemple : il a été jugé que la découverte de photos érotiques dans le tiroir d'un salarié ne constituait pas un risque ou un événement particulier justifiant que l'employeur accède au répertoire intitulé « perso » hors la présence du salarié ou sans que celui-ci en soit informé.

52

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

CYBER SURVEILLANCE - ADMINISTRATEURS SYSTÈMES ET RÉSEAUX

- Administrateurs systèmes et réseaux
 - Ils sont conduits par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions au internet, fichiers "logs" ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail. Un tel accès n'est contraire à aucune disposition de la loi du 6 Aout 2004
 - De même, **l'utilisation encadrée de logiciels de télémaintenance** ne soulève aucune difficulté particulière au regard de la loi du 6 Aout 2004 à condition que les mesures de sécurité nécessaires à la protection des données soient mises en œuvre.
 - Toutefois, aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications ne saurait être opérée, d'initiative ou sur ordre hiérarchique.

53

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

CYBER SURVEILLANCE - ADMINISTRATEURS SYSTÈMES ET RÉSEAUX

- Secret professionnel des administrateurs systèmes et réseaux
 - De même, les administrateurs de réseaux et systèmes, tenus au secret professionnel, ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise.
 - Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.
 - L'obligation de confidentialité pesant sur les administrateurs informatiques doit ainsi être clairement rappelée dans leur contrat, ainsi que dans la charte d'utilisation des outils informatiques annexée au règlement intérieur de l'entreprise ou de l'administration.

54

Copyright Société PRONETIS 2011 - Droits d'utilisation ou de reproduction réservés.

CYBER SURVEILLANCE - ADMINISTRATEURS SYSTÈMES ET RÉSEAUX

- Que faire en cas de difficulté ?
 - En cas de contestation, il appartient aux juridictions compétentes d'apprécier la régularité et la proportionnalité de l'accès par l'employeur au poste informatique ou à la messagerie de l'employé.

« Les hommes ne voient la nécessité que dans la crise »

Jean Monnet



Merci pour votre attention

Pour plus d'information www.pronetis.fr