RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

SGDN

Service central de la sécurité
des systèmes d'information

Issy-les-Moulineaux, le 2 mai 2000

N° 00063**e** SGDN/SCSSI/SI/bc

Note du Service Central de la sécurité des Systèmes d'Information
au sujet de
la protection des informations et systèmes sensibles dans les administrations.

La modernisation des services de l'État[1] et le recours aux technologies de l'information et de la communication, s'ils rendent les administrations et ses services, centraux, déconcentrés et territoriaux, plus efficaces, les exposent aussi à de nouvelles vulnérabilités tout en créant un *nouvel écheveau de responsabilités entrecroisées*[2].

La directive 4201du premier ministre[3], relative à la sécurité des systèmes d'information, clarifie le cadre des actions nécessaires pour maîtriser les risques dans ce domaine: "**Sécuriser l'information doit être un souci général. Sécuriser les systèmes d'information est une obligation nationale majeure**." Elle fonde la recommandation 901 du Premier ministre[4] du 2 mars 1994 pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.

Il convient donc, après avoir défini les rôles et les responsabilités des acteurs, fait l'inventaire des informations sensibles, après avoir choisi et pris les mesures de protection, mis en place des procédures de traitement des incidents, d'identifier les situations à risques pour mieux savoir les prévenir et les gérer[5].

En ce qui concerne la mise en place de procédures d'échanges d'informations *dématérialisées*, les solutions décentralisées qui ont l'avantage de la souplesse, doivent néanmoins s'inscrire dans une politique de sécurité globale clairement définie afin que les informations sensibles restent protégées dans toute la chaîne d'échanges grâce à la prise de responsabilité sans équivoque de tous les acteurs soutenus par les moyens techniques appropriés.

Cette politique est bien celle qui est mise en œuvre dans le cadre du PAGSI[1], en particulier dans le cadre de la mise sur internet des formulaires administratifs[6] et des téléprocédures de façon à "**garantir la qualité et la fiabilité des services offerts**"[7].

En pratique, chaque unité d'un organisme, est tenue, sous la responsabilité de l'autorité qualifiée pour la sécurité des systèmes d'information ou à défaut de l'autorité hiérarchique, de faire l'inventaire[10] structuré des informations et systèmes sensibles qui lui sont propres et, pour chacun d'entre eux, d'en exprimer la sensibilité en analysant l'impact des sinistres[11]. Des mesures de protection utiles et appropriées doivent être déterminées et prises une fois les nécessaires arbitrages rendus, par l'autorité hiérarchique responsable de l'organisme, entre coûts et sécurité[12]. L'autorité hiérarchique de l'unité est personnellement responsable de l'application des mesures résultant de la politique de sécurité interne (nota PSI)de l'organisme et des mesures particulières propres à son unité.

Dans certains ministères[13] cette *recommandation n°901* est devenue *une instruction.* Cette recommandation a la même force exécutoire qu'une circulaire ou une instruction. Certaines affaires récentes[14] montrent qu'il ne faut pas prendre ces questions à la légère et que la responsabilité de l'État peut être engagée[15] à la suite d'une méconnaissance des règles élémentaires de protection des informations *sensibles* et de la responsabilité des organismes et agents des administrations.

En effet, au sein de chaque ministère et des établissements sous tutelle, il existe des informations qui, sans devoir être classifiées de défense[16], nécessitent néanmoins d'être protégées, parfois avec autant, sinon plus, de précautions.

18, rue du Docteur Zamenhof Tel. : 01.41.46.37.84
92131 Issy-les-Moulineaux Cedex Fax : 01.41.46.37.01

Par exemple, le non-respect de la confidentialité de telle ou telle information porterait atteinte au secret de la vie privée. Ou encore, est-il souhaitable qu'une note de la direction de l'administration centrale en direction du cabinet se retrouve à l'extérieur ?

La *confidentialité* est le facteur prédominant dans les sinistres visibles, mais la question de l'intégrité de l'information ou sa disponibilité peuvent jouer un rôle parfois plus important. De telles informations sont qualifiées *d'informations sensibles* et ont fait l'objet de la recommandation[4] du Premier ministre le 2 mars 1994, mentionnée plus haut. Elles comprennent notamment :

- **les informations vitales pour l'exercice de la mission de l'organisme,**
- **les informations protégées par la loi relevant du secret professionnel (secret statistique, secret médical, secret douanier, …)**
- **les informations nominatives au sens de la loi informatique et libertés,**
- **les informations qui sont soumises à l'obligation de réserve ou de discrétion, professionnelle, notamment celles qui préparent une décision finalisée[17] laquelle est seule accessible avec ses motivations définitives,**
- **les informations constitutives du patrimoine scientifique, industriel et technologique,**
- **les informations concernant les appels d'offres et marchés des administrations,**
- **les informations permettant d'authentifier les actes dématérialisés, mettant ainsi en jeu la responsabilité des personnes qui les initient.**

1. PAGSI, voir les sites www.internet.gouv.fr/francais/textesref/sommaire.html et www.mtic.pm.gouv.fr
2. «**Responsabilité des décideurs et systèmes d'information**», L'actualité juridique—Droit administratif du 20 janvier 1999.
3. Directive interministérielle nº4201/SG du 13 avril 1995 relative à la sécurité des systèmes d'information. http://www.ssi.gouv.fr/fr/documentation/4201/4201.html
4. N° 901/DISSI/SCSSI : Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense. (Article 4 pour la définition) http://www.ssi.gouv.fr/fr/documentation/901/index.html.
5. pp 114, 122 et ss dans «**Responsabilité et déontologie, guide de référence pour les chefs de services et pour l'encadrement**», *207 pages*, ISBN 2-85978-285-0, *Presses de l'École Nationale des Ponts et Chaussées*, Janvier 1998. Ministère de l''Équipement, des Transports et du logement Direction du Personnel et des Services DPS/GA2, Tour Pascal B 92055 PARIS – La Défense Cedex 04 téléphone 01.40.81.61.77
6. La circulaire du 31 décembre 1999 (parue au journal officiel du 07/01/2000 page 00279) http://www.legifrance.gouv.fr/citoyen/jorf_nor.cgi?numjo=PRMX0003923C
7. Le communiqué le 7 janvier 2000 http://www.premier-ministre.gouv.fr/PM/070100.HTM
8. La circulaire du 7 octobre 1999 **relative aux sites internet des établissements publics de l'État** (http://www.internet.gouv.fr/francais/textesref/circu071099.htm). Les ministères **"en matière de sécurité sont responsables de leur propres systèmes d'information".**
9. Décret nº80-243 du 03 avril 1980 (JO du 5 avril 1980) portant création **des hauts fonctionnaires de défense modifié par le décret nº86-446 du 14 mars 1986** Il est responsable de l'application des dispositions relatives à la sécurité de défense et à la protection du secret (Décret n° 86-446 du 14 mars 1986, art. 1er), "**ainsi qu'à la sécurité des systèmes d'information**" .
10. **Guide** nº730/SCSSI du 13 janvier 1997 **sur les systèmes d'information et applications sensibles**.
11. Voir la méthode EBIOS (**E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité) mise en œuvre dans de nombreux organismes privés et publics, élaborée par le SCSSI et disponible à l'adresse suivante: http://www.ssi.gouv.fr/fr/confiance/ebios.html Les principes en sont très simples: • **identifier les biens (informations) et services à protéger** en fonction du contexte dont les contraintes légales et réglementaire et la mission de l'organisme, • **analyser les conséquences d'incidents sur ces biens et services** pour déterminer des impacts et qualifier la nature et la priorité des besoins de sécurité, • **analyser, en parallèle, les vulnérabilités des architectures techniques** pour déterminer les scénarios d'agressions possibles créant des incidents de sécurité sur les biens et • **choisir les objectifs de sécurité adéquats pour minimiser les risques**: c'est à dire minimiser les impacts compte-tenu de l'intensité des menaces. Ces objectifs de sécurité (techniques et non techniques) seront mis en œuvre par le responsable du système.
12. Guide technique nº150/SGDN/DISSI/SCSSI du 10 février 1991 **F**iche d'**e**xpression **r**ationnelle des **o**bjectifs de **s**écurité (FEROS) à faire approuver par l'autorité qualifiée. http://www.ssi.gouv.fr/fr/documentation/150/index.html.
13. Ministère de la Défense, ministère de l'Équipement.
14. confer l'affaire de l'hôpital d'Orléans "**L'État est condamné pour la divulgation d'une note de l'Inspection des affaires sociales**", quotidien Le Monde du 21 mai 1999 page 12, Jean Yves Nau. taille 4672 caractères.*Le tribunal administratif d'Orléans à condamné l'État, mardi 18 mai, à verser 119 000 francs à ..*
voir http://archives.lemonde.fr
15. Loi 83-634 du 13 Juillet 1983 modifiée portant **droits et obligations des fonctionnaires**. http://www.legifrance.gouv.fr/textes/html/fic198307130634.htm ou http://www.admi.net/jo/loi83-634.html.
16. IGI nº1300/SGDN/SSD/DR du 12 mars 1982 Instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État.
17. Loi n°78-753 du 17 juillet 1978 : "Mesures des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal" modifiée par la loi nº79-587 du 11 Juillet 1979 (voir l'article 6) complétée par la loi n° 2000-321 du 12 avril 2000 (j.o. page 05646) relative aux droits des citoyens dans leurs relations avec les administrations NOR : FPPX9800029L http://www.legifrance.gouv.fr/citoyen/jorf_nor.ow?numjo=FPPX9800029L ou http://www.admi.net/jo/20000413/FPPX9800029L.html