Conseil d'Administration du 29 Janvier 2010

Université Lille 1
Politique de Sécurité du Système d'Information

Introduction

Comme indiqué dans la « Déclaration d'Intention », l'Université Lille 1 considère que son Système d'Information est indispensable à l'accomplissement de ses missions et a décidé d'établir, de mettre en œuvre, de surveiller et d'améliorer de façon continue un « processus de gestion de la sécurité de l'information ».
Les premières étapes consistent à définir le domaine d'application et la politique de sécurité du Système d'Information.
Ces étapes sont décrites dans le présent document, plus communément appelé « Politique de Sécurité du Système d'Information (PSSI) ».

1. Définitions

Actif : tout élément représentant de la valeur pour l'organisme [ISO/CEI 13335-1:2004] ; on distingue les actifs primordiaux (l'information) et les actifs de support (ressources permettant de traiter l'information : matériels, personnels, réseaux, …)
Confidentialité : propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés
Disponibilité : propriété d'être accessible et utilisable à la demande par une entité autorisée
Intégrité : propriété de protection de l'exactitude et de l'exhaustivité des actifs

2. Domaine d'application

2.1. Contexte

L'Université Lille 1 est un Établissement Public à Caractère Scientifique, Culturel et Professionnel dont les missions sont d'assurer (LRU, Article L123-3) :

- la formation initiale et continue,
- la recherche scientifique et technologique, la diffusion et la valorisation des ses résultats,
- l'orientation et l'insertion professionnelle,
- la diffusion de la culture et l'information scientifique et technique,
- la participation à la construction de l'Espace européen de l'enseignement supérieur et de la recherche,
- la coopération internationale.

L'Université Lille 1 est répartie sur plusieurs sites géographiques de la région Nord Pas-de-Calais mais la grande majorité de ses composantes sont rassemblées sur le Campus de Villeneuve d'Ascq : administration, centres de ressources, bâtiments d'enseignement, unités mixtes d'enseignement et de recherche, IUT, écoles universitaire d'ingénieurs.
Le Campus de Villeneuve d'Ascq héberge également des entités autonomes telles l'Ecole Nationale Supérieure de Chimie de Lille, l'Ecole Centrale de Lille ou Telecom Lille 1 ; ces entités autonomes partagent des ressources matérielles avec l'Université (services généraux, réseau de données).
Les chercheurs de l'Université Lille 1 sont principalement sous tutelle du CNRS, de l'INRIA, de l'INSERM et de l'INRA.

2.2. Actifs vitaux du Système d'Information de l'Université Lille 1

Les éléments du Système d'Information (SI) que l'Université Lille 1 considère comme essentiels (« vitaux ») à ses missions :

- les actifs de la fonction Finance,
- les actifs de la fonction Gestion du Personnel,
- les actifs de la fonction Scolarité,
- les actifs vitaux pour la recherche : gestion des contrats, des brevets et des publications.

2.3. Exclusions actuelles du domaine d'application de la PSSI

Les actifs qui ne sont pas concernés par la présente version de la PSSI sont ceux des établissements autonomes situés sur le campus de Villeneuve d'Ascq :

- Ecole Centrale de Lille,
- Ecole Nationale Supérieure de Chimie de Lille.

Cependant, il convient de souligner que si ces entités partagent des ressources communes avec l'Université Lille 1, les « frontières décisionnelles » devront être clairement définies (exemple : définition des responsabilités concernant la gestion des éléments actifs du réseau de données).
Pour les laboratoires de recherche, la décision d'appliquer la PSSI de l'Université Lille 1 ou la PSSI de l'organisme de recherche sera précisée dans le cadre des contrats ou accords de partenariat.

3. Politique de Sécurité du Système d'Information

3.1. Objectifs principaux de sécurité

L'Université Lille 1 décide que son système d'information doit posséder les caractéristiques suivantes :

- être capable de fournir l'Information uniquement à ceux qui en ont besoin (Confidentialité),
- être capable de fournir l'Information en temps utile (Disponibilité),
- être capable de fournir de l'Information juste (Intégrité),

Pour atteindre et maintenir ses objectifs principaux de sécurité, l'Université Lille 1 mettra en œuvre les mesures de sécurité nécessaires, sans que ces mesures soient en contradiction avec ses principes de gouvernance et le cadre législatif.

3.2. Principes de gouvernance et cadre législatif

La mise en œuvre des mesures de sécurité se devra de respecter les conditions suivantes :

- cohérence avec le contrat d'établissement de l'Université Lille 1,
- recherche d'un consensus en privilégiant dialogue, sensibilisation et formation,
- respect des lois (cf. annexe : principales lois concernant la sécurité du SI),
- respecter les obligations légales de journalisation et d'archivage,
- mise en place d'un processus continu de gestion de la sécurité de l'information,
- prise en compte des ressources (budgets, personnels, etc.),
- suivi des recommandations nationales (cadre commun et SDSSI du MENESR) et internationales (ISO 2700N –SMSI- et « bonnes pratiques »).

3.3. Détail des objectifs de sécurité

3.3.1. Propriétaire des actifs

Etant donné qu'il s'agit d'une condition nécessaire à la gestion des droits d'accès aux actifs, l'Université Lille 1 décide qu'il convient de désigner les propriétaires des actifs et de préciser les responsabilités de ces propriétaires.
Pour l'Université Lille 1, les propriétaires sont désignés par le président de l'Université, dans le respect des dispositions légales (par exemple, le propriétaire pour la fonction Finances est nécessairement l'agent comptable).
Le terme « propriétaire » identifie une personne ou une entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des actifs (informations et ressources). Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur le bien (ISO 27002).

3.3.2. Gestion des utilisateurs

L'Université Lille 1 décide qu'il convient d'authentifier les utilisateurs du S.I., afin de permettre les contrôles d'accès et la journalisation ; il convient également de gérer le « cycle de vie » de ces utilisateurs pour réévaluer régulièrement leurs droits d'accès.

3.3.3. Propriétés de sécurité des actifs

L'Université Lille 1 décide qu'il convient d'attribuer à chaque actif un degré de confidentialité, de disponibilité et d'intégrité ; le triplet (C,D,I) résultant est indispensable à l'évaluation de la valeur de l'actif dans le processus d'analyse et d'évaluation du risque et aux mesures de sécurité devant être appliquées (cf. annexe : Evaluation C,D,I d'un actif).

3.3.3.1. Degrés de confidentialité de l'information

Les degrés de confidentialité sont déterminés par les conséquences résultant d'une divulgation de l'information à des personnes non autorisées. Les degrés de confidentialité retenus par l'Université Lille 1 sont les suivants :

- **`Secret`** : perte de confidentialité grave (pertes financières importantes, sanctions administratives),
- **`Restreint`** : perte de confidentialité dommageable (atteinte à l'image de marque, baisse de confiance des partenaires, poursuites judiciaires, pertes financières faibles) ; exemple : données nominatives, sujets ou notes d'examen, données d'appels d'offre, données de recherche, supports de cours,
- **`Publique`** : perte de confidentialité sans conséquence ; exemple : sites WEB.

3.3.3.2. Degrés de disponibilité d'un actif

Les degrés de disponibilité sont déterminés par les conséquences résultant de l'impossibilité d'accéder ou d'utiliser un actif au moment désiré. Les degrés de disponibilité retenus par l'Université Lille 1 sont les suivants :

- **`Haute`** : indisponibilité grave ; exemple : arrêt du réseau, arrêt de la messagerie, données vitales non disponibles,
- **`Moyenne`** : indisponibilité gênante ; exemple : imprimante, accès à l'Internet,
- **`Faible`** : indisponibilité concernant des éléments de confort ou pour lesquels il existe des solutions de remplacement ; exemple : sites WEB informatifs.

3.3.3.3. Degrés d'intégrité d'un actif

Les degrés d'intégrité sont déterminés par les conséquences résultant de la modification accidentelle ou volontaire non autorisée d'une information. Les degrés d'intégrité retenus par l'Université Lille 1 sont les suivants :

- **`Grave`** ; exemple : coordonnées bancaires de tous les fournisseurs,
- **`Dommageable`** ; exemple : article de recherche,
- **`Sans conséquence`** ; exemple : coordonnée téléphonique.

3.3.4. Confidentialité

3.3.4.1. Accès logique

L'Université Lille 1 décide qu'il convient d'associer à chaque actif des listes de contrôles d'accès sous la forme de triplets Information/Droit d'accès/Utilisateur et qu'il est de la responsabilité du propriétaire d'un actif d'établir et maintenir ces listes de contrôle d'accès (cf. annexe : exemple de fiche « matrices de droits »).

3.3.4.2. Accès physique

L'Université Lille 1 décide qu'il convient de limiter l'accès physique aux ressources matérielles du S.I. afin d'être en conformité avec les critères de confidentialité définis pour les actifs hébergés par ces ressources matérielles.

3.3.5. Disponibilité et Intégrité

3.3.5.1. Conformité des sauvegardes

L'Université Lille 1 décide qu'il convient de vérifier que les sauvegardes des informations sont conformes aux niveaux de confidentialité, de disponibilité et d'intégrité exigés pour ces informations.

3.3.5.2. Plan de reprise d'activité

L'Université Lille 1 décide qu'il convient de définir, mettre en œuvre et tester un plan de reprise d'activité pour les informations jugées critiques en matière de disponibilité.

3.3.6. Respect des obligations légales de journalisation et d'archivage

3.3.6.1. Journaux

L'Université Lille 1 décide qu'il convient de mettre en œuvre des mécanismes de journalisation des accès aux ressources du S.I. et de gérer les durées de conservation des journaux.

3.3.6.2. Droits des utilisateurs

L'Université Lille 1 décide qu'il convient d'informer les utilisateurs des actions de journalisation.

3.3.7. Respect des lois

3.3.7.1. Chartes

L'Université Lille 1 décide qu'il convient de diffuser et de faire accepter des chartes informatiques « Utilisateurs », « Administrateurs » et « Syndicats ».

3.3.7.2. Sensibilisation

L'Université Lille 1 décide qu'il convient d'informer et de sensibiliser toutes les catégories d'utilisateurs sur les risques encourus par le SI.

3.3.8. Respect des « bonnes pratiques »

Indépendamment des choix politiques et des priorités d'action définis par la PSSI, l'Université Lille 1 décide qu'il convient de respecter au moins les recommandations « métier » en matière de SSI. Ces recommandations, appelées « bonnes pratiques » sont détaillées dans la norme internationale ISO 27005 (Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information-), mais nécessitent d'être adaptées aux spécificités de l'Université (cf. document « bonnes pratiques »).

3.3.9. Processus continu de gestion de la sécurité du S.I.

3.3.9.1. Gestion continue de la sécurité

L'Université Lille 1 décide d'établir, de mettre en œuvre de surveiller et d'améliorer de façon continue un processus de gestion de la sécurité du SI.

3.3.9.2. Normes

L'Université Lille 1 décide de s'appuyer sur les recommandations présentées dans les normes ISO 27001 « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences ».

3.4. Organisation

3.4.1. Acteurs de la S.S.I. de l'Université Lille 1

La définition des personnes ou services concernés par la SSI de l'Université Lille 1 ainsi que les relations existant entre ces personnes ou services sont détaillés dans l'annexe Organisation de la SSI pour l'Université Lille 1. On y définit également les relations entre l'Université Lille 1 et les entités extérieures (organismes nationaux de SSI, autorités de police, justice, etc.).

3.4.2. Actions à effectuer en cas d'incident de sécurité

On entend par « incident de sécurité » un acte de malveillance s'attaquant au système d'information (« piratage »). Traiter un incident de sécurité le plus efficacement possible nécessite de respecter certaines règles ; ces règles sont formellement définies dans le document intitulé « Procédure de traitement des incidents de sécurité du système d'information pour l'Université Lille 1 » (Les principes majeurs à respecter sont la définition des intervenants, la conservation des preuves et la formalisation des relations avec les tiers - autorités judiciaires et de police , presse, …-)

3.5. Principales étapes de mise en œuvre de la PSSI

La liste complète des principales étapes de mise en œuvre de la PSSI reste à définir, mais les premières étapes seront les suivantes (détails dans l'annexe Description des premières étapes à mettre en œuvre) :

- Sensibiliser les utilisateurs aux « risques informatiques » et à la loi « informatique et libertés »
- Nommer un Correspondant Informatique et Libertés
- Diffuser et faire accepter une charte informatique « Utilisateur »
- Identifier précisément qui peut avoir accès aux données

3.6. Principaux documents à rédiger

Les documents à rédiger, adapter ou réactualiser sont en priorité les suivants :

- Lettres de mission aux RSSI, CIL, correspondant sécurité
- Charte Utilisateur
- Charte Administrateur
- Charte Syndicat
- Procédure de traitement des incidents de sécurité

Annexe : description des premières étapes à mettre en œuvre

Sensibiliser les utilisateurs aux « risques informatiques » et à la loi « informatique et libertés »

Le principal risque en matière de sécurité informatique est l'erreur humaine. La formation, la sensibilisation et l'information des utilisateurs sont donc cruciales pour la sécurité. Cette sensibilisation peut prendre la forme de formations, de séminaires, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques. La sensibilisation se fait de manière permanente. Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique. Ce document devrait également rappeler les conditions dans lesquelles un utilisateur peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord du CIL de l'établissement.

Nommer un Correspondant Informatique et Libertés (CIL) :

Le CIL permet de garantir la conformité de l'organisme à la loi « informatique et libertés ». Cette maîtrise des risques juridiques est d'autant plus importante que certains manquements à la loi du 6 janvier 1978 sont pénalement sanctionnés. La désignation d'un CIL entraîne la dispense de déclarations des traitements auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). Le CIL est alors chargé de tenir un registre des traitements, mis à disposition du public et de la CNIL. L'une des missions du CIL est de s'assurer que toutes les précautions utiles ont été prises pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des personnes non autorisées y aient accès.

Diffuser et faire accepter une charte informatique « Utilisateur » :

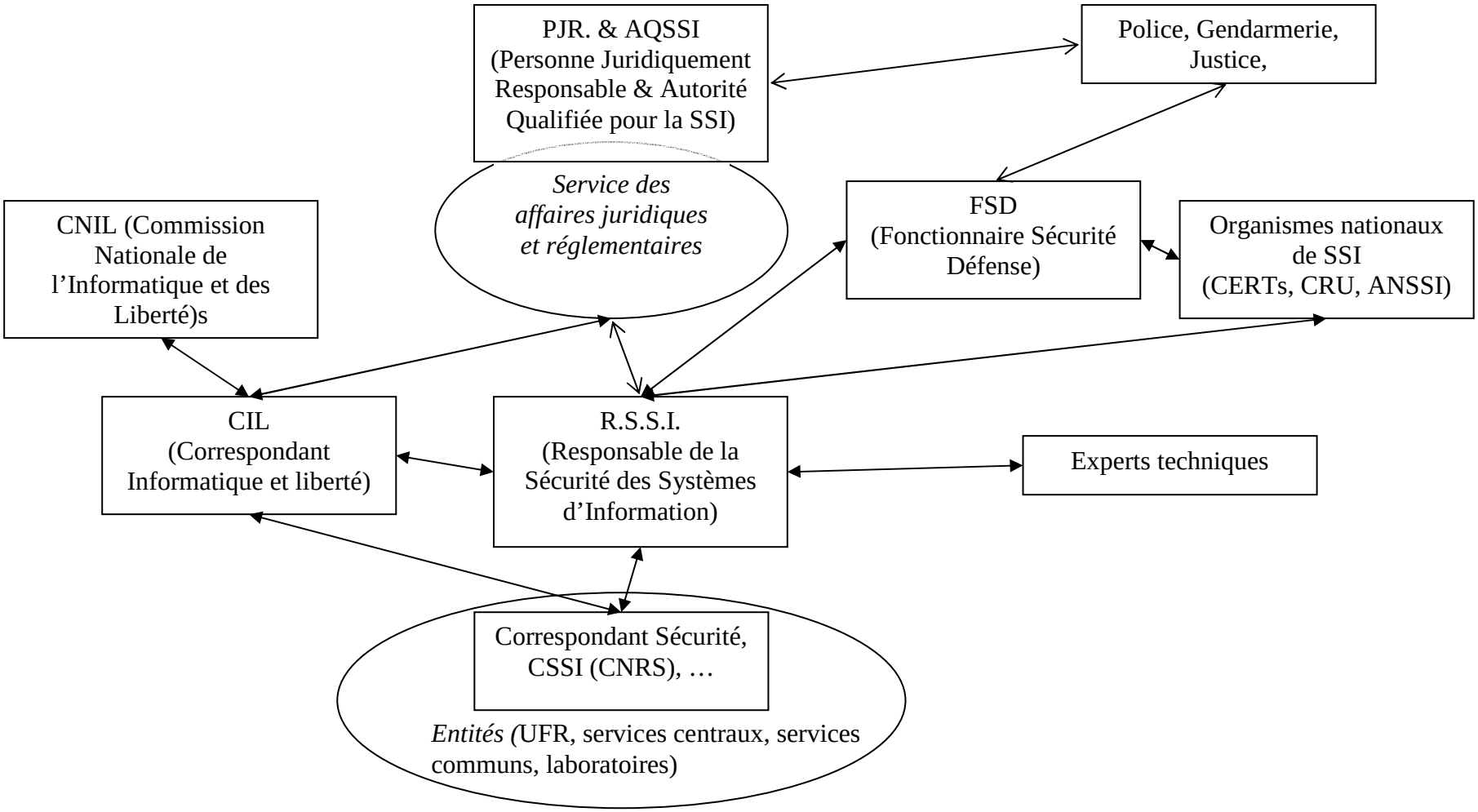
Préalablement à son accès aux outils informatiques, l'utilisateur doit obligatoirement prendre connaissance des droits et devoirs que lui confère la mise à disposition par l'Université Lille1 de ces outils. Cette information se fait au travers d'une charte informatique, qui énonce la « loi commune » régissant l'utilisation des moyens informatiques ; elle est intégrée dans le règlement intérieur.

Identifier précisément qui peut avoir accès aux données :

L'accès aux données traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent concerné. La clarification du processus d'arrivée, de déménagement et de départ d'un agent, permet au supérieur hiérarchique concerné d'identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès. Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

Annexe : Organisation de la SSI pour l'Université Lille 1

Schéma



Rôles de chaque « acteur de la SSI»

Organismes nationaux de S.S.I. (ANSSI, CERTs, …) : un réseau de compétence, de veille et de transfert d'information est opérationnel au niveau national et a pour mission (entre autres) de diffuser des recommandations, d'assister et d'informer les administrations en matière de SSI. Les principales composantes de ce « réseau » sont :

- l'Agence Nationale de la Sécurité des Systèmes d'Information (rattachée au Secrétariat Général de la Défense Nationale),
- le Haut Fonctionnaire de Défense et de Sécurité et le Fonctionnaire de Sécurité des Systèmes d'Information pour le ministère de l'Education Nationale,
- le Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA) et le CERT de Renater (Computer Emergency Response Team).

Personne Juridiquement Responsable (PJR) : personne ayant la responsabilité de représenter l'Université ; il s'agit du Président et ses délégataires.

Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI). L'AQSSI est responsable de la désignation des acteurs de la chaîne fonctionnelle SSI. Pour l'Université Lille 1, l'AQSSI est le Président de l'Université.

Fonctionnaire Sécurité Défense (FSD) : nommé par le Président, il a pour mission la protection, sous tous ses aspects, du patrimoine scientifique et technique de l'établissement

Service des Affaires Juridiques et Réglementaires : le Service des Affaires Juridiques assiste la PJR pour toute question … juridique et réglementaire, y compris en cas d'incidents de SSI.

Responsable de la Sécurité des Systèmes d'Information (RSSI) : Le RSSI et son suppléant reçoivent la mission officielle d'établir et mettre en œuvre le processus continu de gestion de la sécurité du S.I. de l'Université. Le RSSI est le garant de l'application de la PSSI. S'appuyant sur un réseau d'experts et de correspondants, il « orchestre » le fonctionnement quotidien de la SSI. Il centralise les informations concernant les incidents de sécurité et relaye les informations provenant des organismes nationaux de SSI (CERT Renater et ANSSI/CERT-A). La fonction de RSSI est très orientée « organisationnel », nécessite de fréquents contacts avec la direction de l'Université et a besoin d'une certaine indépendance par rapport aux opérationnels, afin d'éviter d'être « juge et partie ».

Correspondant Informatique et Liberté (CIL) : Le CIL permet un allègement des formalités de déclaration des traitements informatiques auprès de la CNIL ; Une fois le correspondant désigné, seuls les traitements soumis à autorisation ou avis préalable de la CNIL devront continuer à être déclarés. Les autres traitements, qui ne comportent pas de risques manifestes pour les droits des personnes, feront l'objet d'une déclaration simplifiée auprès du Correspondant Informatique et Liberté de l'établissement, qui les référencera dans une liste tenue localement.

Experts techniques SSI : informaticiens de l'Université ayant une très bonne connaissance des systèmes et des réseaux et susceptibles de mettre ponctuellement ou quotidiennement leurs compétences au service de la SSI.

Correspondants sécurité : toutes les entités de l'Université (UFR, services centraux, services communs, laboratoires, etc.) sont concernées par la SSI et ont donc tout intérêt à disposer d'un « correspondant sécurité ». Au minimum, le rôle du correspondant sécurité est de relayer l'information provenant des RSSIs et de mettre en œuvre la « Procédure de traitement des incidents de sécurité ». Si l'entité dispose déjà d'un correspondant sécurité d'un organisme de recherche (CSSIs du CNRS en particulier), il n'est pas nécessaire de nommer un correspondant sécurité spécifique à l'Université.

Annexe : principales lois concernant la sécurité du SI

La mise en œuvre de systèmes d'information est soumise à des obligations relevant de nombreux textes d'ordre législatif et réglementaire qui confèrent un enjeu juridique important à cette activité.
On peut citer en particulier,

- loi sur la confiance en l'économie numérique (LCEN),
- loi relative à l'informatique et aux libertés (loi CNIL),
- loi relative à la fraude informatique (loi Godfrain),
- instructions et recommandations interministérielles provenant du Secrétariat Général de la Défense Nationale (SGDN).

S'y ajoutent des dispositions relevant du code de la propriété industrielle, et des dispositions pénales (en particulier articles 226 et 227).

Annexe : Evaluation C,D,I d'un actif

Définitions

Actif : tout élément représentant de la valeur pour l'organisme; on distingue les actifs primordiaux (l'information) et les actifs de support (ressources permettant de traiter l'information : matériels, personnels, réseaux, …).

Confidentialité : propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés.
Disponibilité : propriété d'être accessible et utilisable à la demande par une entité autorisée.
Intégrité : propriété de protection de l'exactitude et de l'exhaustivité des actifs.

Degrés : Les degrés de confidentialité, de disponibilité et d'intégrité sont déterminés par les conséquences d'un accès non autorisé, d'une indisponibilité et d'une altération d'un actif :

- Confidentialité : **`Secret`**, **`Restreint`**, **`Publique`**
- Disponibilité : **`Haute`**, **`Moyenne`**, **`Faible`**
- Intégrité : **`Grave`**, **`Dommageable`**, **`Sans conséquence`**

Exemples

Exemple 1 : évaluation C,D,I de l'actif « article de recherche en cours de rédaction »
Confidentialité : Restreint
Disponibilité : Moyenne
Intégrité : Dommageable

Exemple 2 : évaluation C,D,I de l'actif « site WEB de l'Université Lille 1 »
Confidentialité : Publique
Disponibilité : Moyenne
Intégrité : Dommageable

Exemple 3 : évaluation C,D,I de l'actif « coordonnées bancaires de tous les fournisseurs »
Confidentialité : Publique
Disponibilité : Faible
Intégrité : Grave

Exemple 4 : évaluation C,D,I de l'actif « sujet d'examen »
Confidentialité : Secret
Disponibilité : Haute
Intégrité : Grave

Annexe : exemple de fiche « matrices de droits »

EN COURS
EN COURS
EN COURS
EN COURS
EN COURS
EN COURS
EN COURS

Rimbaus
Propriétaire : VP Scolarité
Utilisateurs :

- Administrateurs Techniques : Responsable pôle gestion et responsable d'application
- Secrétariats pédagogiques :
- Enseignants
- Etudiant : lecture de toutes ses informations personnelles (notes, convocations, …), modification de certaines informations personnelles (adresse ?, …)
-

EN COURS
EN COURS
EN COURS
EN COURS
EN COURS
EN COURS
EN COURS