Schéma Directeur de la Sécurité du Système d'Information

Université de La Réunion

Octobre 2011

Schéma Directeur de la Sécurité du Système d'Information

Table des matières

Préface....3
Avant-Propos....3
Préambule....4
Objectifs....4
Cadre d'élaboration....4
Contexte politique et stratégique....4
Contexte juridique....5
Contexte institutionnel et organisationnel....5
Contexte technique....5
Les missions menées....6
La charte pour les personnels de l'Education Nationale....6
La charte de bon usage des moyens informatiques....6
Gestion des traces informatiques....6
L'autorisation et les droits d'accès....7
La protection d'accès à Internet....7
La sauvegarde de l'information....7
Nomination d'un CIL....7
Les missions à mener....8
Élaboration d'une PSSI....8
Elaboration d'un Plan d'Action Sécurité....8
Elaboration d'un carnet de sécurité du système d'information....9
Désigner la chaîne de la sécurité opérationnelle des SI....9
Le RSSI....10
Les usagers privilégiés du système d'information....11
Les correspondants de sécurité....11
Les usagers du système d'information....11
Organiser des audits réguliers sur la sécurité du SI....12
Sensibilisation à la sécurité....12
Mise en place d'un PRA....12
Outils de suivi et de reporting....12
Outils d'enregistrement des contrôles, actions correctrices, gestion des non conformités....13
AQSSI....14
RSSI....14
CIL....14
Correspondants sécurité du SI....14
Administrateurs Systèmes et réseaux....14
Administrateurs Système d'Information....14

Préface

Avant-Propos

Les technologies de l'information et de la communication, leurs usages pédagogiques et professionnels connaissent une montée en puissance. Les espaces numériques de travail dédiés aux étudiants, aux personnels se multiplient. L'administration électronique se développe rapidement. Dans cette perspective, il importe de mettre en œuvre les conditions d'une confiance accrue dans l'esprit d'une démarche qualité. La sécurité des systèmes : un problème essentiel, majeur ; leur complexité les rend vulnérables car elle accroît les failles non repérées par les concepteurs.

Les systèmes d'information s'ouvrant de plus en plus vers l'extérieur, ils doivent le faire dans un cadre sécurisé et maîtrisé. Dans ce domaine, le service public d'éducation et à fortiori l'université de la Réunion doit se montrer exemplaire.

Avec la modernisation de l'administration et l'évolution des réglementations publiques nationales et européennes, ce schéma directeur de la sécurité des systèmes d'information se révèle un outil indispensable et essentiel, adapté au contexte, pour garantir et coordonner toute la sécurité attendue dans la généralisation de leurs usages par les communautés éducatives.
Des règles éthiques et déontologiques sont par exemple nécessaires en ce qui concerne les usages des TIC par les étudiants et personnels de l'université de la Réunion.

Cette politique de sécurité doit être communiquée et expliquée pour responsabiliser les utilisateurs. Une chaîne de responsabilité et d'alerte doit être mise en place.

L'accroissement des risques de toute nature auxquels sont soumis les systèmes d'information a conduit le Premier ministre à demander en avril 2003 d'établir un plan de renforcement de la sécurité des systèmes d'information de l'État (**PRSSI**). Ce plan, consultable à l'adresse http://www.ssi.gouv.fr doit couvrir les moyens de communication et les systèmes d'information, en termes de capacités opérationnelles de réponse aux attaques informatiques et de gestion de crise.

En point d'entrée de la chaîne fonctionnelle, on trouve au niveau de chaque ministère le haut fonctionnaire de défense (**HFD**) et le fonctionnaire de sécurité des systèmes d'information (**FSSI**). Notre Ministre a nommé en juillet 2005 un FSSI en la personne de Mme Isabelle Morel, ce qui a été d'ailleurs une première pour notre ministère qui ne disposait pas d'un FSSI auparavant. La chaîne se prolonge ensuite pour chaque grande entité du ministère par une "autorité qualifiée pour la sécurité des systèmes d'information" (**AQSSI**) et un "responsable de la sécurité des systèmes d'information" (**RSSI**).

Cette notion d'"autorité qualifiée" recouvre l'exercice de la maîtrise d'ouvrage, la responsabilité de passer les actes contractuels mais aussi la responsabilité de mettre en place des organisations, de faire des arbitrages budgétaires en terme d'équipements, de services et de moyens humains, la responsabilité d'intenter des actions en justice. L'AQSSI est assisté par un RSSI qu'il nomme et mandate pour mettre en place et veiller à la bonne réalisation de la politique générale de sécurité qu'il a lui-même impulsée.

[Dominique Antoine - Bernard Vors, HFD]

Préambule

Le Schéma Directeur de Sécurité Systèmes d'Information (**SDSSI**) est un projet prioritaire s'inscrivant dans un cadre de modernisation des systèmes d'information, de personnalisation des accès et d'ouverture à tous de l'usage des technologies de l'information et la communication (TIC) avec le niveau de sécurité attendu.
Le Schéma Directeur de Sécurité s'inscrit dans une démarche méthodologique consistant à ouvrir tous les trois ans un grand chantier dans le domaine de la sécurité des systèmes d'information (SSI) dans l'optique :

- de vérifier que l'organisation mise en œuvre est opérationnelle et performante ;
- d'actualiser les axes d'orientation au regard des évolutions technologiques ;
- de mesurer l'adéquation entre les enjeux de la SSI et les risques encourus ;
- d'évaluer la compatibilité des moyens accordés avec les objectifs visés ;
- d'actualiser le plan d'action SSI.

Objectifs

Le Schéma Directeur de la Sécurité des Systèmes d'Information vise à :

- expliciter les contextes de mise en œuvre du schéma directeur ;
- identifier et préciser les enjeux de la sécurité pour les communautés éducatives ;
- définir une organisation et préciser les responsabilités à tous les échelons de l'Éducation nationale ;
- offrir un cadre commun pour la définition et la mise d'œuvre des politiques de sécurité dédiées ;
- fixer les orientations techniques sous-jacentes aux projets de modernisation des systèmes d'information (SI) ainsi qu'au développement sécurisé de l'administration électronique ;
- et enfin, à traduire les objectifs de sécurité sous forme de plans d'actions opérationnels.

Cadre d'élaboration

Contexte politique et stratégique

L'élaboration d'une politique de sécurité des systèmes d'information (**PSSI**) revêt un caractère stratégique pour le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, et à fortiori, pour l'université.

Cette politique s'inspire de l'effet conjugué, d'une part, de la généralisation de l'utilisation des technologies de l'information et, d'autre part, des menaces spécifiques que ces technologies induisent en terme de fonctionnement.
De ce fait, l'université est amenée à :

- déterminer la politique de sécurité des systèmes d'information (arbitrages entre sécurisation et ouverture absolue des services par exemple) ;
- renforcer ses capacités de protection des systèmes d'information dans le cadre du PRSSI interministériel (Plan de Renforcement de la Sécurité des Systèmes d'information) ;
- mobiliser des moyens dédiés et à procéder aux nécessaires mutualisations des ressources et compétences.

Par ailleurs, l'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**, créée en 2009, ex-DCSSI) du Secrétariat Général de la Défense Nationale (**SGDN**) incite chaque département

ministériel à mettre en œuvre la recommandation interministérielle relative à la protection des systèmes d'information traitant des information sensibles non classifiées de défense (n° 901du 2 mars 1994).

Cette recommandation définit les grandes orientations de la politique de sécurité à mettre en œuvre en matière de sécurité des systèmes d'information, pour assurer la protection des informations sensibles non classifiées de défense, dans le respect des lois et règlements en vigueur. Elle précise également l'organisation à mettre en place pour appliquer cette politique. Enfin, elle définit et répartit les responsabilités entre les différents intervenants dans ce domaine.

Contexte juridique

Le schéma directeur de la sécurité des systèmes d'information découle également d'une prise en compte au plus haut niveau de l'institution de l'évolution des réglementations publiques nationales et européennes.

Ainsi, la loi a progressivement pris en compte l'importance des TIC, prévoyant dès 1978 de protéger la vie privée des personnes (loi «informatique et libertés») jusqu'à encadrer l'économie numérique en 2004.

La réglementation en vigueur engage la responsabilité de personnes physiques et morales autant dans le système éducatif que dans l'ensemble de la société d'où la nécessité d'organiser la sécurité des systèmes d'information.

Contexte institutionnel et organisationnel

Au sein du système éducatif, étudiants, enseignants, enseignants-chercheurs et personnels administratifs se partagent tous l'usage des systèmes d'information. Le niveau d'appréhension, la perception des objectifs et des contraintes peuvent sembler différents selon le type d'acteur concerné.

C'est pourquoi la sécurité des systèmes d'information, particulièrement dans le monde de l'éducation, doit tenir compte de la diversité des acteurs, du partage des responsabilités défini dans le cadre de la loi, de la spécificité des communautés territoriales et des communautés éducatives.

Cependant cette diversité ne doit pas être un frein à la formation et la sensibilisation de l'ensemble des usagers des ressources numériques.

Contexte technique

L'évolution des moyens techniques est à l'origine d'une interaction forte entre systèmes d'information, systèmes informatiques et organisations. Aujourd'hui, l'importance accrue des réseaux du fait d'un déploiement massif des postes de travail informatiques rend leur fiabilité et leur disponibilité impérative.

L'accroissement des performances des matériels, combinée aux fortes baisses de coûts, a progressivement amené les systèmes d'information à se substituer aux modes de travail traditionnels vers lesquels il ne saurait être envisageable de revenir, ne serait-ce que ponctuellement.

Cette nouvelle organisation tend à abolir la notion d'espace de travail géographiquement localisé,

mais cette souplesse absolue nécessite d'imposer des mesures strictes de cloisonnement des réseaux comme de règles de confinement des zones d'interopérabilité.
La sécurité des systèmes d'information doit s'inscrire dans un cadre technique maîtrisé.

Les missions menées

La charte pour les personnels de l'Education Nationale

Cette charte de référence a été élaborée et mise au point pour encadrer les conditions d'utilisation des ressources informatiques et systèmes d'information de l'institution par les personnels du ministère de l'Éducation nationale.

Exerçant une activité professionnelle au sein d'une entité relevant de la responsabilité d'une PJR, les personnels et autres intervenants (professionnels, associatifs...) se doivent de respecter la réglementation en général et tout particulièrement les règles de déontologie et de sécurité consignées dans la charte d'utilisation des ressources informatiques dont les PJR doivent assurer la diffusion.

En tant qu'utilisateur et/ou personnel de l'état, chaque individu est responsable en tout lieu et tout temps de l'usage qu'il fait des ressources informatiques, des réseaux ou des systèmes qui sont mis à sa disposition.

La charte de bon usage des moyens informatiques

Cette charte a été établie au sein de l'Université par le RSSI et sert à cadrer l'usage des ressources aussi bien des personnels que des étudiants. On y retrouve des mesures visant à limiter l'utilisation de la sortie Internet pour des raisons d'éloignement et de faibles débit pour l'ensemble des usagers, ainsi que des règles légales, de propriété intellectuelle, etc.

La faiblesse de cette Charte réside dans le fait qu'elle n'est pas régulièrement consultée par les usagers, et les nouveaux arrivants n'ont pas pour obligation de la signer à leur arrivée, d'où un axe fort du SDSSI basé sur la communication et la sensibilisation en terme de sécurité du Système d'Information.

Gestion des traces informatiques

Tracer l'activité des systèmes d'information est primordial pour une organisation. L'exploitation des traces, qui doit être déclarée à la CNIL, doit permettre :

- de détecter les attaques, les activités inhabituelles ou inappropriées qu'elles soient d'origine interne ou externe.
- la «Personne Juridiquement Responsable» ainsi que le Responsable de Sécurité des Systèmes d'Information doivent avoir à leur disposition le bon niveau de traces.
- de déterminer l'étendue d'une intrusion éventuelle afin de la circonscrire.
- d'aider à la conduite d'enquête concernant les attaques détectées afin de pouvoir les neutraliser définitivement.

A cet effet, des moyens de traces informatiques ont été mis en place, et une Charte de la gestion des traces informatiques a été diffusée à l'ensemble de la communauté. Elle est disponible sous forme numérique sur le site web de l'université.

L'autorisation et les droits d'accès

L'autorisation (gestion des droits) consiste à accorder à une identité numérique des droits d'accès correspondant à son profil ou à ses missions (rôles).

Les principes de l'authentification et de l'autorisation seront mis en œuvre dans le cadre des Espaces Numériques de Travail (ENT) mis à la disposition des étudiants et personnels de l'université de la Réunion.

Il est recommandé d'utiliser un annuaire de référencement unique afin d'établir l'identification de l'individu et de centraliser l'information, et dans notre cas, le référent est un annuaire LDAP maintenue par l'équipe en charge du SI.

La protection d'accès à Internet

L'usage de l'Internet dans les pratiques éducatives est déjà très largement développé et se banalise progressivement avec le déploiement généralisé des accès. Cette banalisation des accès et des usages doit bénéficier de mesures d'accompagnement adaptées, destinées à faciliter le travail des équipes pédagogiques, tout en prenant en compte des impératifs de sécurité et notamment la protection des mineurs et l'intégrité du réseau.

Différents types de situations peuvent se présenter lors de la navigation sur l'Internet :

- *l'accès à des contenus inappropriés dans le cadre éducatif.*

Concrétisés principalement par l'affichage de contenu inapproprié, que ce soient des contenus répréhensibles vis à vis de la loi et de la protection des mineurs (pages pornographiques, racistes, etc.), ou des contenus qui n'ont pas directement leur place dans le cadre éducatif ;

- *les menaces visant l'intégrité du réseau*

Se manifestant principalement par des attaques virales ainsi du code malveillant présent dans des pages visitées et dont l'objectif final est souvent le vol des données ;

- *l'accès à des contenus inappropriés dans le cadre professionnel*

Concrétisés principalement par l'affichage de contenu inapproprié, que ce soient des contenus répréhensibles vis à vis de la loi ou des contenus qui n'ont pas directement leur place dans le cadre professionnel.

La mise en place d'un dispositif de contrôle ou de sélection, comme cela a été fait pour les courriers électroniques, doit être effectuée également sur l'accès à l'Internet. L'établissement doit identifier les besoins exprimés par l'ensemble des acteurs, et choisir un dispositif qui permette de répondre aux impératifs de sécurité tout en prenant en compte les besoins des acteurs et des usagers.

La sauvegarde de l'information

Les données sensibles doivent être sauvegardées afin de palier à un éventuel soucis, volontaire ou non. Actuellement, une solution de sauvegarde est en place sur bandes magnétiques afin de pouvoir restaurer les données contenues dans les bases de données, les courriels, les pages web de l'université, etc.

Nomination d'un CIL

L'université de la Réunion est pourvu d'un Correspondant Informatique et Libertés (**CIL**) dont la nomination figure en *Annexe A*.

Ce statut a été créé dans le cadre de la refonte de la loi de janvier 1978, votée en été 2004 (loi du 6 août 2004); il répond au mot d'ordre fixé par le président de la CNIL, le sénateur Alex Türk: «Simplifier les procédures (...) et substituer les contrôles a posteriori aux contrôles a priori» des fichiers informatiques.

Concrètement, les organismes qui nommeront de tels correspondants pourront s'affranchir de toute déclaration préalable de leurs fichiers informatiques. Le rôle de la CNIL étant alors cantonné à des contrôles a posteriori et à des sanctions, le cas échéant. Le rôle du CIL sera naturellement de «tenir la liste des traitements», et d'alerter la Commission en cas d'irrégularité.

Les missions à mener

Élaboration d'une PSSI

Définition : Celle de la commission Européenne
Ensemble de lois, règlements et pratiques qui régissent la façon de gérer, protéger, diffuser les biens, en particulier les informations sensibles au sein de l'organisation. -- *Source catalogue des critères d'évaluation de la sécurité des systèmes d'information , ITSEC, Commission Européenne, Juin 1991*

Pour le moment, l'université est pourvue d'une Charte de bon usage des moyens informatique, ce qui est réglementairement suffisant.

Cependant, afin d'étendre notre activité et offrir des services dans un cadre général et légal, il est important de mettre en place une Politique de Sécurité du Système d'Information, en y spécifiant des références réglementaires et légales claires (LCEN, CNIL 2, Loi Godfrain, propriété intellectuelle, etc.) et des consignes et procédures cohérentes.

Les procédures de contrôle et d'audit doivent être clairement définies sur la base de la transparence, de la discussion collective obligatoire avec les organes représentatifs du personnel et de la proportionnalité de mesures pouvant être prise en cas d'infraction en respect de l'article L121-8 du code du travail.

Enfin elle doit préciser de façon non équivoque la position de la Direction quant à l'utilisation à titre privé et personnel des ressources mises à disposition du personnels, notamment les moyens Internet et Mail.

Elaboration d'un Plan d'Action Sécurité

C'est la déclinaison opérationnelle du schéma directeur de la sécurité du Système d'Information.
Le plan d'action sécurité décrit ou met à jour pour l'année les tâches liées à la mise en œuvre de la sécurité des informations au sein de l'université, et il est ordonnancé en fonction des priorités, c'est à dire en fonction des besoins de sécurité calculés lors de l'analyse des risques.
Ceci implique donc de mettre en place au préalable une analyse des risques et des menaces (que

peut-on redouter et si cela se produit, est-ce grave ?) puis de mettre en place une gestion des risques (obtenir une absence de risques inacceptables par la mise en œuvre de mesures de sécurité).

Elaboration d'un carnet de sécurité du système d'information

Toute application ou système d'information doit disposer d'un carnet de sécurité. Ce carnet constitue l'outil de référence en matière de SSI.

Ce carnet a vocation à être renseigné tout au long du cycle de vie du SI par l'ensemble des acteurs impliqués dans le processus de développement et de l'exploitation des SI.

Chaque dossier de sécurité produit au cours du cycle de vie du SI se doit d'être intégré dans le carnet de sécurité, lequel sera partagé par tous les acteurs impliqués.
Le carnet de sécurité contient :

- Le dossier d'identification des objectifs de sécurité émanant de la MOA.
- Les exigences de sécurité déterminées par la MOE.
- Le cahier de spécifications fonctionnelles précisant :
  - le choix des fonctions et des mécanismes de sécurité choisi pour couvrir les exigences de sécurité
  - la définition des tests de sécurité.
- Le cahier de spécifications techniques précisant :
  - l'architecture technique retenue
  - les règles de codification des éléments de sécurité.
- Le cahier de qualification de la sécurité.
- Le dossier CNIL (si besoin, et fourni par notre CIL).
- Le cahier d'exploitation spécifiant :
  - les consignes d'installation
  - les consignes d'utilisation.

La complétude du carnet de sécurité relève de la responsabilité du chef de projet garant de la bonne application des procédures. La mise en production d'un SI est conditionnée par le respect des règles consignées dans le carnet de sécurité mais également par la prise en compte de la PSSI de l'université.

Désigner la chaîne de la sécurité opérationnelle des SI

En préalable à l'identification des acteurs de la chaîne de la sécurité des systèmes d'information, il convient de rappeler le constat suivant : les défaillances de sécurité trouvent leur cause, dans leur grande majorité, dans des comportements humains inappropriés.

En conséquence, les utilisateurs internes des systèmes d'information doivent être informés de leur responsabilité individuelle en matière de sécurité des systèmes d'information dans le cadre de leur fonctions ou des missions qu'ils exercent au sein de l'établissement.

Ceci implique également que chacun puisse disposer des éléments d'informations organisationnels nécessaires pour faire face à des situations d'attaques logiques ou des perturbations du fonctionnement de leur environnement de travail.

En effet, en dépit de la complexité des technologies déployées pour prévenir les risques ou protéger

les systèmes d'information, il convient de réaffirmer la prééminence du facteur humain dans l'organisation de la sécurité des systèmes d'information (SSI).

Il s'agit donc bien, dans un premier temps, de recenser les acteurs concernés ou impliqués à quelque titre que ce soit par cette problématique globale de sécurité.
Interviennent dans le domaine de la SSI au niveau de l'Université de la Réunion :

- Le haut fonctionnaire de défense et ses services.
- Les autorités hiérarchiques (Président, VP)
- Les responsables hiérarchiques (DGS, DRH)
- Le responsable de la sécurité des systèmes d'information (RSSI)
- Les correspondants techniques de sécurité (CIL, chef de projet, ...)
- Les usagers privilégiés du système d'information
- Les usagers du système d'information

L'autorité hiérarchique d'une entité est responsable de la sécurité des systèmes d'information existants ou à venir, exploités par et pour elle-même. Ainsi, elle doit mettre en place une organisation chargée de l'application des mesures de sécurité et du contrôle de son efficacité.

Elle est personnellement responsable de l'application de la PSSI.

Par convention, l'autorité hiérarchique sera appelée «Personne Juridiquement Responsable» ou **PJR**.
Pour exercer cette responsabilité, l'autorité hiérarchique doit s'appuyer sur le Responsable de la Sécurité des Systèmes d'Information (**RSSI**).
Au niveau de l'Université, le responsable de la sécurité des systèmes d'information, les correspondants techniques de sécurité, les usagers privilégiés du système d'information ainsi que les usages du système d'information sont à définir.

Le RSSI

Le Responsable de la Sécurité des Systèmes d'Information est nommé par la «Personne Juridiquement Responsable».

La nomination du RSSI est mentionnée en *Annexe A*.

A ce titre, le Responsable de la Sécurité des Systèmes d'Information conseille la «Personne Juridiquement Responsable» en matière de sécurité des systèmes d'information.
Les missions principales du RSSI sont les suivantes :

- constituer et coordonner un réseau interne de correspondants de sécurité ;
- mettre en place les plans de sécurité adaptés aux établissements et aux services, en cohérence avec le Cadre Commun de la Sécurité des Systèmes d'Information et de Télécommunications ;
- organiser le référencement des sites dangereux ou illicites au niveau de l'université (en accord avec la Charte Renater) et
- assurer la mise à jour des dispositifs de filtrage en conséquence ;
- contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels ;
- informer et sensibiliser les utilisateurs du système d'information aux problématiques de sécurité ;

- améliorer la SSI par une veille technologique active ainsi que par une participation aux groupes de réflexion ad hoc ;
- assurer la coordination avec les différents organismes concernés.

Pour assurer pleinement toutes les composantes de sa mission, le RSSI s'appuie sur une chaîne de Correspondants de Sécurité qu'il organise et dont il est le référent.

Les usagers privilégiés du système d'information

Situés dans la DSI, il s'agit des informaticiens ayant à la fois les connaissances et les privilèges d'accès aux ressources manipulés par les usagers du système d'information, que ce soit au niveau serveur, ou poste local.

Ils travaillent en collaboration avec les correspondants de sécurité, devant sensibiliser les usagers du SI et s'assurer de la bonne application et respect de la Charte de bon usage des moyens informatique. Ils sont tenus de remonter toute anomalie visant à porter atteinte à l'intégrité du SI aux correspondants de sécurité.

Les usagers privilégiés du SI sont soumis à une charte administrateurs informatique.

Les correspondants de sécurité

Sous l'autorité de la PJR et l'appui nécessaire du RSSI, les Correspondants de Sécurité sont chargés de la mise en œuvre de la sécurité au sein d'une entité donnée. Ils ont une qualification informatique de niveau administrateurs systèmes et réseaux ou, à défaut, des compétences reconnues en la matière. Leur nombre peut varier selon la nature et la taille de l'entité dans laquelle ils évoluent.

Les Correspondants de Sécurité mettent en œuvre les règles générales d'exploitation, consignées dans le carnet de sécurité des systèmes d'information, pouvant être complétées par des mesures liées aux spécificités de l'entité.

Chaque correspondant de sécurité devra être désigné. Sa prise de fonction est accompagnée de la prise de connaissance d'une charte nationale «administrateurs» par laquelle il est informé de ses droits et devoirs. Dès lors, il s'engage à respecter cette charte qui est annexée au règlement intérieur de l'université.

Tout correspondant de sécurité doit être identifié et associé à la politique de sécurité.

Les usagers du système d'information

En bout de chaîne de SSI, on trouve les usagers du SI qui seront définis comme des entités ayant accès à des ressources informatiques, dotées de privilèges plus ou moins élevés, leur permettant de manipuler de l'information au travers d'applications gérés par le SI de l'université.

Les usagers du SI sont tenus de lire, d'accepter et d'appliquer les règles relatives à la sécurité du SI, comme la charte de bon usage des moyens informatiques.

Tout usager du système d'information doit être identifié et répertorié dans le carnet de sécurité du SI.

Organiser des audits réguliers sur la sécurité du SI

Bien que prévu dans la PSSI, des interventions d'audits doivent être planifiées afin d'établir le niveau de maturité de notre SI, mais certains audits pourront et devront être effectuées auprès des usagers afin de déterminer le respect des différentes règles de sécurité, leur niveau de sensibilisation à la sécurité du SI, ainsi que la détection éventuelle de failles qui ne seraient
pas couvertes par l'analyse de risques.

Sensibilisation à la sécurité

Les dispositifs de sécurité ne peuvent être efficients que s'ils sont perçus comme des bénéfices et non vécus comme des contraintes.

Pour cela, un apprentissage minimal de la SSI d'ensemble est nécessaire. Divers moyens doivent être utilisés pour y parvenir :

- formation des étudiants au travers du Certificat Informatique et Internet (C2I).
- séminaires de sensibilisation et formation des décideurs, «Personne Juridiquement Responsable» et «Autorités Qualifiées pour la Sécurité des Systèmes d'Information».
- communications sur la sensibilité d'une application à destination des personnels de l'université.
- mise en place de points d'informations à chaque échelon hiérarchique.
- formation des maîtrises d'ouvrages, maîtrises d'œuvres, RSSI, Correspondants Techniques et Correspondants de Sécurité (notamment à la gestion des risques SSI).

Parallèlement à ces actions, la charte d'utilisation des ressources et de bon usage des systèmes d'information doit être diffusée aux personnels pour leur signifier leurs droits et devoirs en la matière.

Mise en place d'un PRA

Un des dispositif central pour la sécurité de notre SI, est la mise en place d'un Plan de Reprise d'activité à minima. Cette procédure repose avant tout sur la bonne santé du SI en général ainsi que sur la solidité du système de sauvegarde.

Une telle procédure est indispensable tout au long de l'année, et principalement durant des périodes clés à déterminer, comme les inscriptions, les examens, etc.
Elle vise avant tout à minimiser les risques de perte de disponibilité des différents services du SI, assurer leur confidentialité ainsi que leur intégrité.

Un travail de gestion des risques et d'études des différentes menaces est donc à faire avant la mise en place de cette procédure, notamment au travers d'un Plan d'Action Sécurité.

Outils de suivi et de reporting

L'idée étant de pouvoir sortir des indicateurs quant à l'utilisation du réseau en interne et en externe, ainsi que les différents services informatiques qui sont le plus sollicités.

Ces outils n'ont pour vocation que de mesurer les différentes pointes de trafic, les éventuels engorgements, les services nécessitants plus de ressources, ressortir les différentes périodes d'activités, etc.

Outils d'enregistrement des contrôles, actions correctrices, gestion des non conformités

L'université de la Réunion a besoin d'assurer un suivi sur les différentes actions menées par les correspondants sécurité que ce soit en terme d'accès aux différentes ressources (physiques et logiques) qu'en terme d'actions menées avec un horodatage centralisé et un déport des journaux électroniques (logs), ceci afin de pouvoir revenir sur une action rapidement en cas de problème, ou de connaître la source d'un incident.

Annexe A – Nominations

AQSSI

L'AQSSI de l'établissement est Pr. Mohamed ROCHDI

RSSI

Le RSSI de l'établissement est M. Laurent PEQUIN
Les RSSI-suppléants sont :

- M. Vincent CARPIER
- M. Matthieu BANNIER

CIL

Le CIL de l'établissement est M. Thierry BRUGNON

Correspondants sécurité du SI

Administrateurs Systèmes et réseaux

M. Vincent CARPIER
M. Laurent PEQUIN
M. Matthieu BANNIER
M. Teddy TRECASSE
M. Didier BOUCHE

Administrateurs Système d'Information

M. Etienne GOURDON
M. Jephte CLAIN
M. Loïc MOUSSELLET
M. Ilias TIMOL
Usagers privilégiés du Système d'Information
M. Teddy THERMIDOR
M. Jean NG-THUNE
M. Majid AMODE
M. Thierry MARDEMOUTOU
Mlle Véronique NASRI
M. Fabien HERMANN
M. Sébastien KRAMARZ
M. Patrick RIVIERE
M. Ausmane MOHAMED
M. Bruno LEUNG-YEN-FOND
M. Mathias PAYET