Politique de Sécurité des systèmes d'Information de l'état (PSSI-E)

Document d'orientation de la sécurité des systèmes d'information de l'Université de la Polynésie Française

V1

30 septembre 2016

Date	Version	Rédacteur	Commentaire
4/6/16	1.0	H.Duarte	Création du document.
30/9/16	1.1	H.Duarte	Présentation COPIL

Préface

Avant-Propos

Les technologies de l'information et de la communication, leurs usages pédagogiques et professionnels connaissent une forte progression. Les espaces numériques de travail dédiés aux étudiants, aux personnels se multiplient. L'administration électronique, la dématérialisation, se développent rapidement.

Dans cette perspective il faudra mettre en œuvre les conditions d'une confiance accrue entre les utilisateurs et les systèmes d'informations.

La complexité des systèmes les rend vulnérables car elle accroît les failles non repérées par les concepteurs et les administrateurs.

Les systèmes d'information sont essentiels à l'action de l'état. Ils sont porteurs d'efficacité mais aussi des risques : menaces d'exfiltration de données confidentielles, atteinte à la vie privée des usagers, voire de sabotage des SI.

1. Introduction

1.1 Le contexte de l'université de la Polynésie Française

L'université de la Polynésie Française (UPF) est le seul établissement universitaire public français à caractère scientifique, culturel et professionnel (EPSCP). Il comporte 3 départements (droit/éco/gestion, Lettres/langues et Sc. Humaines, Sciences/technologies et santé) ainsi qu'un ESPE, un institut (Confucius) et un service de formation continue.

La recherche est représentée par 6 laboratoires (CIRAP, OGT, GEPASUD EA 4238, GAATI, EASTCO, GDI) et une UMR. L'UPF occupe des locaux situés dans un espace géographique unique.

Notre établissement héberge une bibliothèque universitaire qui accueille de nombreux lecteurs externes.

Le fonctionnement de l'établissement est assuré par un ensemble de services qui prennent en charge l'administration, la logistique, la scolarité, la gestion du patrimoine, la restauration, la médecine préventive, les ressources informatiques,…

Dans ce cadre certaines personnes bénéficient d'un logement de fonction. L'université de la Polynésie Française regroupe environ ??? (220) personnels (enseignants et non enseignants) et ??? (3500) étudiants.

1.2 Contexte institutionnel

Au sein de notre établissement étudiants, enseignants, enseignants-chercheurs et personnels administratifs se partagent l'usage des SI.

Les contraintes et objectifs peuvent ainsi être perçus différemment selon le type d'acteur concerné.

Pour ces raisons la sécurité des systèmes d'information doit tenir compte de la diversité des acteurs sans perdre de vue les deux missions phare de l'université : L'enseignement et la recherche

1.3 Contexte Technique

La multiplication et l'évolution des techniques sont à l'origine d'une forte interaction entre les organisations et les systèmes d'information.

L'accroissement des performances matérielles associé aux fortes baisses de coûts ont permis aux SI de se substituer aux modes de travail dits « traditionnels ».

Par ailleurs un retour, même ponctuel, vers ce mode de travail est toujours mal vécu par les différents acteurs concernés.

Dans ce nouvel espace de travail le mot « ubiquité » devient la règle.

Cette souplesse devra être accompagnée des mesures strictes de cloisonnement des réseaux ainsi que de la mise en place des zones d'interopérabilité.

La sécurité de nos systèmes d'information devra donc s'inscrire dans un cadre technique maîtrisé.

1.4 Contexte juridique

L'utilisation des systèmes d'information est soumise à des nombreux textes législatifs et réglementaires, pour citer quelques uns :

- La loi relative à l'informatique et aux libertés (« loi informatique et libertés »)
- La loi relative à la fraude informatique (loi Godfrain)
- La loi pour la confiance dans l'économie numérique (LCEN)
- Les instructions, circulaires et recommandations interministérielles provenant de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
- Les dispositions relevant du code de la propriété intellectuelle et des dispositions pénales
-

La délinquance et les « cyber-attaques » ont connus, ces derniers mois une progression fulgurante.

Tout cela conduit à la mise en place de mesures permettant de restreindre les risques encourus.

2- La sécurité des systèmes d'information

Le présent document a pour objectif d'établir une référence pour la mise en place d'une PSSI-E au sein de l'université de la Polynésie Française en prenant en compte ses spécificités ainsi que ses liens avec des acteurs extérieurs.

Cette PSSI-E fera l'objet de mises à jour en fonction de l'évolution des systèmes d'information et de l'usage qui en sera fait.

Chaque composante de l'UPF devra la mettre en application en l'adaptant à son propre contexte pour constituer une PSSI-E opérationnelle.

Les PSSI des organismes extérieurs hébergés ou à liens contractuels devront respecter les règles de la PSSI-E de l'UPF.

Ce document s'appuie sur la norme ISO 27001 et suivantes portant sur la sécurité des systèmes d'information. Le terme « entité » désigne une composante de l'UPF qu'il s'agisse d'une structure administrative, d'enseignement ou de recherche.

2.1 Le besoin en sécurité

Les actifs constituent le système d'information de l'UPF. Ils sont indispensables aux activités d'enseignement, de recherche et de l'administration.

Notre système d'information comporte de vulnérabilités d'origines diverses :

- Routines de gestion obsolètes ou défaillantes,
- Pannes d'équipements
- Environnement de travail mal contrôlé
- Défaillance humaine
- Attributions incorrectes de droits sur le SI ou ses processus, etc, etc

Ces vulnérabilités si elles sont « exploitées » peuvent avoir des conséquences dommageables pour l'université en termes de temps de travail, perte d'information, de coût financier, d'image, de réputation, etc…

Notre système d'information doit donc être sécurisé et placé à l'abri des menaces internes et externes. Les données doivent être protégées afin de garantir leur disponibilité et leur intégrité. Nos applications et services doivent être disponibles, fiables et garantir des résultats corrects.

L'utilisation et la mise en œuvre des SI s'inscrivent dans un cadre législatif et réglementaire destiné à protéger la vie privée (fichiers nominatifs, cyber-surveillance) et les droits de propriété intellectuelle (droits d'auteurs, brevets…)

Dans ce cadre peuvent être recherchées les responsabilités administratives ou pénales des différents acteurs : les utilisateurs, les administrateurs système, leurs hiérarchies,…)

Pour sécuriser notre SI il faut au préalable identifier, inventorier les biens essentiels et support.

A titre d'exemple parmi ceux dernier on trouve :

- Les équipements, l'infrastructure informatique,
- Les réseaux (filaire, wi-fi),
- Les équipements VoIP/ToIP,
- Les équipements d'impression,
- La vidéosurveillance, le contrôle d'accès, la visioconférence, etc, etc

Des projets comme la politique de site de la Polynésie Française, ou celui du contrôle interne budgétaire et comptable font émerger d'autres types de biens essentiels à protéger :

- Le partage de données de recherche via des archives ouvertes ou Open Access,
- Les données de valorisation et d'innovation de la recherche,
- Les processus représentant des enjeux majeurs pour l'université : Achats, paye, missions, heures d'enseignement..

3 Organisation de la sécurité des systèmes d'information

3.1 Organisation générale

La PSSI-E de l'université de la Polynésie Française s'inscrit dans le cadre de la politique et les directives émanant de l'ANSSI. Cette politique et ses directives sont relayées par le HFDS (Haut Fonctionnaire de Défense et Sécurité) assisté par le FSSI du ministère. Aussi elle s'appui sur la circulaire 38641 du 1er juillet 2014 du premier ministre qui demande une mise en conformité avec la PSSI-E de l'ANSSI.

Au sein de l'UPF la responsabilité générale de la SSI relève du président de l'université en tant que AQSSI (Autorité Qualifiée à la Sécurité des Systèmes d'Information). Il est assisté par les Responsables de la sécurité des systèmes d'information (RSSI). Les orientations stratégiques de la SSI sont définies au sein du comité de pilotage stratégique.

3.2 Chaîne fonctionnelle spécialisée de la SSI

La chaîne fonctionnelle interne SSI de l'UPF s'appuie sur la chaîne fonctionnelle nationale pilotée par l'ANSSI.

Elle est composée comme suit :

- AQSSI (Autorité qualifiée à la sécurité des système d'information) : Il s'agit de la PJR. C'est le président de l'université ou son représentant. Il est responsable général de la SSI de l'établissement,

- Les RSSI (Responsables de la sécurité des systèmes d'information) : Il s'agit des responsables opérationnels de la SSI. Voici quelques unes des missions principales :

    - Coordonner un réseau interne de CSSI (Correspondants sécurité des systèmes d'information),
    - Tracer et contrôler le niveau de sécurité du SI,
    - Informer et sensibiliser les utilisateurs du SI aux problématiques de sécurité,
    - Mettre en œuvre et suivre les dispositions SSI définies au niveau national,
    - Valider les projets d'établissement en ce qui concerne les aspects SSI,
    - Participer aux groupes de travail, réunions de coordination, action de formation au niveau national,
    - Etre contact privilégié du CERT et du CERT-A,
    - Etre le relais d'informations de sécurité (CERT, CERT-A, Renater..),
    - Correspondants auprès des autres RSSI,
    - Rédiger des documents SSI,
    - Mettre en place des opérations de prévention,
    - Analyser les bilans de SSI,
    - Faire des audits de sécurité des systèmes,
    - Organiser des actions de formation/information

- Les correspondants de la sécurité des SI (futur groupe utilisateurs) Assistent les directeurs d'entité dans l'exercice de leur responsabilité en matière de SSI. Dans le cas de l'UPF il s'agit du membre du comité des utilisateurs. Il a pour missions :
    - Veiller à la mise en place des mesures de sécurité nécessaires,
    - Sensibiliser les utilisateurs aux problématiques SI,
    - Relais auprès des RSSI,
    - Mise en place des opérations de prévention (opérationnel),
    - Appliquer les mesures de la chaîne fonctionnelle SSI,

- Le Correspondant Informatique et Libertés (CIL) ou Data Protection Officer (DPO) : Il sera désigné par l'AQSSI et il aura pour missions :

    - Veiller au respect des formalités requises par la loi « Informatique et libertés »,
    - Responsable de la conformité de données de l'établissement,
    - Maintenir un registre des traitements mis en œuvre,
    - Veiller à la bonne application de la loi « informatique et libertés ».

Propositions :

1- Création d'un comité de pilotage stratégique. Il sera composé de l'actuel COPIL SI-TICE _+ DRH + CIL (DPO)
2- Création d'un comité de sécurité opérationnel. Il sera composé des RSSI de l'UPF
3- Création d'un comité de liaison. Il sera composé des utilisateurs. nommés par leur hiérarchie ou l'administration centrale.