Université Fédérale
Toulouse Midi-Pyrénées

Politique de Sécurité des Systèmes d'information du site MP

Jean-François Parache

23/02/2013

Demandez le Programme :

PSSI de l’état

Les services proposés par l’interuniversitaire

Schéma Directeur Numérique de l’Université Fédérale Toulouse Midi-Pyrénées

La PSSI de site : les priorités

La PSSI de site au quotidien

Conclusion

2009 : Ministère de la défense
2011 : Ministère des Finances
2011 : Ministère de l'intérieur
2011 : gendarmerie nationale
2012 : Ministère de la Justice
2012 : l'Elysée
2013 : TV5 monde
2014 : Ministère de la santé
2015 : Étudiants de Lyon III
2015 : Ministère de l'intérieur
2016 : Ministère de la défense
2016 : Ministère des transports

1998 création des RSSI obligation d'écrire une politique de sécurité.
2002 schéma directeur de la sécurité.
2005 schéma directeur de la sécurité des systèmes d'information.
2006 PSSI au CNRS.
2011 Politique Générique de Sécurité des Systèmes d'Information.
Chaque année : Sensibilisation des gouvernances

Politique de Sécurité des Systèmes d'Information de l'état : Juillet 2014

C'est une instruction qui s'impose à nous ➔**182 mesures (197)**

Nous avons 3 ans pour nous y conformer.

Etat des lieux fourni Juillet 2015 (janvier 2015)

- Plan d'action
- Impact sur les activités
- Moyens financiers
- Moyens humains.

Premier Ministre

Renforcement rôle de l'ANSSI.

Renforcement des effectifs de l'ANSSI 150 ➔ 420 ➔ 730 (2017)

Contrôles réguliers.

L’organisation de la PSSIE :

1. Préambule : 10 principes stratégiques

2. Instruction : 10 articles « organisation PSSIE »

3. Objectifs et règles :
   13 thèmes
   34 objectifs
   182 mesures

7 : Politique, organisation, gouvernance
6 : Ressources humaines
4 : Gestion des biens
10 : SSI dans le cycle de vie des SI
16 : Sécurité physique
9 : Sécurité du développement
4 : Traitement des incidents

8 : Continuité d'activité
2 : Conformité, audit, inspection, contrôle
16 : Sécurité des réseaux
3 : Architecture des SI
71 : Exploitation des SI
26 : Sécurité du poste de travail

PSSIE : un impact fort pour les informaticiens.

GDB-CARTO : cartographie. La cartographie précise les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle.

DEV-LOG-CYCLE : intégrer la sécurité dans le cycle de vie logiciel. La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

PCA-LOCAL : définition du plan local de continuité d'activité des systèmes d'information. Le directeur des systèmes d'information ou le RSSI d'une entité définit la structure et les attendus du plan de continuité d'activité des systèmes d'information permettant d'assurer effectivement, en cas de sinistre, la continuité d'activité.

PSSIE : un impact fort pour les informaticiens (c’est pas fini).

RES-MAITRISE : systèmes autorisés sur le réseau. Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d’une entité.

INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d’information. Tout système d’information doit faire l’objet d’une décision d’homologation de sa sécurité avant sa mise en exploitation dans les conditions d’emploi définies.

Cette décision s’appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d’emploi.(analyse de risque systématique pour tout SI avec un niveau de profondeur adapté aux enjeux)

PSSIE : une révolution pour nos usagers.

RH-UTIL : sensibilisation des utilisateurs des systèmes d'information. Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles SSI.

RH-SSI : charte d'application SSI. Une charte d'application de la politique SSI, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle SSI, est communiquée à l'ensemble des agents de chaque entité. Cette charte doit être opposable juridiquement et, si possible, intégrée au règlement intérieur de l'entité. Le personnel non permanent (stagiaires, intérimaires, prestataires…) est informé de ses devoirs dans le cadre de son usage des SI de l'État.

PDT-STOCK : stockage des informations. Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur.

RH-CONF : personnels de confiance. Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention et une probité particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.

PSSIE : légitimation de nos demandes.

PHY-TECH : sécurité physique des locaux techniques. L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie, doit être physiquement protégé.

PHY-CI-MOYENS : délivrance des moyens d'accès physique. La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs, …), intervient systématiquement et impérativement sous surveillance permanente.

PHY_CI-EAU : lutte contre les voies d'eau. Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

RH-MOUV : gestion des arrivées, des mutations et des départs. Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les SI doit être formalisée, et appliquée strictement. Cette procédure doit couvrir au minimum :

Sommaire :

Services offerts par l'interU : CICT /COMUE / UNR / PRES / UFTMIP / UT

Gestion des cartes MUT

CAS / LDAP

Scout

Cloud

SICD / Bibliothèque

SIMPPS

Remip

Aster

Antispam

Schéma Directeur Numérique de l'Université Fédérale Toulouse Midi-Pyrénées

approuvé par le comité stratégique

Président du PRES
6 représentants des membres fondateurs
1 représentant des membres associés
1 représentant de la région

Fiche projet n°P4-5 – Définition d'une Politique de Sécurité des Systèmes d'Information (PSSI) de site

Sommaire :

Projet PSSI de Site : l'équipe

Yann Bachy, OSSI de l'ISAE,

Roland Dartiguepeyron, RSI et RSSI de la DR14 du Cnrs,

Frédéric Druilhet, RSI et RSSI Adjoint de la DR14,

Vincent Nicomette, enseignant chercheur INSA, Laas

Fabrice Prigent RSSI de l'Université Toulouse Capitole,

Jean-François Parache, RSSI de l'Université Toulouse Jean-Jaurès,

Ronan Tournier, enseignant chercheur l'Université Toulouse Capitole, IRIT.

Projet PSSI de Site : les priorités

1) Sécuriser et fiabiliser de manière progressive les services numériques existants fournis par l'UFTMIP aux établissements.

   Intégration d'une composante sécurité dans tout nouveau projet lié de près ou de loin à l'informatique.

2) Disposer d'une charte commune de sécurité des systèmes d'information en fonction des différentes populations d'utilisateurs.

3) Etude, spécification et maintien en condition opérationnelle d'une politique de sécurité relative à tous les projets des établissements de la COMUE et des Unités Recherche du site sur lesquelles ils exercent une tutelle.

4) Animer le réseau des RSSI du site.
   Favoriser une harmonisation progressive.
   Favoriser, par mutualisation, la formation des équipes informatiques des établissements.
   Favoriser une meilleure acceptabilité des mesures par les utilisateurs.

Sécuriser et fiabiliser de manière progressive

1) Etat des lieux :

objectif :

- Réaliser ou se procurer :
  - Cartographie applicative.
  - Cartographie Serveur.
  - Cartographie Réseau (physique, logique)
- Recenser les compétences à mobiliser

Démarche :

rencontrer ou contacter les acteurs (Comue, équipe de chaque projet, prestataire interne, hébergeur….)

se procurer la documentation ou la construire

Groupe de travail :

équipe projet

Livrables :

cartographies

Proposition de l'ordre de traitement pour l'expertise

Sécuriser et fiabiliser de manière progressive

2) Démarche d'expertise :

objectif :

Pour chaque service offert, mesure la distance à la PSSIE.

Fournir une appréciation sur le niveau de sécurité.

Proposer une roadmap priorisée.

Démarche :

utiliser la cartographie comme document de référence

rencontrer les équipes projets et/ou MCO.

établir la correspondance avec les règles SSI applicables

mesurer la distance à la norme.

Groupe de travail :

travail en sous groupe : membres de l'équipe projet + expert en fonction du thème abordé.

Livrables :

road map priorisée avec estimation financière, planning et RH.

POC : traitement de 2 services par 2 groupes de travail pilotes pour validation de la démarche,
mise en commun des compétences, harmonisation des pratiques, standardisation des livrables.

Sécuriser et fiabiliser de manière progressive

3) expertise fine :

objectif :

Homologation selon le RGS (obligation règlementaire : Référentiel Général de Sécurité)

Démarche :

étude de risque

remédiation ou acceptation

Groupe de travail :

travail en sous groupe : membres de l'équipe projet + expert en fonction du thème abordé.

+ autorité métier.

Livrables :

étude de risque + traitement des risques

L'attestation d'homologation

Sommaire :

Disposer d'une Charte commune :

objectif :

Construire une charte applicable aux services numériques UFT.

La faire valider par chaque établissement.

Démarche :

- Inventaire des chartes des établissements.
- Anatomie comparée des chartes existantes en Midi-Pyrénées.
- Rédaction d'une charte par type d'utilisateur (usagers, personnels, personnel affecté au traitement de l'information).
- Validation par les services juridiques de chaque établissement.
- Passage devant les instances.
- Éventuellement annexion au règlement intérieur des établissements volontaires.
- Information des utilisateurs.

Groupe de travail :

membres de l'équipe projet + Cil + juristes (enseignants, master)

Livrables :

Chartes des services numériques de l'UFT.

PSSI de la Recherche : de la clarification à l'harmonisation.

objectif :

Par Unité de recherche ou groupe d'unités,

Construire des points de convergence successifs visant à atteindre une PSSI commune au moins équivalente à la PSSIE

Proposer un roadmap spécifique ou commune par Unité de recherche ou groupe d'unités.

Démarche :

Cartographie des Unités de recherche du site (matrice laboratoire/tutelle).

Recherche éventuellement des profils types et constitution de regroupements.

Choix de 2 regroupements pilotes.

Par regroupement, anatomie comparée des PSSI, clarifier les situations / éliminer les zones de flous

Eliminer les incompatibilités entre les PSSI applicables dans une Unité.

Acceptation de priorités communes.

Itération du processus.

PSSI de la Recherche :

Livrables :

- cartographie des Unités de Recherche.
- liste des regroupements.
- document de comparaison point par point, règle par règle.
- la documentation liée à chaque point de convergence.

Groupe de travail :

- constitué par regroupement. 1 représentant du groupe projet.
- correspondant sécurité des systèmes d'information de chaque Unité.
- au moins 1 rssi d'établissement hôte.

Sommaire :

Animer le réseau des RSSI

Objectif : favoriser la convergence en matière de SSI (idées, pratiques, stratégies)

Éviter les démarches identiques mais isolées.

Démarche : mise à disposition d'un environnement favorable à l'échange et à la mutualisation

mailing list

forum « tout ce que vous voulez savoir sur la PSSI sans jamais oser le demander »

Espace numérique d'échange et de stockage.

Journée (1/2) annuelle de la PSSI de site.

Relai d'informations

Liaison avec la communauté des CIL.

Livrables :

- Documentation commune (tous les travaux, compte rendu, étude, schéma, supports de sensibilisation auprès des utilisateurs, auprès des instances…)
- Inventaire des mesures abordées pour chaque ETB
- Présentations d'exemple de stratégies de mise en œuvre par mesure traitée.
- Présentation de la méthode de sélection des mesures à traiter

Groupe de travail permanent : tout RSSI ou RSSI Adjoint.

Sommaire :

PSSI de Site : le quotidien

Sécuriser et fiabiliser : le scout
- étude ebios
- tests d'intrusions
- audit technique

Disposer d'une Charte commune :
- Démarrage difficile
- Constitution du groupe de travail

Animer le réseau des RSSI :
- difficile tout le monde est occupé
- niveau de maturité différent.
- établissements très differents

PSSI de la Recherche :
- Pas de démarrage officiel
- Liens renforcés avec le cnrs

Conclusion :

La PSSIE connait des débuts difficiles dans les établissements.

La prise en compte de la sécurité dans l'intégralité du cycle de vie de chaque projet
Est loin d'être rentrée dans les mœurs.

Si quelqu'un connait la façon de sensibiliser les utilisateurs, qu'il le dise.

Les RSSI sont tellement occupés par leurs propres problèmes et
sont à des niveaux de préoccupations tellement différents
qu'il est difficile de capitaliser sur les expériences de chacun.

L'application de la PSSI au niveau de la recherche relève du chemin de croix.

Mais, on garde le moral et on avance lentement.

PSSIE : annexes DSI

Les acteurs :

Objet : Mise en œuvre de la politique de sécurité des systèmes d'information de l'État (PSSIE) [circulaire PM N°5725, signée le 17 juillet 2014].

En tant qu'autorité qualifiée en sécurité des systèmes d'information (AQSSI) et conformément à ce qui avait été publié dans le schéma directeur de la sécurité des systèmes d'information en 2005 (réf. 1), vous portez la responsabilité de la mise en œuvre de cette politique au sein de vos entités, assisté d'un responsable de la SSI que vous avez désigné. (cf. PJ.)

L'AQSSI est assisté par un ou plusieurs **responsables de la sécurité des systèmes d'information (RSSI)** qu'il nomme et mandate pour définir et veiller à la bonne réalisation de la politique sécurité qu'il a lui-même impulsée. C'est cette position de rattachement direct auprès de l'AQSSI qui lui confère toute sa légitimité et qui lui permet d'assurer pleinement sa mission. Ils ont un rôle de conseiller technique pour les questions de sécurité des systèmes d'information et peuvent notamment être chargés :

- d'assurer la formation et la sensibilisation des responsables, des informaticiens et des usagers en matière de sécurité des systèmes d'information ;
- de s'assurer de l'application, par les personnels d'exploitation et les utilisateurs, des règles de sécurité prescrites ;
- de veiller à la mise en œuvre des mesures de protection prescrites, d'établir des consignes particulières et de contrôler leur application ;
- de vérifier périodiquement l'installation et le bon fonctionnement des dispositifs de sécurité ;
- de rendre compte de toute anomalie constatée ou de tout incident de sécurité.

http://www.lemonde.fr/actualite-medias/article/2011/08/31/un-hacker-parvient-a-pirater-les-sites-web-de-neuf-prefectures_1565712_3236.html

https://www.undernews.fr/hacking-hacktivisme/un-pirate-met-a-mal-la-securite-du-site-de-la-gendarmerie-nationale.html

https://www.undernews.fr/hacking-hacktivisme/anonymous-piratage-du-cimd-sous-domaine-du-ministere-de-la-defense.html

https://www.undernews.fr/hacking-hacktivisme/des-anonymous-arretes-suite-au-piratage-du-ministere-de-la-justice.html

https://www.industrie-techno.com/un-rancongiciel-contamine-la-messagerie-de-la-direction-generale-de-l-aviation-

http://www.lemondeinformatique.fr/actualites/lire-hack-de-l-elysee-2012-l-ancien-patron-de-la-dgse-se-confie-65876.htmlcivile.42057

https://www.univ-toulouse.fr/sites/default/files/schema_directeur_du_numerique_uftmp.pdf