atilf
ANALYSE ET TRAITEMENT INFORMATIQUE DE LA LANGUE FRANÇAISE

PSSI à l'ATILF

28/04/2022
olivier.servas@atilf.fr






www.atilf.fr

cnrs dépasser les frontières

UNIVERSITÉ DE LORRAINE

PSSI - Introduction

Politique de sécurité des systèmes d'information

- Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/

- **La vie en collectivité** ou dans une communauté (internet, l'entreprise, le travail, une copropriété, la cellule familiale , ..) **nécessite des règles** pour son bon fonctionnement.
- Si **initialement des règles de bonnes pratiques** et de bonnes conduites sont apparues comme la Netiquette [1] pour internet, elles ne **s'avèrent pas suffisantes.**
- **Pour améliorer** cela, dans un contexte délimité nous trouvons les **Chartes**, comme la charte des droits de l'homme [2], ou différents écrit qui consignent des droits ou règles en fonction des intérêts de cette communauté **avec le cas échéant une sanction en application des droits** (Nul n'est censé ignoré la Loi [3]) .
- Pour le Bon fonctionnement de notre Système d'information et dans l'intérêt de nos entités (CNRS, Universités, ...) qui confèrent un caractère stratégique à la **protection de son patrimoine scientifique et technique** nous devons avoir une stratégie ou politique pour organiser cela.

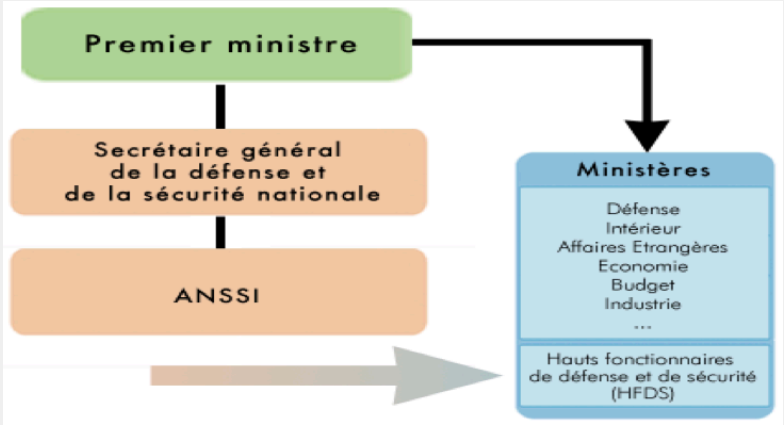
PSSI - Descriptif et SMSI

- **Politique de sécurité des systèmes d'information**
  - Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/
  - Si initialement des mesures techniques étaient mises en œuvre [4], ils manquaient le contexte formel [4.1] et décisionnel [4.2] [5] ?
    - [4] SIARS / UREC
    - [4.1] Groupe CAPSEC - ANSSI (méthode EBIOS)
    - [4.2] Ecole thématique CNRS – INRIA vCARS : vers des communications et des applications Réseaux plus Séecurisées Autrans 2002
    - [5]
  - Avec, la **PSSI**, nous allons prendre en compte des mesures techniques dans le périmètre de l'unité de recherche géré et organisé par un système de management de la sécurité de l'information (**SMSI**) normé par l' ISO/CEI 27001, utilisant la méthode et l'approche de la **Roue de Deming** dans un contexte organisationnel et décisionnel .

PSSI - organisationnel et décisionnel

Politique de sécurité des systèmes d'information

- Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/
- Contexte organisationnel et décisionnel .
  - Fonctionnaire de Défense CNRS
  - Directeur CNRS
  - RSSI CNRS
  - RSSI Délégation Régionale
  - Directeur Unité
  - CSSI



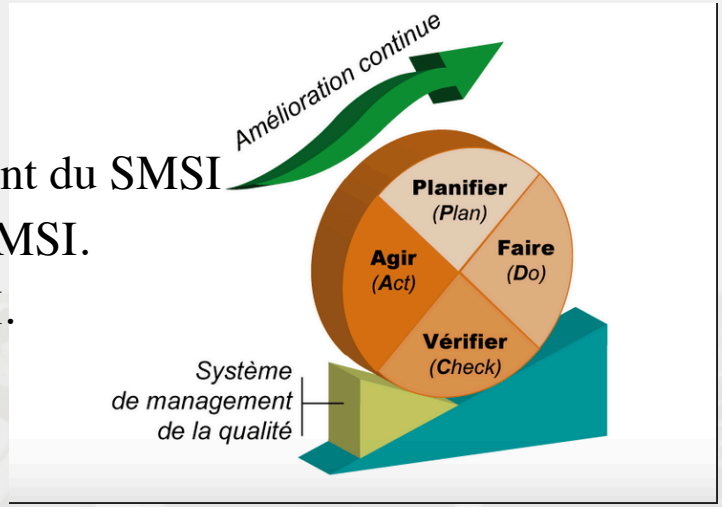
- Sa mise en œuvre, se décline par :
  - Un document qui décrit les enjeux, le contexte et objectifs en fonction des menaces et impact, les principes d'organisation et de mise en œuvre . Ce document est lisible par l'ensemble des utilisateurs : https://intranet.atilf.fr/wp-content/uploads/Missions/CSSI/PSSI-SMSI-ATILFv1.2.5.pdf

PSSI - Descriptif et SMSI

- **Politique de sécurité des systèmes d'information**
  - Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/

- le **SMSI** avec l'approche de la **Roue de Deming** correspond à la mise en œuvre des règles techniques. Ce document ou catalogue technique des règles appliquées n'est accessible que par les ayants droit .
  Planifier, déployer, contrôler et agir. ((Plan), (Do), (Check) (Act)) Le sigle PDCA ne signifie pas : please don't change anything (« prière de ne rien changer ») .

  - **Planifier** : Établissement du SMSI.
  - **Déployer** : Mise en œuvre et fonctionnement du SMSI
  - **Contrôler** : Surveillance et rééxamen du SMSI.
  - **Agir** : Mise à jour et amélioration du SMSI.



PSSI - Descriptif et SMSI

- **Politique de sécurité des systèmes d'information**
  - Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/

- Avec la **norme** ISO-27002 [7] qui propose une **ensemble de règles** (bonnes pratiques sous forme de contrôles nécessaire à la mise en place et au maintien du SMSI) que nous appliquerons en fonction de la sensibilité de l'unité de recherche

- La sécurité du Système d'Information **repose sur trois critères** : (Ces critères peuvent être quantifiés selon une échelle de besoins de sécurité)

  1. **Confidentialité** : « propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés » norme ISO 27001 § 3.3).
  2. **Disponibilité** : « propriété d'être accessible et utilisable à la demande par une entité autorisée » norme ISO 27001 § 3.2).
  3. **Intégrité** : « propriété de protection de l'exactitude et de l'exhaustivité des actifs » norme ISO 27001 § 3.8).

PSSI - références : introduction, descriptif et SMSI

Politique de sécurité des systèmes d'information

- Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/

- [1] netiquette rfc1855 : https://datatracker.ietf.org/doc/html/rfc1855 , https://www.usenet-fr.net/fr-chartes/rfc1855.html
- [2] https://www.un.org/fr/universal-declaration-human-rights/index.html
- [3] https://www.fonction-publique.gouv.fr/statut-general-des-fonctionnaires , https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952/, https://www.cnil.fr/ , https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- [4] SIARS : (Sécurité Informatique pour les Administrateurs Réseaux et Systèmes). Un collectif d'ASR (Administrateurs systèmes et Réseaux) créent une formation (ouvrage collectif et formation de 5 jours) pour les unités de recherches sous la direction de l'UREC (Unité Réseaux du CNRS).
- [5] Initialement le choix normé c'est orienté vers EBIOS : https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ , avec le groupe CAPSEC (Comment Adapter une Politique de Sécurité pour les Entités du CNRS) : https://halshs.archives-ouvertes.fr/halshs-00096276/document , https://www.dgdr.cnrs.fr/bo/2007/01-07/416-bo0107-pb0.htm , retour d'expérience club EBIOS, présentation au JRES 2006.
- https://securite-si.cnrs.fr/pssi/
- [7] https://www.iso.org/fr/standard/54533.html visualisation : https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:fr

Contact :

RSSI CNRS : PIERRON Laetitia laetitia.pierron@cnrs.fr RSSI Université : rssi <rssi@univ-lorraine.fr>

PSSI du CNRS et mise en œuvre à l'ATILF

- **Politique de sécurité des systèmes d'information**
  - Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/
- Elle est constituée:
  - d'une *politique générale* (PGSI)
  - d'une *politique opérationnelle pour les services* (PSSI-O Services)
  - **d'une *politique opérationnelle pour les unités*** (PSSI-O Recherche)
- La PSSI pour les unités de recherche décline les mesures de sécurité qui doivent être mises en œuvre selon trois niveaux par ordre croissant de robustesse:
  - Une étoile pour les unités de sensibilité faible
  - **Deux étoiles pour les unités de sensibilité standard (la majorité)**
  - Trois étoiles pour les unités de sensibilité la plus élevée (principalement les unités impactées par le dispositif "Zone à Régime Restrictif" ou ZRR)
- **.dgdr.cnrs.fr/bo/2007/01-07/416-bo0107-pb0.htm**

PSSI - prérequis

- **Politique de sécurité des systèmes d'information**
  - Vous pouvez consulter ici la PSSI du CNRS dans sa version applicable. https://securite-si.cnrs.fr/pssi/
- La sensibilité d'une unité est directement fonction du type de science qui y est produite. L'arrêté "PPST" [1] (pour "Protection du potentiel scientifique et technique de la Nation") du 3 juillet 2012 définit les disciplines scientifiques protégées et les mesures de protection.

- [1] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000026140136/
- https://www.ssi.gouv.fr/uploads/IMG/pdf/pssie_anssi.pdf
- https://www.dgdr.cnrs.fr/bo/2007/01-07/416-bo0107-pb0.htm

PSSI - ATILF -Mise en œuvre

- **Bilan à l'ATILF**
  - *2005 - 2006 Première rèalisation : ANSSI – groupe EBIOS : Olivier SERVAS (CNRS / **ATILF**), Retour d'expérience de l'utilisation d'EBIOS du groupe de travail CAPSEC 14/03/2006*
  - *2005 - Retour d'expérience PSSI : CAPSEC Jres*
  - *2019 - Presentation de la PSSI : PSSI-SMSI-ATILF v1.2.5*
- **Les incidents :**
  - Utilisateur qui n'effectue pas de sauvegarde , qui ne respecte pas certaines consignes
  - Mise œuvre d'un serveur mail (machine en libre service au centre documentation) : notre unité était considéré comme SPAM
  - Prise en main d'une machine (*Problème d'un développement Perl*) pour attaquer d'autres sites : Centrale électrique USA, Chaine TV Australie
  - Création ISCSI *(avec des restrictions*) et dans la gestion du lien ISCSI perte de luns (pas d'accès aux données)
  - Attaque du serveur Web (*mise à jour Spip en retard*)
  - Vol de mot de passe, utilisation des comptes pour du spam et phising, Vol d'ordinateur
  - Phishing, virus, Cryptoloker

PSSI - - ATILF -Mise en œuvre

- **PSSI : Création d'un groupe de travail :**
  - Rappel des enjeux
  - On définit : le contexte, le périmètre, les besoins, …
  - On décrit : l'organisation et les principes
  - On met en œuvre les règles via un SMSI *(Système de Management de la Sécurité de l'Information)*

- **https://securite-si.cnrs.fr/pssi/**
  - Documents
  - Règles (SMSI)

- ATILF -Mise en œuvre -groupe

Mouture : **PSSI-SMSI-ATILF v1.2.5** du *27/11/2019* réalisée par :

dominique.schloupt@atilf.fr Fonction : ACMO
etienne.petitjean@atilf.fr Fonction : Responsable STR
olivier.servas@atilf.fr Fonction : CSSI pour l'ATILF
sabrina.martin@atilf.fr Fonction : SG
yan.greub@atilf.fr Fonction : Équipe Direction et chercheur

PSSI - ATILF -Mise en œuvre : exemple

- Exemple : https://intranet.atilf.fr/securite-des-systemes-dinformation/

Politique de Sécurité des Systèmes d'Information

De l'ATILF (UMR 7118 – CNRS et Université de Lorraine)

Auteurs : pssi@atilf.fr Version : 1.2.5 Date :07/01/2022

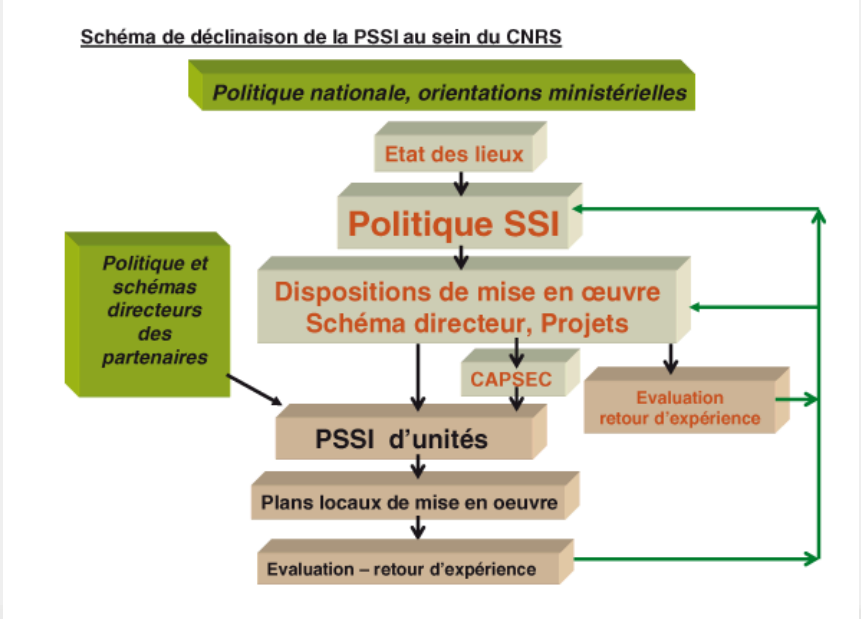
1) Pilotage

2) Mise en œuvre

Chaîne organique et fonctionnelle au CNRS en matière de SSI :

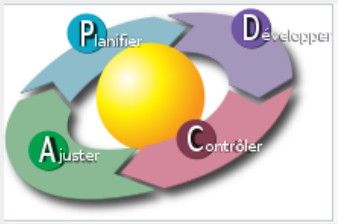
- Chaîne organique
  - DG du CNRS (AQSSI : Autorité Qualifiée pour la sécurité des Systèmes d'Information)
  - FSD (**FSSI** Fonctionnaire de Sécurité des Systèmes d'Information)
  - Institut Scientifique, Délégation Centre-Est, Université de Lorraine, Directeur de l'Unité, CSSI
- Chaîne fonctionnelle spécialisée de la SSI
  - Au niveau national : FSD et RSSI du CNRS
  - Au niveau régional : RSSI de la délégation Centre-Est, RSSI de l'université de Lorraine et coordination régionale de la SSI (CRSSI) et CSSI de l'unité

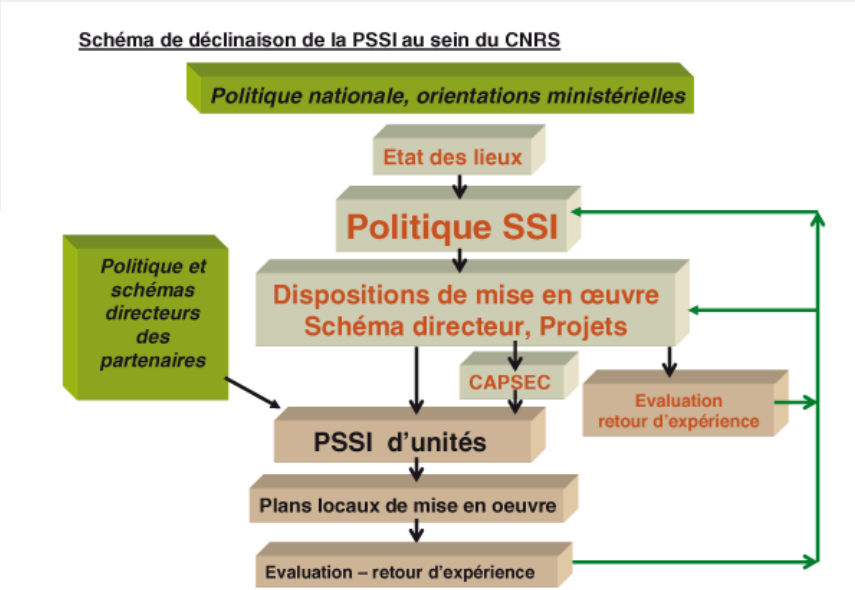
2) Coordination avec les autres tutelles : **Chapitre 5 de l'ISO 27001**



PSSI - ATILF -Mise en œuvre : exemple

- Exemple :





Plan : Analyse, identification et définition

N°	Exigences de la PSSI
1	**1.1 Responsabilité des différents acteurs** Les acteurs intervenant en matière de sécurité des systèmes d'information, au titre d'autorité hiérarchique ou au titre de la chaîne fonctionnelle doivent être informés de leurs responsabilités en matière de SSI. Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve voire à des obligations de secret professionnel. Ils peuvent si nécessaire faire l'objet d'une habilitation au secret de défense.

DO : Mise en oeuvre de la solution

Les acteurs :

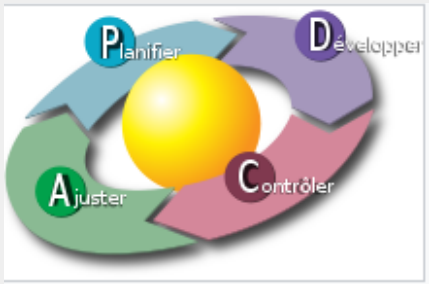
- **ATILF :**
  - Directeur Unité : Alex Boulton
  - CSSI : Olivier SERVAS : olivier.servas@atilf.fr
    - groupe PSSI atilf : pssi@atilf.fr
- **RSSI :**
  - CNRS : Michel Chabanne : Michel.CHABANNE@dsi.cnrs.fr
  - CNRS Centre-EST : Laeticia Pieron : laetitia.pierron@dr6.cnrs.fr
  - Université Lorraine :
    - rssi@univ-lorraine.fr
    - https://numerique.univ-lorraine.fr/gouvernance-du-numerique/securite-des-systemes-dinformation-a-luniversite-de-lorraine
- **Fonctionnaire Défense CNRS**
  - Philippe Gasnot : http://www.cnrs.fr/fr/personne/philippe-gasnot-0
-

l'organisation et du pilotage de la sécurité des SI : https://aresu.dsi.cnrs.fr/IMG/pdf/Organisation_securite_CNRS_-_RSSIC_-_2013_-_3.pdf

---NON Visible aux usagers ---

PSSI

- **Exemple :**



Au niveau des Unités

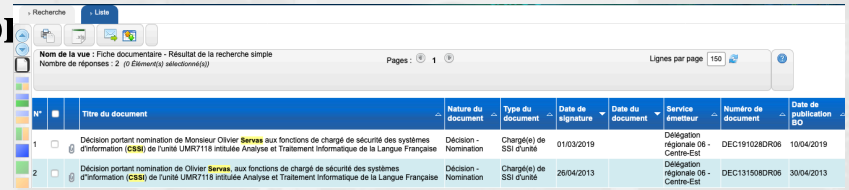
cnrs

P. 8

- Le CSSI https://aresu.dsi.cnrs.fr/spip.php?article120
  - **assiste son DU pour la mise en œuvre de la PSSI du CNRS dans son unité**
  - sensibilise les agents à la SSI
  - met en œuvre les recommandations SSI transmises par le RSSI du CNRS
  - gère les alertes et incidents

NOTA : un CSSI peut intervenir auprès de plusieurs DU avec l'accord du DU de sa structure

- **Check / Vérification -> nomination**
  - https://docutiles.cnrs.fr/



N°	Titre du document	Nature du document	Type du document	Date de signature	Date du document	Service émetteur	Numéro de document	Date de publication BO
1	Décision portant nomination de Monsieur Olivier Servas aux fonctions de chargé de sécurité des systèmes d'information (CSSI) de l'unité UMR7118 intitulée Analyse et Traitement Informatique de la Langue Française	Décision - Nomination	Chargé(e) de SSI d'unité	01/03/2019		Délégation régionale 06 - Centre-Est	DEC191028DR06	10/04/2019
2	Décision portant nomination de Olivier Servas, aux fonctions de chargé de sécurité des systèmes d'information (CSSI) de l'unité UMR7118 intitulée Analyse et Traitement Informatique de la Langue Française	Décision - Nomination	Chargé(e) de SSI d'unité	26/04/2013		Délégation régionale 06 - Centre-Est	DEC131508DR06	30/04/2013

- **Act : Correction**
  - **Pas de texte sur la responsabilité / fonctions CSSI**
  - **Responsabilité du DU**

Questions – Conclusion

- Il existe une PSSI à l'ATILF
  - Groupe PSSI
  - Communication : information liste ATILF [CSSI]
  - Finalisation du SMSI et documentation :
  - Un audit est prévu en Juin 2022
    - https://www.darktrace.com/fr/?uid=004809
  - Prise en compte de la RGPD* dans la conception des projets
  - Prise en compte dans le paradigme DevOp** – avec DevOp sec

* Le règlement général sur la protection des données RGPD : https://www.cnil.fr/fr/comprendre-le-rgpd

** DevOps développement (Dev) et opérations (Ops), permet la coordination et la collaboration des rôles autrefois cloisonnés (développement, opérations informatiques, ingénierie qualité et sécurité)

Questions – Réponses ?