2019-07

Détail sur comparaison PSSI-E / guide d'hygiène

1) Liste des régles de la PSSI-E sans correspondance dans le guide d'hygiène :

ORG-SSI : organisation SSI

ORG-ACT-SSI : identification des acteurs SSI

ORG-RSSI : désignation du responsable SSI

ORG-PIL-PSSIM : définition et pilotage de la PSSI ministérielle

ORG-APP-INSTR : application de l'instruction dans l'entité

ORG-APP-DOCS : formalisation de documents d'application

RH-SSI : charte d'application SSI

RH-CONF : personnels de confiance

RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, prestataires…)

INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information

INT-SSI : intégration de la sécurité dans les projets

INT-TDB : créer un tableau de bord SSI

PHY-CI-HEBERG : convention de service en cas d'hébergement tiers

PHY-CI-ENERGIE : local énergie

PHY-CI-CLIM : climatisation

PHY-CI-INC : lutte contre l'incendie

RES-INTERCOGEO : interconnexion des sites géographiques locaux d'une entité

RES-RESS : cloisonnement des ressources en cas de partage de locaux

RES-INTERNET-SPECIFIQUE : cas particulier des accès spécifiques dans une entité

RES-COUCHBAS : implanter des mécanismes de protection contre les attaques sur les couches basses

RES-ROUTDYN : surveiller les annonces de routage

RES-ROUTDYN-IGP : configurer le protocole IGP de manière sécurisée

RES-ROUTDYN-EGP : sécuriser les sessions EGP

EXP-DOC-CONFIG : documentation des configurations

EXP-SECX-DIST : sécurisation des outils de prise de main à distance

EXP-REAFFECT : réaffectation de matériels informatiques

EXP-IMP-SENS : impression des informations sensibles

EXP-IMP-2 : sécurité des imprimantes et copieurs multifonctions

EXP-CI-LTA : logiciels en Tiers Application

EXP-CI-LTD : logiciels en Tiers Données

EXP-CI-DNS : service de noms de domaine

EXP-CI-DESTR : destruction de support

EXP-CI-TRAC : traçabilité / imputabilité

PDT-SUPPR-PART : suppression des données sur les postes partagés

PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions

PDT-MUL-SECNUM : sécurisation de la fonction de numérisation

PDT-TEL-MINIM : sécuriser la configuration des autocommutateurs

PDT-TEL-DECT : limiter l'utilisation du DECT

DEV-LOG-CRIT : instaurer des critères de développement sécurisé

TI-OPS-SSI : chaînes opérationnelles SSI

PCA-MINIS : définition du plan ministériel de continuité d'activité des Systèmes d'Information (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

PCA-LOCAL : définition du plan local de continuité d'activité des systèmes d'information (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

PCA-SUIVILOCAL : suivi de la mise en œuvre du plan de continuité d'activité local des Systèmes d'Information (PCA des SI) (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

PCA-PROC : mise en œuvre des dispositifs techniques et des procédures opérationnelles (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

PCA-SAUVE : protection de la disponibilité des sauvegardes (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

PCA-PROT : protection de la confidentialité des sauvegardes (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

PCA-EXERC : exercice régulier du plan local de continuité d'activité des systèmes d'information (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

PCA-MISAJOUR : mise à jour du plan local de continuité d'activité des systèmes d'information (excepté le principe de sauvegarde -règle 37 du guide d'hygiène)

CONTR-BILAN-SSI : bilan annuel

Ceci représente 1/4 des 197 règles de la PSSI-E

Les domaines qui sont peu traités sont ceux de l'ORGanisation, et du PCA (Plan de Continuité d'Activité)

Dans les autres domaines, sont absents les règles de sécurité physiques (pourquoi ?) et des points annexes ou demandant une forte expertise ou de détail (ex : sécurité des couches basses du réseau, sécurité des copieurs multi-fonctions)

2) Liste des règles du guide d'hygiène sans correspondance dans la PSSI-E :

Aucune... mais le niveau de détail n'est pas présenté de la même façon : chaque règle du guide d'hygiène se détaille dans son texte lui-même et coïncide souvent avec plusieurs règles de la PSSI-E

3) Conclusions

Le guide d'hygiène et la PSSI-E sont quasi équivalents en terme de règles macroscopiques et vis à vis des niveaux de sécurité nécessaires (rien sur le sujet...)

Le classement des règles est différent : le guide d'hygiène est organisé plutôt par rapport aux besoins de sécurité (ex : "authentifier et contrôler les accès"), la PSSI-E est organisée par rapport aux métiers (décideurs, RSSI, experts SSI, sécurité physique, réseau, exploitation/infrastructure, gestion des postes de travail, développeurs, ...)

Les deux sources ne s'adressent pas au même type d'organisation : le guide d'hygiène est plus accessible (signifiant, compréhensible) et s'adresse à toute entité publique ou privée disposant d'une DSI, alors que la PSSI-E s'adresse en priorité aux administrations centrales (ça se "sent" dans son vocabulaire et dans un certains nombre de règles "fortes")

Les deux sources ne s'adressent pas non plus au même public : le guide d'hygiène est plutôt destiné à la gouvernance et aux fonctionnels, la PSSI-E s'adresse aux spécialistes de chaque métier des SI

4) Liens avec la PSSI de l'Université

Etant donné que les deux sources correspondent assez bien, sont à peu près de la même époque, utilisent à peu près le même vocabulaire, on peut considérer que ce sont deux façon de parler de la même chose.

Dans la PSSI de l'Université on indiquera que le choix d'utiliser l'une ou l'autre des références (ou les deux) sera laissé à l'appréciation de chacun.

à la rigueur, on aurait même pu se contenter de faire référence au guide d'hygiène, d'autant plus que ORGanisaton et CONTrôle, qui manquent dans le guide d'hygiène sont des chapitres à part de la PSSI...

5) Réflexions en vrac

La PSSI-E facilite l'évaluation et le rapport annuel destiné au Ministère (qui l'utilise comme référence). Les RSSI ne peuvent donc échapper à la PSSI-E ;-)