

ÉLABORER UNE PES

La directive 27 précise que tout système d'information dispose d'un document intitulé « procédures d'exploitation de sécurité » (PES¹). Celui-ci est **un prérequis indispensable pour l'homologation du SI** quelle que soit la démarche d'homologation utilisée.

Les PES ont pour objectif de définir :

- Les différents acteurs du SI et les tâches qui leur incombent.
- Les moyens et mesures spécifiques au SI pour répondre au traitement des risques mis en œuvre au préalable.
- Les modalités de MCS.

Les points clés des PES

Les PES doivent être **un document utile et pragmatique**.

Les PES sont **destinées aux acteurs du SI**, c'est-à-dire à l'autorité d'emploi, à l'autorité d'homologation, au centre expert de l'AH, aux responsables en charge de l'exploitation et de la sécurité du SI, aux autorités utilisatrices et aux utilisateurs et à tous les intervenants sur le SI. Les PES doivent donc **leur être accessibles**. Cela implique plusieurs exigences dans l'élaboration du document :



- **Le niveau de confidentialité** apposé aux PES doit permettre son exploitation par les acteurs concernés. Si des informations requièrent un niveau plus important, qui limitent son accessibilité, elles doivent être regroupées dans une ou plusieurs annexes accessibles aux intéressés.
- Les informations doivent être **rapidement disponibles aux acteurs concernés**. Pour cela, les consignes propres à certains acteurs peuvent être regroupées dans des annexes ou des fiches réflexes mises en annexe, le corps ne contenant que celles intéressant l'ensemble des intervenants. Les PES doivent donc être **modulables** ;
- Les informations fournies doivent être **compréhensibles** aux destinataires.

Les PES concernent uniquement les questions de sécurité. Toutes autres considérations ou procédures sont à traiter dans d'autres documents. Elles n'ont pas en effet pour vocation de décrire le SI en question et son emploi.



Les PES définissent des consignes propres au SI. Par conséquent, il est inutile qu'elles rappellent les règles définies de manière générale dans les textes réglementaires à appliquer, et théoriquement connues, sauf pour des points traitant de domaines particuliers et sensibles. Si des consignes sont déjà définies dans une procédure appliquée par les utilisateurs, les PES doivent y faire référence au lieu de rappeler les consignes qu'elle renferme.



Les PES décrivent les mesures dérogatoires aux différentes réglementations. Certaines règles peuvent ne pas être appliquées et, sur autorisation de l'AH, conduire à des dérogations et à des mesures palliatives



Les mesures organisationnelles définies lors de la démarche d'homologation pour traiter des risques ou corriger des vulnérabilités ou failles identifiées doivent être rappelées dans les PES. C'est la raison d'être des PES.

Les PES doivent répondre à **tous les contextes d'emploi du SI**.

¹ Terme employé au pluriel.

Le contenu des PES varie en fonction du SI, de ses enjeux donc de la démarche d'homologation mise en œuvre, et de ses caractéristiques. Une structure globale est donnée en exemple dans cette fiche.



Les PES sont signées par l'autorité d'emploi du SI et validées par l'AH avant la première mise en service du SI.



Les PES évoluent avec le système et son environnement. De nouvelles conditions d'exploitations ou d'organisation, ou encore une modification majeure du SI impliquent une remise en cause des PES et peut nécessiter une remise à jour ainsi qu'une nouvelle validation.



En phase d'exploitation, le RSSI (généralement le RSSI-A) fait évoluer les PES en fonction des modifications apportées au SI, de sa politique d'emploi et de l'environnement dans lequel il évolue. Une évolution majeure du SI pourrait nécessiter une nouvelle validation de l'AH sur avis de son centre d'expert.

Après sa validation, **le document doit être accessible à tous les utilisateurs concernés**. Le RSSI doit diffuser les PES aux OSSI/CSSI des organismes concernés. Ces derniers doivent alors s'assurer que les utilisateurs du SI y accèdent, ou au moins aux informations dont ils ont besoin selon leur profil.

PES globales

Lorsqu'un socle ou un réseau héberge **un ensemble de SI de même type et technologie**, il est possible d'élaborer un seul document PES pour cet ensemble afin de décrire les mesures communes appliquées sur ces SI. À ce corps seront jointes des annexes précisant pour chaque SI les mesures qui lui sont propres.

Méthode d'homologation de déploiement : PES générique et locale

Lorsqu'un SI est déployé sur des sites, des réseaux ou des instances différentes, il est recommandé d'utiliser **une méthode d'homologation dite de déploiement**. Dans ce cadre, sont élaborées deux types de PES :

- les PES génériques pour définir les mesures de sécurité génériques du SI quelle que soit l'instance, le réseau ou le lieu de déploiement.
- les PES locales pour définir les consignes propres à l'instance, au réseau ou au lieu de déploiement.

Les PES locale sont alors accompagnées d'un modèle de certificat de conformité qui énumère l'ensemble des exigences à appliquer sur le SI déployé. Ce certificat peut être structuré en deux partie, l'une destinée aux opérateurs locaux, l'autre aux organismes utilisateurs s'ils sont différents. Les PES locales et les certificats de conformité, une fois renseignés, sont à conserver dans les dossiers de sécurité du site ou de l'organisme. Ils sont retournés au RSSI (généralement RSSI-A) du système concerné qui les détiennent tous.

Les PES génériques définissent les responsabilités et les modalités portant sur les PES locales et le certificat de conformité (remplissage, stockage, diffusion, etc.).



Les PES locales ne sont pas une reprise des PES génériques mais elles en sont **une déclinaison locale**. Elle ne contient que ce qui est nécessaire aux différents utilisateurs.



Les PES locales définissent enfin **les mesures dérogatoires aux mesures définies dans les PES génériques**.



Procédures d'exploitation
de sécurité

Acteurs



RSSI



RCP/PO, Autorité
d'emploi/Autorité cliente



Centre expert SSI de l'AH



Autorité d'homologation (AH)

Structure globale d'une PES

Chaque section doit répondre à des questions portant sur la sécurité numérique.

Une section inutile est à supprimer.

Les rubriques en bleu indiquent celles qui sont nécessairement complétées.

Section		Question à se poser
	Préambule	Quels sont les principaux risques ?
1	Organisation de la sécurité numérique	Qui est responsable? et de quoi ?
2	Textes de référence	Quels sont les textes qui s'appliquent sur le SI et qui intéressent les utilisateurs et les intervenants techniques en termes de sécurité numérique ?
3	Domaine d'application <ul style="list-style-type: none"> - Périmètre fonctionnel, technique - Site - Contexte d'emploi 	Sur quels périmètres s'appliquent les procédures et mesures définies dans la PES ?
4	Protection des données <ul style="list-style-type: none"> - Données métier et techniques - Éléments d'authentification - Données à caractère personnel 	Que faut-il protéger en termes de données ?
5	Sécurité liée au personnel <ul style="list-style-type: none"> - Habilitation - Sensibilisation - Formation 	Quelles sont les personnes ayant accès ? Quelles sont les consignes propres aux personnes ?
6	Gestion de la connaissance du SI <ul style="list-style-type: none"> - Cartographie - Configuration - Documentation 	Comment s'assurer de la connaissance du SI ? Comment peut-on garantir la pérennité de la documentation ?
7	Sécurité physique et environnementale <ul style="list-style-type: none"> - Sécurité des zones - Protection contre les SPC - Circuit approuvé - Sécurité environnemental - Protection des équipements 	Où sont situés les biens ? Comment garantir leur sécurité ? Quels sont les moyens mis en œuvre pour protéger l'environnement du SI (climatisation, énergie, etc.) ? Comment protéger ces biens de manière physique ? Cela comprend les postes, les serveurs, les supports, les biens particuliers...
8	Gestion des accès du SI <ul style="list-style-type: none"> - Gestion des utilisateurs, administrateurs - Droits d'accès aux applications et données - Authentification - Contrôle des accès et des droits 	Comment sont gérés l'accès au SI et les comptes des utilisateurs et administrateurs selon leur profil ? Comment sont assurés les droits d'accès aux applications et aux données ? Quels sont les moyens d'authentification ?

Section		Question à se poser
9	Sécurité des systèmes d'exploitation et des applications	
10	Sécurité du réseau - Administration - Équipements actifs - Cloisonnement et filtrage - Virtualisation - Contrôle des accès au réseau - Segment d'interface et interconnexion	Comment garantir la sécurité du réseau et de ses équipements ? Comment sécuriser l'administration du réseau ? Comment est assurée la protection des dispositifs d'interface ?
11	Sécurité des communications	Comment protéger les communications ?
12	Protection contre les codes malveillants	Quelles sont les mesures mises en place pour réduire le risque associé aux codes malveillants ?
13	Continuité d'activité et résilience - Sauvegarde et restauration système - Sauvegarde et restauration des données - Plan de continuité et de reprise informatique	Comment l'activité peut-elle se poursuivre après un incident majeur ? Quels sont les cas dégradés ? Comment est assurée la sauvegarde des données et du système ? Comment les restaurer ?
14	Maintien en condition de sécurité	Comment est garanti le maintien en condition de sécurité du SI ?
15	Surveillance et gestion des traces - Journalisation - Supervision de sécurité	Comment sont mises en œuvre la supervision du SI, journalisation des logs et leur exploitation ?
17	Gestion des incidents	Comment sont gérés les incidents ?

En annexe :

- la liste des points de contact ;
- la stratégie de MCS (si nécessaire) ;
- une fiche de procédure d'exploitation de sécurité pour l'utilisateur ;
- la liste des zones et locaux sensibles, etc.