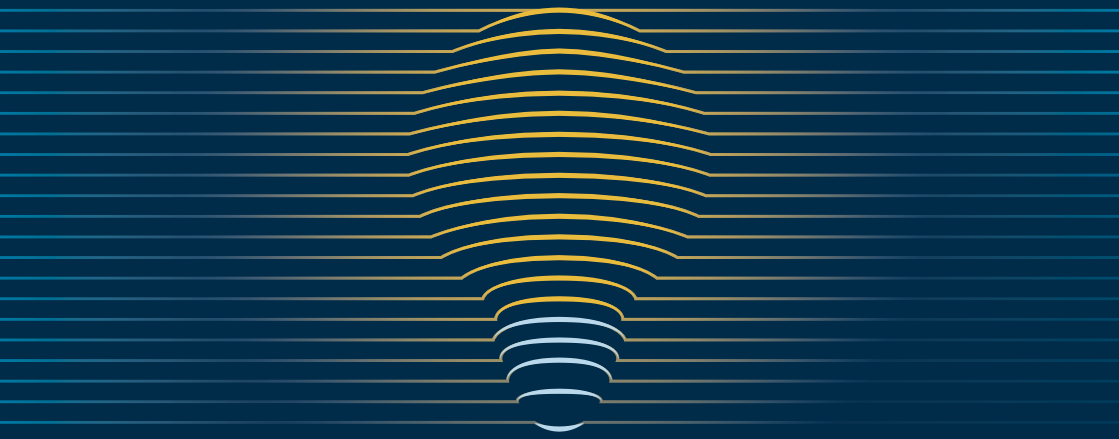
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN

PROTECTION NUMÉRIQUE DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION

GUIDE MÉTHODOLOGIQUE



AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

ÉDITO

Placée sous la responsabilité du secrétariat général de la défense et de la sécurité nationale (SGDSN), la protection du potentiel scientifique et technique de la nation (PPST) a pour objectif de lutter contre les tentatives de captation ou de détournement des savoirs, savoir-faire et technologies sensibles ayant trait aux intérêts fondamentaux de notre pays. Elle s'appuie notamment sur la création dans les établissements concernés – universités, laboratoires, entreprises – de zones à régime restrictif (ZRR) dont l'accès est contrôlé.

La PPST ne saurait toutefois se résumer à la nécessaire protection physique de documents ou à la limitation de la circulation dans les ZRR. À l'heure où la numérisation de nos sociétés s'accompagne d'un accroissement des risques d'attaques cyber, elle doit prendre en compte également les enjeux relatifs à la sécurité des systèmes d'information.

Sur l'impulsion du haut fonctionnaire de sécurité et de défense du ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation, le présent guide a été élaboré conjointement par l'agence nationale de sécurité des systèmes d'information (ANSSI) et la direction des affaires internationales, stratégiques et technologiques du SGDSN, afin de sensibiliser les personnels travaillant dans des ZRR à cette dimension désormais incontournable de la protection de notre potentiel scientifique et technique.

Ce document rappelle, en premier lieu, l'importance primordiale d'un certain nombre de règles élémentaires en matière d'hygiène d'informatique, pour réduire les risques liés aux usages du numérique.

Il expose ensuite les notions fondamentales, les bases juridiques et les principaux instruments des politiques de sécurité des systèmes d'information (SSI) déployées dans le cadre de la PPST.

Ce guide se veut aussi pratique et opérationnel que possible. Il vous permettra de protéger plus efficacement vos recherches, vos découvertes, et avec elles les moyens qu'amène la reconnaissance du succès !

Claire Landais

Secrétaire générale de la Défense et de la Sécurité nationale

TABLE DES MATIÈRES

PRÉAMBULE

PRÉSENTATION

Contexte

Face aux nombreuses vulnérabilités induites par une dépendance de plus en plus grande aux systèmes d'informations, il apparaît nécessaire de préciser le cadre selon lequel il convient de protéger, au sens de la **protection du potentiel scientifique et technique de la nation** (PPST), les données numériques des **zones à régime restrictif** (ZRR).

Pour rappel, le dispositif de protection du potentiel scientifique et technique de la nation a pour but de protéger, au sein des établissements publics et privés, les savoirs et savoir-faire stratégiques ainsi que les technologies sensibles qu'ils détiennent. Cette réglementation offre une protection juridique et administrative fondée sur le contrôle des accès aux informations stratégiques ou sensibles détenues. La protection contre l'espionnage technologique est l'objectif premier du dispositif.

Les locaux abritant des activités de recherche ou de production stratégiques reçoivent le statut de zones protégées, qualifiées de **ZRR**. Il peut s'agir notamment de bureaux, de laboratoires ou de plates-formes expérimentales. Ce statut permet légalement d'en interdire l'accès et prévoit des poursuites pénales en cas de tentative de captation ou d'intrusion sans autorisation préalable.

Objectif

L'objectif de ce guide est d'accompagner la prise en compte des besoins spécifiques de **protection d'informations numériques sensibles** au titre de la **protection du potentiel scientifique et technique de la nation**.

Destinataires

Ce guide s'adresse en priorité aux **responsables de la sécurité des systèmes d'information (RSSI)** en charge de la protection informatique des zones à régime restrictif ainsi qu'à **toute personne en charge de la protection globale des ZRR.**

Il s'agit d'un guide méthodologique présentant les étapes à suivre pour sécuriser les systèmes d'information d'une ZRR.

DÉFINITIONS ET APPLICATIONS

Les définitions présentées ci-dessous n'ont pas une valeur réglementaire. Elles ont pour objet de faciliter la lecture et la compréhension de ce guide et des notions techniques qui y sont évoquées.

Information à régime restrictif (IRR)

Un ensemble d'informations, quel que soit son support, est qualifié de « sensible », au sens de la PPST, lorsque sa divulgation à des tiers non autorisés aurait un impact significatif au regard des risques ayant justifié la création de la ZRR. Les IRR sont donc par principe sensibles.

À titre d'exemple, il peut s'agir de travaux de recherche, de données techniques provenant d'équipements, d'images ou autres.

Les IRR sont sensibles : elles sont soumises à l'instruction interministérielle n° 901 et doivent à ce titre être marquées en fonction de l'échelle de sensibilité adoptée localement.

Marquage des informations à régime restrictif

L'objet du marquage est d'apporter la connaissance du niveau de sensibilité des informations à une personne les manipulant. Il peut être fait classiquement sur les documents, par exemple à l'aide d'encadrés rouges.

Dans le cas des fichiers informatiques, le marquage peut être fait dans le nom du fichier ou du répertoire voire sur le support physique, par exemple

à l'aide d'une étiquette sur une clé USB. Cela permet notamment de renseigner l'utilisateur sur le niveau de sensibilité avant toutes manipulations telles que l'ouverture ou la copie.

> ***Note :*** *Le marquage des IRR doit être explicite afin qu'une personne les manipulant ne puisse en ignorer la sensibilité et qu'elle sache quelles précautions prendre en fonction du niveau de sensibilité.*

En cas d'échange avec d'autres entités, il convient de s'assurer que le receveur a bien connaissance des précautions requises par le niveau de sensibilité déclaré. Il doit notamment savoir s'il peut, ou non, diffuser ou retransmettre les IRR considérées.

Système d'information à régime restrictif (SIRR)

Un système d'information donnant accès directement à des IRR est nommé « système d'information à régime restrictif ». Il intègre *de facto* tous supports et équipements électroniques stockant ou véhiculant un ensemble d'IRR non sécurisé. À titre d'exemple, il peut s'agir d'un ordinateur portable, d'une clé USB, d'un serveur de fichiers, etc.

Toutefois, les systèmes numériques et les systèmes d'information concourant à la sécurité physique (caméra, contrôle d'accès et d'intrusion, détection d'incendie, SCADA, etc.) ne sont pas des SIRR.

> ***Note :*** *Un SI contenant ou véhiculant des IRR sécurisées n'est pas pour autant un SIRR. Échanger par courriel des IRR chiffrées n'implique pas que les serveurs de messagerie soient des SIRR.*

Les SIRR sont soumis à l'instruction interministérielle n° 901.

Identification des informations à régime restrictif

Si le processus d'identification des IRR n'est pas réalisé, alors la totalité des informations de la ZRR et des systèmes qui les hébergent sont respectivement considérées comme IRR et SIRR et doivent respecter les mesures de sécurité correspondantes.

Les données sensibles, non classifiées, qui ont justifié un classement en ZRR de l'établissement et qui relèvent des spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs, sont des IRR de niveau Diffusion Restreinte, conformément à l'instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles.

Accès aux informations à régime restrictif

Conformément à la terminologie employée dans la PPST, un accès à une IRR ou à un SIRR, quelle que soit la localisation de l'accédant, est considéré comme un accès virtuel à la ZRR. Cet accès nécessite un avis ministériel, comme s'il s'agissait d'un accès physique.

La possibilité de donner accès ou de transmettre une information provenant d'un SIRR à un tiers non autorisé doit être évaluée en tenant compte des critères suivants :

- **si l'information est une IRR**, un avis ministériel est requis comme pour un accès physique (un élément d'information isolé provenant d'un SIRR n'est pas forcément une IRR) ;
- **si l'information n'est pas une IRR**, un accord de confidentialité peut toutefois être nécessaire (ex. : accord commercial ou échanges internationaux) ;
- **si l'information n'est pas confidentielle**, ou ne l'est plus suite à une réévaluation, elle peut parfois être rendue publique, notamment dans le cadre de la publication d'une thèse par exemple.

CONTEXTE RÉGLEMENTAIRE

Afin d'élever le niveau de sécurité des systèmes d'information, les mesures d'hygiène numérique doivent être complétées par des normes et réglementations adaptées au type d'organisme concerné et à son activité.

Les fondements juridiques de la PPST sont présentés dans la partie *Références* du présent guide (p. 39).

Dans le cadre de la PPST, le référentiel réglementaire suivant s'applique pour tous les organismes publics et privés :

1 / L'instruction interministérielle n° 901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles.

L'instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles fixe les règles de protection appropriée contre toutes les menaces, qu'elles soient d'origine humaine ou non.

Ces règles sont divisées en deux parties :

- **une partie relative à la protection des SI sensibles** qui concerne toute entité publique ou privée soumise à la réglementation PPST ;
- **une partie relative à la protection des SI Diffusion Restreinte** qui décrit des exigences complémentaires. Dans le contexte de la PPST, ces exigences ne concernent que les systèmes d'information sensibles, non classifiés, des entités qui traitent d'informations relatives aux spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs[1].

2 / La circulaire nº 3415/SGDSN/AIST/PPST du 7 novembre 2012

Conformément à la circulaire nº 3415/SGDSN/AIST/PPST du 7 novembre 2012, « *les services, établissements ou entreprises qui comprennent une ou plusieurs ZRR se dotent d'une* ***politique de sécurité des systèmes d'information (PSSI)*** *et la mettent en œuvre. La PSSI s'intègre dans une politique de sécurité interne (PSI) qui doit être cohérente avec le dispositif de PPST. Dans ce cadre, le chef d'établissement ou d'entreprise désigne un responsable de la sécurité des systèmes d'information (RSSI).* »

Un établissement qui abrite une zone à régime restrictif doit en premier lieu rédiger une PSSI et nommer un RSSI. La PSSI définie par l'organisme doit être conforme aux règles définies par l'ANSSI relatives aux informations sensibles telles que définies dans l'instruction interministérielle nº 901. L'annexe du présent guide définit et précise le contenu d'une PSSI.

À noter que la circulaire stipule également que « *la PSSI organise le signalement des incidents majeurs au ministre chargé d'exercer la tutelle, ou à celui qui a déterminé le besoin de protection, ainsi qu'à l'ANSSI si l'incident est susceptible de révéler une compromission du système d'information. Son articulation avec la protection du potentiel scientifique et technique relève de la responsabilité du chef de service, d'établissement ou d'entreprise.* » Ce point particulier lié à la gestion des incidents sera abordé ultérieurement dans ce guide.

3 / La politique de sécurité des systèmes d'information de l'État (PSSIE), publiée dans la circulaire du 17 juillet 2014

> ***Note :*** *S'applique uniquement aux systèmes d'information des administrations de l'État.*

Dans le cas où les ZRR considérées regroupent des systèmes d'information des administrations de l'État (ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'État et autorités administratives indépendantes), la PSSI doit également être conforme aux exigences définies dans la Politique de sécurité des systèmes d'information de l'État (PSSIE).

Pour les organismes privés, la PSSIE constitue un guide de bonnes pratiques pour mettre en place leur propre politique de sécurité des systèmes d'information.

AVANT D'ALLER PLUS LOIN

L'augmentation du nombre de tentatives d'atteintes au potentiel scientifique et technique de la nation et la sophistication croissante de la menace cyber rendent nécessaire la mise en place de mesures d'hygiène numérique. Elles constituent un socle de base en matière de sécurité des systèmes d'information.

Ces mesures génériques, applicables pour la plupart des systèmes d'information, sont décrites dans le *Guide d'hygiène informatique – renforcer la sécurité de son système d'information en 42 mesures*, publié par l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Le guide présente des principes de base qui concernent :

- la sensibilisation et la formation des utilisateurs ;
- la connaissance du système d'information ;
- l'authentification et le contrôle des accès ;
- la sécurisation des postes de travail ;
- la sécurisation du réseau ;
- la sécurisation de l'administration ;
- la gestion du nomadisme ;
- le maintien à jour du système d'information ;
- la supervision, l'audit et la réaction face à des incidents de sécurité.

L'application de l'ensemble de ces mesures permet de prendre en compte les risques de bas niveau — en particulier les risques non intentionnels — et de limiter l'impact des attaques cyber dites « à large spectre » (ex. : courriels d'hameçonnage, etc.).

En cas d'incompatibilité opérationnelle avec certaines des règles d'hygiène informatique, il est nécessaire, dans le cadre de la démarche d'homologation, de mener une analyse de risques, de proposer des contre-mesures (organisationnelles ou techniques) pour les limiter puis de faire valider les éventuels risques résiduels par la direction.

Pour aller plus loin :

- *Guide d'hygiène informatique : Renforcer la sécurité de son système d'information en 42 mesures*[2] - Guide ANSSI
- Le site de l'ANSSI[3] met à disposition de nombreux guides techniques permettant d'approfondir chaque thématique abordée et d'accompagner les opérateurs dans leur démarche de sécurisation globale des systèmes d'information.

MESURES DE SÉCURISATION DES SYSTÈMES D'INFORMATION COMMUNES À TOUTES LES ZONES À RÉGIME RESTRICTIF

Face à l'évolution des menaces et à l'interconnexion des systèmes d'information, une approche strictement technique ne suffit plus à leur sécurisation.

La démarche de sécurisation consiste à mettre en place une organisation de gestion des risques inscrite dans un processus d'amélioration continue de la sécurité. Cette démarche est pilotée par une gouvernance SSI forte où les responsabilités de chacun sont bien définies.

Le pilotage de la SSI au sein de l'organisme, en particulier pour la protection des informations sensibles, s'effectue en concertation entre les acteurs des systèmes d'informations et de la protection du potentiel scientifique et technique.

RÔLES ET RESPONSABILITÉS DES AQSSI ET DES RSSI

Le responsable de la politique de sécurisation des SI, nommé « autorité qualifiée en sécurité des systèmes d'information » (AQSSI), est le chef d'établissement. Il s'appuie, avec le responsable de la ZRR, sur une chaîne opérationnelle SSI pour définir et mettre en œuvre une PSSI adaptée à l'organisme et aux éléments constitutifs du potentiel scientifique et technique des ZRR concernées. L'AQSSI désigne un responsable de la SSI.

Les mesures de sécurité, leur respect par les utilisateurs et les administrateurs et leur efficacité sont régulièrement contrôlés, notamment sur demande de l'AQSSI ou du haut fonctionnaire de défense et de sécurité (HFDS).

L'AQSSI arbitre les décisions relatives à la sécurité de ces systèmes d'information et s'engage au respect des réglementations. Conseillé par le RSSI, il arbitre la stratégie SSI et identifie les moyens associés. Le RSSI, son conseiller, est responsable de la mise en œuvre opérationnelle des mesures de sécurité.

En cas d'incident et en fonction de la gravité, le RSSI alerte l'AQSSI, le RSSI national et le fonctionnaire de la sécurité des systèmes d'information (FSSI) du service du HFDS de son ministère de tutelle. Le FSSI est en liaison avec l'agence nationale de la sécurité des systèmes d'information (ANSSI).

DÉFENSE EN PROFONDEUR DES SIRR

La sécurisation des SIRR passe par des mesures de défense en profondeur s'inscrivant dans une démarche d'amélioration continue pilotée par une gouvernance SSI forte. La défense en profondeur des ZRR passe par la définition et la mise en œuvre d'une **politique de protection, de défense et de résilience.**

1 / Protection des SIRR

Pour aller plus loin :

- *La défense en profondeur appliquée aux systèmes d'information* — Guide ANSSI[4]

L'ensemble des mesures de protection doit permettre de garantir que **les IRR ne puissent être manipulées que par des personnes autorisées à accéder à la ZRR** les abritant, et cela à chaque instant quel que soit le lieu où elles se trouvent (serveur, ordinateur portable, messagerie électronique, etc.).

Les mesures de protection des ZRR doivent répondre aux objectifs de confidentialité et d'intégrité des IRR. Elles peuvent être d'ordre technique, organisationnel, logique ou physique.

Exemples de scénarii de risque :

■ *Un outil malveillant introduit dans le SIRR modifie de manière aléatoire les résultats de recherche.*

■ *Une clé USB, connectée au SIRR par un prestataire corrompu exfiltre des informations exclusives.*

Parmi les mesures permettant de répondre aux besoins principaux de sécurité des IRR, nous pouvons citer :

- séparer physiquement ou à défaut, logiquement, le réseau d'expérimentation du réseau de saisie ;
- écraser, par un logiciel *ad hoc*, les données présentes sur un poste de travail dans le cas d'une réattribution de matériel ;
- supprimer les droits d'accès aux systèmes d'information dès la fin de la période d'emploi ou au terme du contrat d'un utilisateur (fin de stage, fin de prestation, etc.).

Les autres besoins de sécurité des IRR peuvent notamment être couverts par les mesures suivantes :

- le chiffrement des IRR à l'aide de solutions qualifiées[5]. Des IRR chiffrées, donc sécurisées, peuvent être manipulées comme tout autre fichier. En effet, le chiffrement n'empêche pas l'accès aux fichiers et leur manipulation (la copie par exemple) mais les rend illisibles pour les personnes n'ayant pas la connaissance de l'élément secret ;
- la mise en place d'un contrôle d'accès avec chiffrement des répertoires partagés sur un serveur mutualisé à l'aide d'outils qualifiés ;
- la segmentation stricte des droits d'accès selon le principe du besoin d'en connaître ;
- la sécurisation du réseau Wi-Fi ;
- l'interconnexion maîtrisée des SIRR avec d'autres réseaux de sensibilité différente (maîtrise des flux, journalisation, etc.) ;
- l'installation d'une machine ou un réseau local à la ZRR, accessible uniquement depuis les locaux soumis au contrôle d'accès ou depuis un SIRR nomade utilisant un VPN IPsec ;
- le chiffrement complet du disque dur d'un ordinateur portable contenant des IRR ;
- l'installation d'une baie sécurisée dans un centre de données partagé, dont la clé est détenue par le responsable de la ZRR, et dont les échanges avec la ZRR sont chiffrés ;
- la gestion des prestataires de service.

Pour aller plus loin :

- *Maîtriser les risques de l'infogérance*[6] – Guide ANSSI ;
- *Recommandations de sécurité relatives aux réseaux Wi-Fi* – Guide technique ANSSI[7] ;
- Liste des produits qualifiés[8] ;
- Liste des prestataires qualifiés :
  - Prestataires d'audit de la sécurité des systèmes d'information (PASSI)[9] ;
  - Prestataires de détection d'incidents de sécurité (PDIS)[10] ;
  - Prestataires de réponse aux incidents de sécurité (PRIS)[11].

Un prestataire de service ayant obtenu un avis favorable à une demande d'accès dans une ZRR peut exercer son activité habituelle dans n'importe quelle ZRR, dans les conditions fixées par un contrat de prestation de service, car il est réputé avoir obtenu un avis favorable.

L'efficacité des mesures de protection des IRR doit être régulièrement contrôlée, notamment au travers d'audits techniques et organisationnels.

2 / Défense des SIRR

Les mesures de défense des ZRR doivent permettre de garantir que **l'organisme détecte et réagisse dans les meilleurs délais en cas d'attaque de son SIRR.**

Comme stipulé précédemment, la PSSI de l'établissement doit organiser le signalement des incidents majeurs au service du HFDS du ministre, ainsi qu'à l'ANSSI si l'incident est susceptible de révéler une compromission du système d'information.

Ainsi, l'organisme doit définir et mettre en œuvre une politique de gestion des traces d'accès et de fonctionnement des SIRR permettant la détection et la résolution des incidents. Les incidents de sécurité impliquant des IRR ou des SIRR sont remontés sans délai au RSSI et au responsable de la sécurité selon une organisation locale prédéfinie et régulièrement testée. En fonction de sa gravité, l'incident est remonté sans délai au HFDS, au fonctionnaire de la sécurité des systèmes d'information, qui pourra le faire suivre à l'ANSSI.

De plus, il est rappelé aux responsables des ZRR l'importance de déposer plainte auprès des services de sécurité locaux compétents (police ou gendarmerie) en cas d'incident de sécurité de type intrusion ou vol de données.

Pour aller plus loin :

- *En cas d'incident* – Site internet de l'ANSSI[12]

3 / Résilience des SIRR

La définition et la mise en place de mesures de résilience des ZRR doit permettre à **l'organisme de poursuivre son activité opérationnelle malgré la survenance d'une attaque.**

> ***Exemple de scénario de risque :***
> ■ *Un outil malveillant (rançongiciel) chiffre l'intégralité des données du SIRR et l'attaquant demande une rançon à l'organisme afin de déchiffrer les données.*

Afin de répondre au besoin de disponibilité des IRR, il est indispensable de définir et mettre en place une politique de sauvegarde des SIRR qui les supportent.

Pour éviter le risque de corruption de la sauvegarde, elle doit être réalisée sur un support séparé du système d'information et conservé dans un état déconnecté.

La sauvegarde déconnectée doit être stockée dans un lieu sécurisé. Ce lieu doit être pris en compte dans l'étude de sûreté et de sécurité. Il doit respecter au minimum les mesures les plus élevées prises pour le SI support des IRR.

La durée de rétention et la fréquence de sauvegarde doivent être adaptées au risque. Par exemple : une sauvegarde sur bandes, stockées dans un coffre ignifugé, localisé dans un autre bâtiment qui peut être une zone à régime restrictif.

Les sauvegardes doivent être testées régulièrement afin de s'assurer de la bonne restauration des données sauvegardées.

MESURES DE SÉCURISATION PARTICULIÈRES À CHAQUE ZONE À RÉGIME RESTRICTIF

ÉTUDE DES RISQUES PARTICULIERS AU SYSTÈME D'INFORMATION À RÉGIME RESTRICTIF

En premier lieu, il convient de réaliser une analyse des risques du SIRR. La plus-value de cette analyse de risques repose sur la prise en compte des risques spécifiques à l'organisme ou au système étudié. Aussi, un organisme ayant un niveau de maturité suffisant consacrera ses efforts aux risques non traités par les mesures d'hygiène et le cadre réglementaire. Cette démarche doit permettre de prendre en compte les spécificités de chaque SI qui diffèrent selon les organismes.

Dans le cadre de la ZRR, il est important d'effectuer une analyse de risques ciblant notamment les impacts liés spécifiquement aux risques PPST, à savoir l'analyse des conséquences en cas d'incident tels la perte d'exclusivité de découvertes, les conséquences pour les partenaires industriels, le non-respect du secret médical, la fuite de données personnelles, la rupture de contrat, etc.

Cette analyse des risques doit débuter en effectuant une cartographie spécifique qui identifie à la fois les IRR et les SI supports.

Au terme de la réalisation de l'analyse de risques, des mesures de sécurisation complémentaires sont définies, au besoin, pour la ZRR concernée. Ces mesures de sécurisation s'articulent selon la démarche de défense en profondeur dans les politiques de protection, défense et résilience. Elles s'inscrivent dans une démarche d'amélioration continue à la ZRR concernée. L'étude des risques est validée par une homologation qui consiste en une acceptation formelle des risques résiduels par l'AQSSI. L'homologation est nécessaire à la mise en service du SIRR ou à la continuation de l'activité du SIRR.

Pour aller plus loin :

- *L'homologation de sécurité en neuf étapes simples* — Guide ANSSI[13]
- Méthode EBIOS[14]

AMÉLIORATION CONTINUE DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

Les menaces numériques évoluent en permanence. Aussi, il est indispensable que la sécurité du SI évolue en conséquence en suivant un processus d'amélioration continue.

La mise en place de mesures de sécurité doit donc être évaluée avec des indicateurs de performance visant à mesurer l'efficacité de la politique de sécurité à un instant t. L'évaluation de la performance doit être couplée à une veille des menaces numériques et des analyses des incidents qui impactent le système.

Ces éléments permettent l'évolution de la politique de sécurité du SI à moyen et long terme via la définition d'un plan d'action. L'objectif est de disposer d'une politique de sécurité cohérente vis-à-vis des menaces et des risques qu'elles font peser sur le système d'information.

ANNEXE :
LA POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

QU'EST-CE QU'UNE PSSI ?

La PSSI est le document de référence en matière de sécurité des systèmes d'information (SSI) qui reflète la vision stratégique de la direction de l'établissement en la matière. Sa signature par le chef de l'établissement garantit que son contenu traduit le niveau d'importance accordé à la SSI.

Une PSSI s'adresse à l'ensemble du personnel de l'établissement sans exception (membres de la direction, informaticiens, personnels administratifs, techniques et commerciaux, ouvriers secrétaires) ainsi qu'aux intervenants tiers (fournisseurs, clients, sous-traitants, opérateurs de maintenance, etc.).

La PSSI est évolutive car elle doit prendre en compte les transformations du contexte de l'établissement (changement d'organisation, évolution des activités, etc.) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux).

À QUI ET À QUOI PEUT SERVIR UNE PSSI ?

La PSSI sert :

1. à la direction, en fixant le cadre réglementaire qui permettra au personnel de travailler dans les conditions de sécurité nécessaires et indispensables à la pérennité de l'établissement ;
2. aux professionnels de la sécurité/sûreté, qui, dans le cadre d'une bonne gouvernance qu'elle permet, voient définies leurs fonctions et leurs missions ;
3. aux informaticiens qui doivent prendre des décisions au quotidien et qui ont besoin de référentiels ;
4. à l'ensemble du personnel (toutes catégories confondues), pour faire valoir ses droits et connaître ses devoirs.

La PSSI est également un **instrument de sensibilisation et de communication.** Une fois validée, la PSSI doit être diffusée à l'ensemble du personnel (utilisateurs, sous-traitants, prestataires, etc.) pour que chaque utilisateur adhère aux principes de sécurité de l'établissement et adopte les bons réflexes au quotidien dans le but de réduire les incidents de sécurité et les coûts associés.

La diffusion de la PSSI permet la **responsabilisation** de chaque utilisateur, ce dernier s'engageant personnellement dans la démarche d'amélioration continue de la SSI (charte informatique, attribution d'objectifs liés à la sécurité, etc.).

QUEL EST LE CONTENU DE LA PSSI ?

La PSSI fixe des objectifs en matière :

1. d'organisation et de gouvernance

Par exemple : identifier et désigner les acteurs et les responsables SSI.

2. de ressources humaines

Par exemple : sensibiliser, rédiger une charte d'application SSI et gérer les arrivées et départs du personnel.

3. de gestion des biens, de la sécurité du poste de travail et du réseau

Par exemple : élaborer une cartographie des SIRR.

4. d'intégration de la SSI dans le cycle de vie des systèmes d'information

Par exemple : apprécier, traiter et communiquer sur les risques relatifs à la sécurité des systèmes d'information ainsi que gérer dynamiquement les mesures de protection, tout au long de la vie du système d'information.

5. de sécurité physique

Par exemple : assurer la sécurité physique des locaux abritant les systèmes d'information et des centres serveurs.

6. de sécurité des réseaux

Par exemple : établir une cartographie des réseaux et des interconnexions de l'entité.

7. d'architecture des systèmes d'information

Par exemple : mettre en place une architecture sécurisée des centres informatiques.

8. d'exploitation des systèmes d'information

Par exemple : surveiller et configurer les ressources informatiques ainsi que gérer les autorisations et contrôles d'accès logiques.

9. de sécurité du poste de travail

Par exemple : durcir les configurations des postes de travail et sécuriser la téléphonie.

10. de sécurité du développement des systèmes

Par exemple : prendre en compte la sécurité dans le développement des systèmes d'information, des logiciels et sécuriser les applications à risques.

11. de traitement des incidents

Par exemple : partager l'information (alertes, incidents) dans le respect des règles de prudence.

12. de continuité d'activité

Par exemple : se doter de plans de continuité d'activité et les tester.

13. de conformité, audit, inspection, contrôle

Par exemple : effectuer des contrôles et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

Pour aller plus loin :

- *PSSI – Guide d'élaboration de politiques de sécurité des systèmes d'information* — Guide ANSSI[15]

RÉFÉRENCES

TEXTES RÉGLEMENTAIRES

Protection du potentiel scientifique et technique de la nation

- Article 410-1 du Code pénal

- Décret nº 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation

- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation

- Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation nº 3415/SGDSN/AIST/PST du 7 novembre 2012

Sécurité des systèmes d'information

- Instruction interministérielle relative à la protection des systèmes d'information sensibles nº 901/SGDSN/ANSSI

- Circulaire du Premier ministre nº 5725/SG du 17 juillet 2014 portant politique de sécurité des systèmes d'information de l'État

NOTES

1. En effet, tous les systèmes d'information dans une ZRR ne sont pas concernés par cette partie de l'instruction interministérielle n° 901, par exemple les serveurs mail

2. ANSSI, *Guide d'hygiène informatique* [en ligne], 2017 (v.2), https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

3. Pour en savoir plus, rendez-vous sur https://www.ssi.gouv.fr/

4. ANSSI, *La défense en profondeur appliquée aux systèmes d'information* [en ligne], 2011, https://www.ssi.gouv.fr/guide/la-defense-en-profondeur-appliquee-aux-systemes-dinformation/

5. ANSSI, *La qualification* [en ligne], 2018, https://www.ssi.gouv.fr/administration/qualifications/

6. ANSSI, *Externalisation des systèmes d'information* [en ligne], 2010, https://www.ssi.gouv.fr/externalisation/

7. ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi* [en ligne], 2013, https://www.ssi.gouv.fr/nt-wifi/

8. ANSSI, *Produits de sécurité qualifiés* [en ligne], 2018, https://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/

9. ANSSI, *Prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés* [en ligne], 2018, https://www.ssi.gouv.fr/passi/

10. ANSSI, *Prestataires de détection d'incidents de sécurité PDIS* [en ligne], 2018, https://www.ssi.gouv.fr/pdis/

11. ANSSI, *Prestataires de réponse aux incidents de sécurité PRIS* [en ligne], 2018, https://www.ssi.gouv.fr/pris/

12. ANSSI, *En cas d'incident* [en ligne], https://www.ssi.gouv.fr/en-cas-dincident/

13. ANSSI, *L'homologation de sécurité en neuf étapes simples* [en ligne], 2014, https://www.ssi.gouv.fr/guide-homologation-securite/

14. ANSSI, *EBIOS — Expression des Besoins et Identification des Objectifs de Sécurité* [en ligne], 2010, https://www.ssi.gouv.fr/ebios/

15. ANSSI, *PSSI — Guide d'élaboration de politiques de sécurité des systèmes d'information* [en ligne], 2004, https://www.ssi.gouv.fr/pssi/

ANSSI-PA-049

Version 1.0 - Avril 2018

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr - communication@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN