

${N°rue} rue ${RueAvenue}

${Zip code} ${Ville}

${Pays}

Tél : ${N°tel}

${LienSite}

${Titre}

*Table des matières* :

[Activité 1 (Cadrage et socle de sécurité) 1](#_Toc71626256)

[Activité 1.a (Cadrer l’étude) 1](#_Toc71626257)

[Activité 1.b (Biens primordiaux/support) 4](#_Toc71626258)

[Activité 1.c (Événement redoutés) 7](#_Toc71626259)

[Activité 1.d (Les socles de sécurité) 10](#_Toc71626260)

[Activité 2 (Source de risque) 12](#_Toc71626261)

[Activité 2.a (Identifier les sources de risques et les objectifs) 12](#_Toc71626262)

[Activité 2.b (Évaluer les couples sources de risque/objectifs visés) 13](#_Toc71626263)

[Activité 2.c (Sélectionner les couples SR/OV retenus pour la suite de l’analyse) 14](#_Toc71626264)

[Activité 3 (Scénarios stratégiques) 16](#_Toc71626265)

[Activité 3.a (Construire la cartographie des menaces numériques de l'écosystème et sélectionner les parties prenantes critiques) 16](#_Toc71626266)

[Activité 3.b (Élaborer des scénarios stratégiques) 18](#_Toc71626267)

[Activité 3.c (Définir des mesures de sécurité sur l'écosystème) 22](#_Toc71626268)

[Activité 4 (Scénarios opérationnels) 24](#_Toc71626269)

[Activité 4.a (Élaborer les scénarios opérationnels) 24](#_Toc71626270)

[Activité 4.b (Évaluer la vraisemblance des scénarios opérationnels) 25](#_Toc71626271)

[Activité 5 (Traitement du risque) 27](#_Toc71626272)

[Activité 5.a (Réaliser une synthèse des scénarios de risque) 27](#_Toc71626273)

[Activité 5.b (Décider de la stratégie de traitement du risque et définir les mesures de sécurité) 28](#_Toc71626274)

[Activité 5.c (Évaluer et documenter les risques résiduels) 29](#_Toc71626275)

# Activité 1 (Cadrage et socle de sécurité)

## Activité 1.a (Cadrer l’étude)

Données principales ( f\_projet)

Nom du projet : ${nomProjet}

Objectif à atteindre : ${Objectif}

Cadre Temporel :

Atelier 1 : ${jj/mm/aaaa1}

Atelier 2 : ${jj/mm/aaaa2}

Atelier 3 : ${jj/mm/aaaa3}

Atelier 4 : ${jj/mm/aaaa4}

Atelier 5 : ${jj/mm/aaaa5}

Durée des cycles stratégiques et opérationnels

Durée des cycles stratégiques : ${dure1}

Durée des cycles opérationnels : ${dure2}

Niveau de confidentialité : ${niveauConfidentialite}

Personne responsable d'accepter les risques résiduels au terme de l'étude : ${responsable}

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.a (Cadrer l’étude)

Acteurs

| **nom** | **prenom** | **poste** |
| --- | --- | --- |
| ANTON RAVEENDRAN | Joyston | Ingénieur Cybersécurité |
| PINTO | Carlos | Ingénieur sécurité |
| Sec | YourDev | Ingé |
| ANTON | Joyston | Ingénieur |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.a (Cadrer l’étude)

RACI

| **nom** | **prenom** | **id\_atelier** | **ecriture** |
| --- | --- | --- | --- |
| ANTON RAVEENDRAN | Joyston | 1.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 1.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 1.c | Réalisation |
| ANTON RAVEENDRAN | Joyston | 1.d | Réalisation |
| ANTON RAVEENDRAN | Joyston | 2.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 2.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 2.c | Réalisation |
| ANTON RAVEENDRAN | Joyston | 3.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 3.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 3.c | Réalisation |
| ANTON RAVEENDRAN | Joyston | 4.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 4.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 5.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 5.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 5.c | Réalisation |
| PINTO | Carlos | 1.a | Réalisation |
| PINTO | Carlos | 1.b | Réalisation |
| PINTO | Carlos | 1.c | Réalisation |
| PINTO | Carlos | 1.d | Réalisation |
| PINTO | Carlos | 2.a | Réalisation |
| PINTO | Carlos | 2.b | Réalisation |
| PINTO | Carlos | 2.c | Réalisation |
| PINTO | Carlos | 3.a | Réalisation |
| PINTO | Carlos | 3.b | Réalisation |
| PINTO | Carlos | 3.c | Réalisation |
| PINTO | Carlos | 4.a | Réalisation |
| PINTO | Carlos | 4.b | Réalisation |
| PINTO | Carlos | 5.a | Réalisation |
| PINTO | Carlos | 5.b | Réalisation |
| PINTO | Carlos | 5.c | Réalisation |
| Sec | YourDev | 1.a | Information |
| Sec | YourDev | 1.b | Information |
| Sec | YourDev | 1.c | Information |
| Sec | YourDev | 1.d | Information |
| Sec | YourDev | 2.a | Information |
| Sec | YourDev | 2.b | Information |
| Sec | YourDev | 2.c | Information |
| Sec | YourDev | 3.a | Information |
| Sec | YourDev | 3.b | Information |
| Sec | YourDev | 3.c | Information |
| Sec | YourDev | 4.a | Information |
| Sec | YourDev | 4.b | Information |
| Sec | YourDev | 5.a | Information |
| Sec | YourDev | 5.b | Information |
| Sec | YourDev | 5.c | Information |
| ANTON | Joyston | 1.a | Information |
| ANTON | Joyston | 1.b | Information |
| ANTON | Joyston | 1.c | Information |
| ANTON | Joyston | 1.d | Information |
| ANTON | Joyston | 2.a | Information |
| ANTON | Joyston | 2.b | Information |
| ANTON | Joyston | 2.c | Information |
| ANTON | Joyston | 3.a | Information |
| ANTON | Joyston | 3.b | Information |
| ANTON | Joyston | 3.c | Information |
| ANTON | Joyston | 4.a | Information |
| ANTON | Joyston | 4.b | Information |
| ANTON | Joyston | 5.a | Information |
| ANTON | Joyston | 5.b | Information |
| ANTON | Joyston | 5.c | Information |

**Activité 1 (Cadrage et socle de sécurité)**

## Activité 1.b (Biens primordiaux/support)

Valeur métier

| **nom\_valeur\_metier** | **nature\_valeur\_metier** | **description\_valeur\_metier** |
| --- | --- | --- |
| Mot de passe | Information | Desc MDP |
| Vente en ligne | Processus | Processus de vente en ligne de produit de grande consommation |
| tggggAAA | Processus | gggg |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.b (Biens primordiaux/support)

Bien support

| **nom\_bien\_support** | **description\_bien\_support** |
| --- | --- |
| Clé usb | Desc BS |
| Disque | desc disqie |
| Serveur | Serveur amazon pour la vente en ligne |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.b (Biens primordiaux/support)

Mission

| **Nom de la mission** | **Description de la mission** | **Responsable** | **Valeur Métier** | **Responsable de la valeur métier** | **Bien Support** | **Responsable du bien support** |
| --- | --- | --- | --- | --- | --- | --- |

**Activité 1 (Cadrage et socle de sécurité)**

## Activité 1.c (Événement redoutés)

Echelle

| **Nom de l'échelle** | **Échelle de gravité** |
| --- | --- |
| CarlosEchelle | 4 |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.c (Événement redoutés)

Niveau

| **Valeur du niveau** | **Description du niveau** |
| --- | --- |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.c (Événement redoutés)

Événements redoutés

${m\_evenement\_redoute}

**Activité 1 (Cadrage et socle de sécurité)**

## Activité 1.d (Les socles de sécurité)

Socle de sécurité

| **Type de référentiel** | **Nom du référentiel** | **État d'application** |
| --- | --- | --- |
| Référentiel de sécurité | Cloisonnement système | Appliqué sans restriction |
| Référentiel de sécurité | Guide d'hygiène informatique | Appliqué sans restriction |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.d (Les socles de sécurité)

Règles

| **ID de la règle** | **Titre de la règle** | **Description de la règle** | **État de la règle** | **Justification des écarts** | **Responsable** | **Date limite de la mise en application** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Appliquer le principe de moindre privilège dès la conception | Interdire par défaut toute action et procéder à l’autorisation exclusive de ce qui estnécessaire aux tâches constitue la stratégie la plus efficace de mise en œuvre duprincipe de moindre privilège. Il convient de s’y conformer autant que possible dèsla phase de conception du composant. | Non conforme |  |  | 0000-00-00 |
| 2 | Tenir compte de ses besoins en cloisonnement dès l'initiation d'un projet | Les besoins en cloisonnement d’un composant doivent faire l’objet d’un diagnosticet être considérés comme des besoins au même titre que les besoins fonctionnels, etce dès le début du projet. |  |  |  |  |
| 3 | Préférer des composants implémentant un cloisonnement pertinent | Lors d’un choix entre différentes solutions, celles qui démontrent la meilleure priseen compte du principe du moindre privilège devront être préférées. |  |  |  |  |
| 4 | Garantir l'intégrité des composants de confiance | Il est impératif de garantir concrètement l’intégrité des composants de confiancepour que la sécurité de l’ensemble du composant soit assurée. Des recommandationsplus précises sont fournies en4.1. |  |  |  |  |
| 5 | Rédiger l'analyse de la sécurité attendue du composant | Une analyse de la sécurité attendue du composant doit faire partie des documentsde conception ou intégration mis à disposition.Elle doit comporter les définitions des quatre éléments cités ci-dessus : la liste des biens sensibles à protéger; le modèle d’attaquant pris en compte (duquel découle en particulier l’identifica-tion des composants de confiance); nle périmètre du composant, c’est-à-dire sa surface d’attaque et sa surface de fric-tion avec le système global; nles fonctions de sécurité attendues. |  |  |  |  |
| 6 | Caractériser des usages du composant | Réaliser une liste des usages du composant à partir de ses fonctionnalités et de laliste des ressources auxquelles il accède. |  |  |  |  |
| 7 | Minimiser de la surface d'attaque | Réduire systématiquement la surface d’attaque pour chaque usage, de manière à n’-exposer que les interfaces externes utiles pour l’usage considéré. |  |  |  |  |
| 8 | Cloisonner les usages entre eux | Mettre en place un moniteur de référence en s’appuyant sur les composants de con-fiance pour faire en sorte que chaque usage soit confiné dans un domaine. |  |  |  |  |
| 9 | Minimiser la surface de friction | Réduire systématiquement les actions possibles pour chaque domaine aux seuls be-soins liés à l’usage, c’est-à-dire réduire la surface de friction avec le système global. |  |  |  |  |
| 10 | Considérer le moniteur comme un composant de confiance | Vis-à-vis d’un attaquant de la fonction de sécurité de cloisonnement, le moniteur deréférence fait partie des composants de confiance. Ainsi, il doit respecter les recom-mandations de cette section. |  |  |  |  |
| 11 | Identifier les composants de confiance | Tout composant du système qui dispose d’un privilège lui permettant de porter at-teinte à l’intégrité du moniteur, ou des politiques de sécurité qu’il met en place, est àconsidérer comme faisant partie des composants de confiance vis-à-vis du composantanalysé.Tous ces composants doivent donc vérifier les exigences propres aux composants deconfiance. |  |  |  |  |
| 12 | Concevoir des composants simples et concis | Les composants de confiance doivent être conçus en suivant des spécifications claireset complètes, permettant de définir et combiner des éléments simples (suivant leprincipe « Keep It Short and Simple ») qui facilitent développement et validation. |  |  |  |  |
| 13 | Choisir un langage approprié | Utiliser un langage de programmation fortement typé, qui entre autres prévient lesdébordements de tableau, d’entier, ou l’utilisation de pointeurs invalides, est forte-ment souhaitable pour le développement des composants de confiance. |  |  |  |  |
| 14 | Développer selon un référentiel de sécurité | Un référentiel de développement sécurisé doit être utilisé systématiquement lors dudéveloppement de composants de confiance.La vérification du respect du référentiel de codage doit être assurée.Le respect de cette recommandation est critique dans le cas du choix d’un langagene respectant pas les critères conseillés ci-dessus. |  |  |  |  |
| 15 | Auditer le code de l'implémentation des composants de confiance | L’intégralité du code des composants de confiance devra faire l’objet d’un audit decode par des personnels qui n’en sont pas développeurs, de préférence indépendantsdu projet concerné. |  |  |  |  |
| 16 | Valider l'implémentation des composants de confiance | Des tests fonctionnels complets devront permettre de valider le bon fonctionnementdes fonctions de sécurité implémentées. Une attention particulière sera portée àtester aussi bien les opérations qui doivent être refusées que celles qui doivent êtremenées à bien avec succès. |  |  |  |  |
| 17 | Prouver l'implémentation des composants de confiance | Il est fortement recommandé de compléter les tests par une preuve formelle del’absence d’erreur à l’exécution d’un composant de confiance, par exemple à l’aided’outils d’analyse (statique ou dynamique) pour prévenir certains types de vulnérabilités. |  |  |  |  |
| 18 | Supprimer toute partie inutilisée d'un composant de confiance | Un composant de confiance doit être minimal. Dès que possible, la suppression ducode inutilisé sera privilégiée. A défaut, sa désactivation par configuration sera effectuée. |  |  |  |  |
| 19 | Appliquer des techniques de durcissement aux composants de confiance | Les composants de confiance doivent se voir appliquer des techniques de durcisse-ment à l’état de l’art afin de compliquer l’exploitation d’une vulnérabilité et le dé-tournement du flot de contrôle, comme par exemple : présence de motifs d’intégrité de la pile et du tas (canaris); principe W+X : au cours de toute son utilisation par le système, une zone mé-moire donnée ne doit pas être inscriptible et exécutable, que ce soit simultané-ment ou non; répartition aléatoire de l’espace d’adressage (ou Address Space Layout Random-ization (ASLR)). |  |  |  |  |
| 20 | Justifier le respect des propriétés fondamentales du moniteur de référence | Le développement, l’intégration et la validation du moniteur de référence doiventpermettre de garantir qu’il vérifie les propriétés suivantes. 1.Complétude du contrôle exercé: le moniteur est impliqué pour chaque tenta-tive d’accès à une ressource, et ce au moment opportun (i.e. absence d’attaquesTOCTTOU (Time Of Check To Time Of Use), liées à une évolution des propriétésde l’objet entre le moment de la requête au moniteur et l’action effective). 2.Maintien de l’intégrité du moniteur. 3.Validation et audit de la politique de sécurité. La possibilité de consulter la poli-tique de sécurité implémentée par le moniteur à un instant donné permettral’audit de celle-ci.Des justifications construites confirmant le respect de ces propriétés doivent figurerdans les documents de conception du composant utilisant le moniteur de référence. |  |  |  |  |
| 21 | Assurer au moniteur de référence un niveau de privilège supérieur à celuides tâches cloisonnées | De manière à préserver l’intégrité du moniteur et des politiques de sécurité qu’il meten application, les tâches cloisonnées ne doivent pas disposer des privilèges néces-saires à la relaxe de la politique de sécurité appliquée.Une façon de garantir ceci est d’assurer que les politiques sont non-modifiables parles tâches cloisonnées et que le moniteur s’exécute à un niveau de privilège supérieurà celui des tâches qu’il cloisonne. |  |  |  |  |
| 22 | Appliquer le principe d'interdiction par défaut | Un moniteur de référence doit être configurable pour que toute action soit interditeà une tâche, sauf à lui être explicitement autorisée. |  |  |  |  |
| 23 | Minimiser le nombre et l'impact des configurations possibles | Dans une démarche de durcissement du moniteur, les options de configuration lais-sées au choix de l’utilisateur (même privilégié) en production doivent être restreintesau strict minimum, de manière à réduire l’impact possible d’une erreur sur la sécuritéglobale du système. Pour les choix laissés à l’utilisateur, les messages d’avertissementsur les conséquences en terme de sécurité doivent être suffisamment explicites. |  |  |  |  |
| 24 | Spécifier le cloisonnement proposé | Pour présenter le cloisonnement mis en place, il est recommandé de procéder de lamanière suivante. 1.Expliciter les usages identifiés. 2.Décrire le mécanisme de cloisonnement mis en oeuvre en explicitant ce àquoi correspondent les définitions de tâches, ressources propres et partagéeset moniteur de référence. 3. Expliciter la politique de sécurité mise en place pour chaque usage.Pour chaque domaine, il faut reprendre la liste des interfaces externes dressées précédem-ment et caractériser les actions autorisées. |  |  |  |  |
| 25 | Assurer l'innocuité du composant pour le système qui l'accueille | Un composant ne doit pas dégrader la sécurité globale du système, notamment enlimitant la mise en place du cloisonnement par d’autres composants utilisés sur lemême système.En particulier, un composant ne doit pas exiger pour fonctionner d’abaisser le niveaude sécurité du système qui l’héberge : le composant doit être compatible avec unniveau de durcissement à l’état de l’art au moment de sa mise en production. |  |  |  |  |
| 26 | Ma règle | Ma description | Non traité |  |  | 2020-09-03 |
| 1 | Former les équipes opérationnelles à la sécurité des systèmes d’information | / standard Les équipes opérationnelles (administrateurs réseau, sécurité et système, chefs de projet, développeurs, RSSI) ont des accès privilégiés au système d’information. Elles peuvent, par inadvertance ou par méconnaissance des conséquences de certaines pratiques, réaliser des opérations génératrices de vulnérabilités. Citons par exemple l’affectation de comptes disposant de trop nombreux privilèges par rapport à la tâche à réaliser, l’utilisation de comptes personnels pour exécuter des services ou tâches périodiques, ou encore le choix de mots de passe peu robustes donnant accès à des comptes privilégiés. Les équipes opérationnelles, pour être à l’état de l’art de la sécurité des systèmes d’information, doivent donc suivre - à leur prise de poste puis à intervalles réguliers - des formations sur : > la législation en vigueur ; > les principaux risques et menaces ; > le maintien en condition de sécurité ; > l’authentification et le contrôle d’accès ; > le paramétrage fin et le du |  |  |  |  |
| 2 | Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique | / standard Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d’information. À ce titre et dès son arrivée dans l’entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d’information à travers des actions de sensibilisation et de formation. Ces dernières doivent être régulières, adaptées aux utilisateurs ciblés, peuvent prendre différentes formes (mails, affichage, réunions, espace intranet dédié,etc.) et aborder au minimum les sujets suivants : >> les objectifs et enjeux que rencontre l’entité en matière de sécurité dessystèmes d’information ; >> les informations considérées comme sensibles ;>> les réglementations et obligations légales ; >> les règles et consignes de sécurité régissant l’activité quotidienne : respect de la politique de sécurité, non-connexion d’équipements personnels au réseau de l’entité, non-divulgation de mots de passe à un tiers, non-réutilisation |  |  |  |  |
| 3 | Maîtriser les risques de l’infogérance | / standard Lorsqu’une entité souhaite externaliser son système d’information ou ses données, elle doit en amont évaluer les risques spécifiques à l’infogérance (maîtrise du système d’information, actions à distance, hébergement mutualisé, etc.) afin de prendre en compte, dès la rédaction des exigences applicables au futur prestataire, les besoins et mesures de sécurité adaptés. Les risques SSI inhérents à ce type de démarche peuvent être liés au contexte de l’opération d’externalisation mais aussi à des spécifications contractuelles déficientes ou incomplètes. En faveur du bon déroulement des opérations, il s’agit donc : >> d’étudier attentivement les conditions des offres, la possibilité de les adapter à des besoins spécifiques et les limites de responsabilité du prestataire ; >> d’imposer une liste d’exigences précises au prestataire : réversibilité du contrat, réalisation d’audits, sauvegarde et restitution des données dans un format ouvert normalisé, maintien à niveau de la sécurit |  |  |  |  |
| 4 | Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau | /Standard Chaque entité possède des données sensibles. Ces dernières peuvent porter sur son activité propre (propriété intellectuelle, savoir-faire, etc.) ou sur ses clients, administrés ou usagers (données personnelles, contrats, etc.). Afin de pouvoir les protéger efficacement, il est indispensable de les identifier. À partir de cette liste de données sensibles, il sera possible de déterminer sur quels composants du système d’information elles se localisent (bases de données, partages de fichiers, postes de travail, etc.). Ces composants correspondent aux serveurs et postes critiques pour l’entité. À ce titre, ils devront faire l’objet de mesures de sécurité spécifiques pouvant porter sur la sauvegarde, la journalisation, les accès, etc. Il s’agit donc de créer et de maintenir à jour un schéma simplifié du réseau (ou cartographie) représentant les différentes zones IP et le plan d’adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs,etc.) et les |  |  |  |  |
| 5 | Disposer d’un inventaire exhaustif des comptes privilégiés et le maintenir à jour | /Standard Les comptes bénéficiant de droits spécifiques sont des cibles privilégiées par les attaquants qui souhaitent obtenir un accès le plus large possible au système d’information. Ils doivent donc faire l’objet d’une attention toute particulière. Il s’agit pour cela d’effectuer un inventaire de ces comptes, de le mettre à jour régulièrement et d’y renseigner les informations suivantes : >> les utilisateurs ayant un compte administrateur ou des droits supérieurs à ceux d’un utilisateur standard sur le système d’information ; >> les utilisateurs disposant de suffisamment de droits pour accéder aux répertoires de travail des responsables ou de l’ensemble des utilisateurs ; >> les utilisateurs utilisant un poste non administré par le service informatique et qui ne fait pas l’objet de mesures de sécurité édictées par la politique de sécurité générale de l’entité. Il est fortement recommandé de procéder à une revue périodique de ces comptes afin de s’assurer que les accès aux éléments |  |  |  |  |
| 6 | Organiser les procédures d’arrivée, de départ et de changement de fonction des utilisateurs | / Standard Les effectifs d’une entité, qu’elle soit publique ou privée, évoluent sans cesse : arrivées, départs, mobilité interne. Il est par conséquent nécessaire que les droits et les accès au système d’information soient mis à jour en fonction de ces évolutions. Il est notamment essentiel que l’ensemble des droits affectés à une personne soient révoqués lors de son départ ou en cas de changement de fonction. Les procédures d’arrivée et de départ doivent donc être définies, en lien avec la fonction ressources humaines. Elles doivent au minimum prendre en compte : >> la création et la suppression des comptes informatiques et boîtes aux lettres associées ; >> les droits et accès à attribuer et retirer à une personne dont la fonction change ; >> la gestion des accès physiques aux locaux (attribution, restitution des badges et des clés, etc.) ; >> l’affectation des équipements mobiles (ordinateur portable, clé USB, disque dur, ordiphone, etc.) ; >> la gestion des documents et information |  |  |  |  |
| 7 | Autoriser la connexion au réseau de l’entité aux seuls équipements maîtrisés | /Standard Pour garantir la sécurité de son système d’information, l’entité doit maîtriser les équipements qui s’y connectent, chacun constituant un point d’entrée potentiellement vulnérable. Les équipements personnels (ordinateurs portables, tablettes, ordiphones, etc.) sont, par définition, difficilement maîtrisables dans la mesure où ce sont les utilisateurs qui décident de leur niveau de sécurité. De la même manière, la sécurité des équipements dont sont dotés les visiteurs échappe à tout contrôle de l’entité. Seule la connexion de terminaux maîtrisés par l’entité doit être autorisée sur ses différents réseaux d’accès, qu’ils soient filaire ou sans fil. Cette recommandation, avant tout d’ordre organisationnel, est souvent perçue comme inacceptable ou rétrograde. Cependant, y déroger fragilise le réseau de l’entité et sert ainsi les intérêts d’un potentiel attaquant. La sensibilisation des utilisateurs doit donc s’accompagner de solutions pragmatiques répondant à leurs besoins. Cito |  |  |  |  |
| 8 | Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur /admini | /Standard Afin de faciliter l’attribution d’une action sur le système d’information en cas d’incident ou d’identifier d’éventuels comptes compromis, les comptes d’accès doivent être nominatifs. L’utilisation de comptes génériques (ex : admin, user) doit être marginale et ceux-ci doivent pouvoir être rattachés à un nombre limité de personnes physiques. Bien entendu, cette règle n’interdit pas le maintien de comptes de service, rattachés à un processus informatique (ex : apache, mysqld). Dans tous les cas, les comptes génériques et de service doivent être gérés selon une politique au moins aussi stricte que celle des comptes nominatifs. Par ailleurs, un compte d’administration nominatif, distinct du compte utilisateur, doit être attribué à chaque administrateur. Les identifiants et secrets d’authentification doivent être différents (ex : pmartin comme identifiant utilisateur, adm-pmartin comme identifiant administrateur). Ce compte d’administration, disposant de plus de privilèges, doit |  |  |  |  |
| 9 | Attribuer les bons droits sur les ressources sensibles du système d’information | /Standard Certaines des ressources du système peuvent constituer une source d’information précieuse aux yeux d’un attaquant (répertoires contenant des données sensibles, bases de données, boîtes aux lettres électroniques, etc.). Il est donc primordial d’établir une liste précise de ces ressources et pour chacune d’entre elles : >> de définir quelle population peut y avoir accès ; >> de contrôler strictement son accès, en s’assurant que les utilisateurs sont authentifiés et font partie de la population ciblée ; >> d’éviter sa dispersion et sa duplication à des endroits non maîtrisés ou soumis à un contrôle d’accès moins strict. Par exemple, les répertoires des administrateurs regroupant de nombreuses informations sensibles doivent faire l’objet d’un contrôle d’accès précis. Il en va de même pour les informations sensibles présentes sur des partages réseau : exports de fichiers de configuration, documentation technique du système d’information, bases de données métier, etc. Une revue ré |  |  |  |  |
| 10 | Définir et vérifier des règles de choix et de dimensionnement des mots de passe | /Standard L’ANSSI énonce un ensemble de règles et de bonnes pratiques en matière de choix et de dimensionnement des mots de passe. Parmi les plus critiques de ces règles figure la sensibilisation des utilisateurs aux risques liés au choix d’un mot de passe qui serait trop facile à deviner, ou encore la réutilisation de mots de passe d’une application à l’autre et plus particulièrement entre messageries personnelles et professionnelles. Pour encadrer et vérifier l’application de ces règles de choix et de dimensionnement, l’entité pourra recourir à différentes mesures parmi lesquelles : >> le blocage des comptes à l’issue de plusieurs échecs de connexion ; >> la désactivation des options de connexion anonyme ; >> l’utilisation d’un outil d’audit de la robustesse des mots de passe. En amont de telles procédures, un effort de communication visant à expliquer le sens de ces règles et éveiller les consciences sur leur importance est fondamental. |  |  |  |  |
| 11 | Protéger les mots de passe stockés sur les systèmes | /Standard La complexité, la diversité ou encore l’utilisation peu fréquente de certains mots de passe, peuvent encourager leur stockage sur un support physique (mémo, post-it) ou numérique (fichiers de mots de passe, envoi par mail à soimême, recours aux boutons « Se souvenir du mot de passe ») afin de pallier tout oubli ou perte. Or, les mots de passe sont une cible privilégiée par les attaquants désireux d’accéder au système, que cela fasse suite à un vol ou à un éventuel partage du support de stockage. C’est pourquoi ils doivent impérativement être protégés au moyen de solutions sécurisées au premier rang desquelles figurent l’utilisation d’un coffre-fort numérique et le recours à des mécanismes de chiffrement. Bien entendu, le choix d’un mot de passe pour ce coffre-fort numérique doit respecter les règles énoncées précédemment et être mémorisé par l’utilisateur, qui n’a plus que celui-ci à retenir. |  |  |  |  |
| 12 | Changer les éléments d’authentification par défaut sur les équipements et services | /Standard Il est impératif de partir du principe que les configurations par défaut des systèmes d’information sont systématiquement connues des attaquants, quand bien même celles-ci ne le sont pas du grand public. Ces configurations se révèlent (trop) souvent triviales (mot de passe identique à l’identifiant, mal dimensionné ou commun à l’ensemble des équipements et services par exemple) et sont, la plupart du temps, faciles à obtenir pour des attaquants capables de se faire passer pour un utilisateur légitime. Les éléments d’authentification par défaut des composants du système doivent donc être modifiés dès leur installation et, s’agissant de mots de passe, être conformes aux recommandations précédentes en matière de choix, de dimensionnement et de stockage. Si le changement d’un identifiant par défaut se révèle impossible pour cause, par exemple, de mot de passe ou certificat « en dur » dans un équipement, ce problème critique doit être signalé au distributeur du produit afin que ce |  |  |  |  |
| 13 | Privilégier lorsque c’est possible une authentification forte | /Standard Il est vivement recommandé de mettre en oeuvre une authentification forte nécessitant l’utilisation de deux facteurs d’authentification différents parmi les suivants : >> quelque chose que je sais (mot de passe, tracé de déverrouillage, signature) ; >> quelque chose que je possède (carte à puce, jeton USB, carte magnétique, RFID, un téléphone pour recevoir un code SMS) ; >> quelque chose que je suis (une empreinte biométrique). /Renforcé Les cartes à puces doivent être privilégiées ou, à défaut, les mécanismes de mots de passe à usage unique (ou One Time Password) avec jeton physique. Les opérations cryptographiques mises en place dans ces deux facteurs offrent généralement de bonnes garanties de sécurité. Les cartes à puce peuvent être plus complexes à mettre en place car nécessitant une infrastructure de gestion des clés adaptée. Elles présentent cependant l’avantage d’être réutilisables à plusieurs fins : chiffrement, authentification de messagerie, authentification sur |  |  |  |  |
| 14 | Mettre en place un niveau de sécurité minimal sur l’ensemble du parc informatique | /Standard L’utilisateur plus ou moins au fait des bonnes pratiques de sécurité informatique est, dans de très nombreux cas, la première porte d’entrée des attaquants vers le système. Il est donc fondamental de mettre en place un niveau de sécurité minimal sur l’ensemble du parc informatique de l’entité (postes utilisateurs, serveurs, imprimantes, téléphones, périphériques USB, etc.) en implémentant les mesures suivantes : >> limiter les applications installées et modules optionnels des navigateurs web aux seuls nécessaires ; >> doter les postes utilisateurs d’un pare-feu local et d’un anti-virus (ceux-ci sont parfois inclus dans le système d’exploitation) ; >> chiffrer les partitions où sont stockées les données des utilisateurs ; >> désactiver les exécutions automatiques (autorun). En cas de dérogation nécessaire aux règles de sécurité globales applicables aux postes, ceux-ci doivent être isolés du système (s’il est impossible de mettre à jour certaines applications pour des raisons d |  |  |  |  |
| 15 | Se protéger des menaces relatives à l’utilisation de supports amovibles | /Standard Les supports amovibles peuvent être utilisés afin de propager des virus, voler des informations sensibles et stratégiques ou encore compromettre le réseau de l’entité. De tels agissements peuvent avoir des conséquences désastreuses pour l’activité de la structure ciblée. S’il n’est pas question d’interdire totalement l’usage de supports amovibles au sein de l’entité, il est néanmoins nécessaire de traiter ces risques en identifiant des mesures adéquates et en sensibilisant les utilisateurs aux risques que ces supports peuvent véhiculer. Il convient notamment de proscrire le branchement de clés USB inconnues (ramassées dans un lieu public par exemple) et de limiter au maximum celui de clés non maîtrisées (dont on connait la provenance mais pas l’intégrité) sur le système d’information à moins, dans ce dernier cas, de faire inspecter leur contenu par l’antivirus du poste de travail. /Renforcé Sur les postes utilisateur, il est recommandé d’utiliser des solutions permettant d’i |  |  |  |  |
| 16 | Utiliser un outil de gestion centralisée afin d’homogénéiser les politiques de sécurité | /Standard La sécurité du système d’information repose sur la sécurité du maillon le plus faible. Il est donc nécessaire d’homogénéiser la gestion des politiques de sécurité s’appliquant à l’ensemble du parc informatique de l’entité. L’application de ces politiques (gestion des mots de passe, restrictions de connexions sur certains postes sensibles, configuration des navigateurs Web, etc.) doit être simple et rapide pour les administrateurs, en vue notamment de faciliter la mise en oeuvre de contre-mesures en cas de crise informatique. Pour cela, l’entité pourra se doter d’un outil de gestion centralisée (par exemple Active Directory en environnement Microsoft) auquel il s’agit d’inclure le plus grand nombre d’équipements informatiques possible. Les postes de travail et les serveurs sont concernés par cette mesure qui nécessite éventuellement en amont un travail d’harmonisation des choix de matériels et de systèmes d’exploitation. Ainsi, des politiques de durcissement du système d’explo |  |  |  |  |
| 17 | Activer et configurer le parefeu local des postes de travail | /Standard Après avoir réussi à prendre le contrôle d’un poste de travail (à cause, par exemple, d’une vulnérabilité présente dans le navigateur Internet), un attaquant cherchera souvent à étendre son intrusion aux autres postes de travail pour, in fine, accéder aux documents des utilisateurs. Afin de rendre plus difficile ce déplacement latéral de l’attaquant, il est nécessaire d’activer le pare-feu local des postes de travail au moyen de logiciels intégrés (pare-feu local Windows) ou spécialisés. Les flux de poste à poste sont en effet très rares dans un réseau bureautique classique : les fichiers sont stockés dans des serveurs de fichiers, les applications accessibles sur des serveurs métier, etc. /Renforcé Le filtrage le plus simple consiste à bloquer l’accès aux ports d’administration par défaut des postes de travail (ports TCP 135, 445 et 3389 sous Windows, port TCP 22 sous Unix), excepté depuis les ressources explicitement identifiées (postes d’administration et d’assistance uti |  |  |  |  |
| 18 | Chiffrer les données sensibles transmises par voie Internet | /Standard Internet est un réseau sur lequel il est quasi impossible d’obtenir des garanties sur le trajet que vont emprunter les données que l’on y envoie. Il est donc tout à fait possible qu’un attaquant se trouve sur le trajet de données transitant entre deux correspondants. Toutes les données envoyées par courriel ou transmises au moyen d’outils d’hébergement en ligne (Cloud) sont par conséquent vulnérables. Il s’agit donc de procéder à leur chiffrement systématique avant de les adresser à un correspondant ou de les héberger. La transmission du secret (mot de passe, clé, etc.) permettant alors de déchiffrer les données, si elle est nécessaire, doit être effectuée via un canal de confiance ou, à défaut, un canal distinct du canal de transmission des données. Ainsi, si les données chiffrées sont transmises par courriel, une remise en main propre du mot de passe ou, à défaut, par téléphone doit être privilégiée. |  |  |  |  |
| 19 | Segmenter le réseau et mettre en place un cloisonnement entre ces zones | /Standard Lorsque le réseau est " à plat ", sans aucun mécanisme de cloisonnement, chaque machine du réseau peut accéder à n’importe quelle autre machine.La compromission de l’une d’elles met alors en péril l’ensemble des machines connectées. Un attaquant peut ainsi compromettre un poste utilisateur et ensuite " rebondir " jusqu’à des serveurs critiques. Il est donc important, dès la conception de l’architecture réseau, de raisonner par segmentation en zones composées de systèmes ayant des besoins de sécurité homogènes. On pourra par exemple regrouper distinctement des serveurs d’infrastructure, des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, etc. Une zone se caractérise alors par des VLAN et des sous-réseaux IP dédiés voire par des infrastructures dédiées selon sa criticité. Ainsi, des mesures de cloisonnement telles qu’un filtrage IP à l’aide d’un pare-feu peuvent être mises en place entre les différent |  |  |  |  |
| 20 | S’assurer de la sécurité des réseaux d’accès Wi-Fi et de la séparation des usages | /Standard/nL’usage du Wi-Fi en milieu professionnel est aujourd’hui démocratisé mais présente toujours des risques de sécurité bien spécifiques : faibles garanties en matière de disponibilité, pas de maîtrise de la zone de couverture pouvant mener à une attaque hors du périmètre géographique de l’entité, configuration par défaut des points d’accès peu sécurisée, etc. La segmentation de l’architecture réseau doit permettre de limiter les conséquences d’une intrusion par voie radio à un périmètre déterminé du système d’information. Les flux en provenance des postes connectés au réseau d’accès Wi-Fi doivent donc être filtrés et restreints aux seuls flux nécessaires. De plus, il est important d’avoir recours prioritairement à un chiffrement robuste (mode WPA2, algorithme AES CCMP) et à une authentification centralisée, si possible par certificats clients des machines. La protection du réseau Wi-Fi par un mot de passe unique et partagé est déconseillée. À défaut, il doit être complexe et so |  |  |  |  |
| 21 | Utiliser des protocoles réseaux sécurisés dès qu’ils existent | /Standard Si aujourd’hui la sécurité n’est plus optionnelle, cela n’a pas toujours été le cas. C’est pourquoi de nombreux protocoles réseaux ont dû évoluer pour intégrer cette composante et répondre aux besoins de confidentialité et d’intégrité qu’impose l’échange de données. Les protocoles réseaux sécurisés doivent être utilisés dès que possible, que ce soit sur des réseaux publics (Internet par exemple) ou sur le réseau interne de l’entité. Bien qu’il soit difficile d’en dresser une liste exhaustive, les protocoles les plus courants reposent sur l’utilisation de TLS et sont souvent identifiables par l’ajout de la lettre « s » (pour secure en anglais) à l’acronyme du protocole.Citons par exemple https pour la navigation Web ou IMAPS, SMTPS ou POP3S pour la messagerie. D’autres protocoles ont été conçus de manière sécurisée dès la conception pour se substituer à d’anciens protocoles non sécurisés. Citons par exemple SSH (Secure SHell) venu remplacer les protocoles de communication hist |  |  |  |  |
| 22 | Mettre en place une passerelle d’accès sécurisé à Internet | /Standard L’accès à Internet, devenu indispensable, présente des risques importants : sites Web hébergeant du code malveillant, téléchargement de fichiers « toxiques » et, par conséquent, possible prise de contrôle du terminal, fuite de données sensibles, etc. Pour sécuriser cet usage, il est donc indispensable que les terminaux utilisateurs n’aient pas d’accès réseau direct à Internet. C’est pourquoi il est recommandé de mettre en oeuvre une passerelle sécurisée d’accès à Internet comprenant au minimum un pare-feu au plus près de l’accès Internet pour filtrer les connexions et un serveur mandataire (proxy) embarquant différents mécanismes de sécurité. Celui-ci assure notamment l’authentification des utilisateurs et la journalisation des requêtes. /Renforcé Des mécanismes complémentaires sur le serveur mandataire pourront être activés selon les besoins de l’entité : analyse antivirus du contenu, filtrage par catégories d’URLs, etc. Le maintien en condition de sécurité des équipements |  |  |  |  |
| 23 | Cloisonner les services visibles depuis Internet du reste du système d’information | /Standard Une entité peut choisir d’héberger en interne des services visibles sur Internet (site web, serveur de messagerie, etc.). Au regard de l’évolution et du perfectionnement des cyberattaques sur Internet, il est essentiel de garantir un haut niveau de protection de ce service avec des administrateurs compétents, formés de manière continue (à l’état de l’art des technologies en la matière) et disponibles. Dans le cas contraire, le recours à un hébergement externalisé auprès de professionnels est à privilégier. De plus, les infrastructures d’hébergement Internet doivent être physiquement cloisonnées de toutes les infrastructures du système d’information qui n’ont pas vocation à être visibles depuis Internet. Enfin, il convient de mettre en place une infrastructure d’interconnexion de ces services avec Internet permettant de filtrer les flux liés à ces services de manière distincte des autres flux de l’entité. Il s’agit également d’imposer le passage des flux entrants par un serveu |  |  |  |  |
| 24 | Protéger sa messagerie professionnelle | /Standard La messagerie est le principal vecteur d’infection du poste de travail, qu’il s’agisse de l’ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant. Les utilisateurs doivent être particulièrement sensibilisés à ce sujet : l’expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l’authenticité du message par un autre canal (téléphone, SMS, etc.) est nécessaire. Pour se prémunir d’escroqueries (ex : demande de virement frauduleux émanant vraisemblablement d’un dirigeant), des mesures organisationnelles doivent être appliquées strictement. Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue une fuite irrémédiable d’informations de l’entité. Si nécessaire des moyens maîtrisés et sécurisés pour l’accès distant à la mess |  |  |  |  |
| 25 | Sécuriser les interconnexions réseau dédiées avec les partenaires | /Standard Pour des besoins opérationnels, une entité peut être amenée à établir une interconnexion réseau dédiée avec un fournisseur ou un client (ex : infogérance, échange de données informatisées, flux monétiques, etc.). Cette interconnexion peut se faire au travers d’un lien sur le réseau privé de l’entité ou directement sur Internet. Dans le second cas, il convient d’établir un tunnel site à site, de préférence IPsec, en respectant les préconisations de l’ANSSI. Le partenaire étant considéré par défaut comme non sûr, il est indispensable d’effectuer un filtrage IP à l’aide d’un pare-feu au plus près de l’entrée des flux sur le réseau de l’entité. La matrice des flux (entrants et sortants) devra être réduite au juste besoin opérationnel, maintenue dans le temps et la configuration des équipements devra y être conforme. /Renforcé Pour des entités ayant des besoins de sécurité plus exigeants, il conviendra de s’assurer que l’équipement de filtrage IP pour les connexions partenaires e |  |  |  |  |
| 26 | Contrôler et protéger l’accès aux salles serveurs et aux locaux techniques | /Standard Les mécanismes de sécurité physique doivent faire partie intégrante de la sécurité des systèmes d’information et être à l’état de l’art afin de s’assurer qu’ils ne puissent pas être contournés aisément par un attaquant. Il convient donc d’identifier les mesures de sécurité physique adéquates et de sensibiliser continuellement les utilisateurs aux risques engendrés par le contournement des règles. Les accès aux salles serveurs et aux locaux techniques doivent être contrôlés à l’aide de serrures ou de mécanismes de contrôle d’accès par badge. Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont à proscrire, sauf s’il est possible de tracer strictement les accès et de limiter ces derniers en fonction des plages horaires. Une revue des droits d’accès doit être réalisée régulièrement afin d’identifier les accès non autorisés. Lors du départ d’un collaborateur ou d’un changement de prestataire, il est nécessaire de procéder au retr |  |  |  |  |
| 27 | Interdire l’accès à Internet depuis les postes ou serveurs utilisés pour l’administration du système | /Standard Un poste de travail ou un serveur utilisé pour les actions d’administration ne doit en aucun cas avoir accès à Internet, en raison des risques que la navigation Web (à travers des sites contenant du code malveillant) et la messagerie (au travers de pièces jointes potentiellement vérolées) font peser sur son intégrité. Pour les autres usages des administrateurs nécessitant Internet (consultation de documentation en ligne, de leur messagerie, etc.), il est recommandé de mettre à leur disposition un poste de travail distinct. À défaut, l’accès à une infrastructure virtualisée distante pour la bureautique depuis un poste d’administration est envisageable. La réciproque consistant à fournir un accès distant à une infrastructure d’administration depuis un poste bureautique est déconseillée car elle peut mener à une élévation de privilèges en cas de récupération des authentifiants d’administration. /Renforcé Concernant les mises à jour logicielles des équipements administrés, elles |  |  |  |  |
| 28 | Utiliser un réseau dédié et cloisonné pour l’administration du système d’information | /Standard Un réseau d’administration interconnecte, entre autres, les postes ou serveurs d’administration et les interfaces d’administration des équipements. Dans la logique de segmentation du réseau global de l’entité, il est indispensable de cloisonner spécifiquement le réseau d’administration, notamment vis-à-vis du réseau bureautique des utilisateurs, pour se prémunir de toute compromission par rebond depuis un poste utilisateur vers une ressource d’administration. Selon les besoins de sécurité de l’entité, il est recommandé : >> de privilégier en premier lieu un cloisonnement physique des réseaux dès que cela est possible, cette solution pouvant représenter des coûts et un temps de déploiement importants ;/Renforcé >> à défaut, de mettre en oeuvre un cloisonnement logique cryptographique reposant sur la mise en place de tunnels IPsec. Ceci permet d’assurer l’intégrité et la confidentialité des informations véhiculées sur le réseau d’administration vis-à-vis du réseau bureautique |  |  |  |  |
| 29 | Limiter au strict besoin opérationnel les droits d’administration sur les postes de travail | /Standard De nombreux utilisateurs, y compris au sommet des hiérarchies, sont tentés de demander à leur service informatique de pouvoir disposer, par analogie avec leur usage personnel, de privilèges plus importants sur leurs postes de travail : installation de logiciels, configuration du système, etc. Par défaut,il est recommandé qu’un utilisateur du SI, quelle que soit sa position hiérarchique et ses attributions, ne dispose pas de privilèges d’administration sur son poste de travail. Cette mesure, apparemment contraignante, vise à limiter les conséquences de l’exécution malencontreuse d’un code malveillant. La mise à disposition d’un magasin étoffé d’applications validées par l’entité du point de vue de la sécurité permettra de répondre à la majorité des besoins. Par conséquent, seuls les administrateurs chargés de l’administration des postes doivent disposer de ces droits lors de leurs interventions. Si une délégation de privilèges sur un poste de travail est réellement nécessaire |  |  |  |  |
| 30 | Prendre des mesures de sécurisation physique des terminaux nomades | /Standard Les terminaux nomades (ordinateurs portables, tablettes, ordiphones) sont, par nature, exposés à la perte et au vol. Ils peuvent contenir localement des informations sensibles pour l’entité et constituer un point d’entrée vers de plus amples ressources du système d’information. Au-delà de l’application au minimum des politiques de sécurité de l’entité, des mesures spécifiques de sécurisation de ces équipements sont donc à prévoir. En tout premier lieu, les utilisateurs doivent être sensibilisés pour augmenter leur niveau de vigilance lors de leurs déplacements et conserver leurs équipements à portée de vue. N’importe quelle entité, même de petite taille, peut être victime d’une attaque informatique. Dès lors, en mobilité, tout équipement devient une cible potentielle voire privilégiée. Il est recommandé que les terminaux nomades soient aussi banalisés que possible en évitant toute mention explicite de l’entité d’appartenance (par l’apposition d’un autocollant aux couleurs de |  |  |  |  |
| 31 | Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable | /Standard Les déplacements fréquents en contexte professionnel et la miniaturisation du matériel informatique conduisent souvent à la perte ou au vol de celui-ci dans l’espace public. Cela peut porter atteinte aux données sensibles de l’entité qui y sont stockées. Il faut donc ne stocker que des données préalablement chiffrées sur l’ensemble des matériels nomades (ordinateurs portables, ordiphones, clés USB, disques durs externes, etc.) afin de préserver leur confidentialité. Seul un secret (mot de passe, carte à puce, code PIN, etc.) pourra permettre à celui qui le possède d’accéder à ces données. Une solution de chiffrement de partition, d’archives ou de fichier peut être envisagée selon les besoins. Là encore, il est essentiel de s’assurer de l’unicité et de la robustesse du secret de déchiffrement utilisé. Dans la mesure du possible, il est conseillé de commencer par un chiffrement complet du disque avant d’envisager le chiffrement d’archives ou de fichiers. En effet, ces derniers |  |  |  |  |
| 32 | Sécuriser la connexion réseau des postes utilisés en situation de nomadisme | /Standard En situation de nomadisme, il n’est pas rare qu’un utilisateur ait besoin de se connecter au système d’information de l’entité. Il convient par conséquent de s’assurer du caractère sécurisé de cette connexion réseau à travers Internet. Même si la possibilité d’établir des tunnels VPN SSL/TLS est aujourd’hui courante, il est fortement recommandé d’établir un tunnel VPN IPsec entre le poste nomade et une passerelle VPN IPsec mise à disposition par l’entité. Pour garantir un niveau de sécurité optimal, ce tunnel VPN IPsec doit être automatiquement établi et ne pas être débrayable par l’utilisateur, c’est-à-dire qu’aucun flux ne doit pouvoir être transmis en dehors de ce tunnel. Pour les besoins spécifiques d’authentification aux portails captifs, l’entité peut choisir de déroger à la connexion automatique en autorisant une connexion à la demande ou maintenir cette recommandation en encourageant l’utilisateur à utiliser un partage de connexion sur un téléphone mobile de confiance |  |  |  |  |
| 33 | Adopter des politiques de sécurité dédiées aux terminaux mobiles | /Standard Les ordiphones et tablettes font partie de notre quotidien personnel et/ou professionnel. La première des recommandations consiste justement à ne pas mutualiser les usages personnel et professionnel sur un seul et même terminal, par exemple en ne synchronisant pas simultanément comptes professionnel et personnel de messagerie, de réseaux sociaux, d’agendas, etc. Les terminaux, fournis par l’entité et utilisés en contexte professionnel doivent faire l’objet d’une sécurisation à part entière, dès lors qu’ils se connectent au système d’information de l’entité ou qu’ils contiennent des informations professionnelles potentiellement sensibles (mails, fichiers partagés, contacts, etc.). Dès lors, l’utilisation d’une solution de gestion centralisée des équipements mobiles est à privilégier. Il sera notamment souhaitable de configurer de manière homogène les politiques de sécurité inhérentes : moyen de déverrouillage du terminal, limitation de l’usage du magasin d’applications à des a |  |  |  |  |
| 34 | Définir une politique de mise à jour des composants du système d’information | /Standard De nouvelles failles sont régulièrement découvertes au coeur des systèmes et logiciels. Ces dernières sont autant de portes d’accès qu’un attaquant peut exploiter pour réussir son intrusion dans le système d’information. Il est donc primordial de s’informer de l’apparition de nouvelles vulnérabilités (CERTFR) et d’appliquer les correctifs de sécurité sur l’ensemble des composants du système dans le mois qui suit leur publication par l’éditeur. Une politique de mise à jour doit ainsi être définie et déclinée en procédures opérationnelles. Celles-ci doivent notamment préciser : >> la manière dont l’inventaire des composants du système d’information est réalisé ; >> les sources d’information relatives à la publication des mises à jour ; >> les outils pour déployer les correctifs sur le parc (par exemple WSUS pour les mises à jour des composants Microsoft, des outils gratuits ou payants pour les composants tiers et autres systèmes d’exploitation) ; >> l’éventuelle qualification d |  |  |  |  |
| 35 | Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles | /Standard L’utilisation d’un système ou d’un logiciel obsolète augmente significativement les possibilités d’attaque informatique. Les systèmes deviennent vulnérables dès lors que les correctifs ne sont plus proposés. En effet, des outils malveillants exploitant ces vulnérabilités peuvent se diffuser rapidement sur Internet alors même que l’éditeur ne propose pas de correctif de sécurité. Pour anticiper ces obsolescences, un certain nombre de précautions existent : >> établir et tenir à jour un inventaire des systèmes et applications du système d’information ; >> choisir des solutions dont le support est assuré pour une durée correspondant à leur utilisation ; >> assurer un suivi des mises à jour et des dates de fin de support des logiciels ; >> maintenir un parc logiciel homogène (la coexistence de versions différentes d’un même produit multiplie les risques et complique le suivi) ; >> limiter les adhérences logicielles, c’est-à-dire les dépendances de fonctionnement d’un logiciel par |  |  |  |  |
| 36 | Activer et configurer les journaux des composants les plus importants | /Standard Disposer de journaux pertinents est nécessaire afin de pouvoir détecter d’éventuels dysfonctionnements et tentatives d’accès illicites aux composants du système d’information. La première étape consiste à déterminer quels sont les composants critiques du système d’information. Il peut notamment s’agir des équipements réseau et de sécurité, des serveurs critiques, des postes de travail d’utilisateurs sensibles, etc. Pour chacun, il convient d’analyser la configuration des éléments journalisés (format, fréquence de rotation des fichiers, taille maximale des fichiers journaux, catégories d’évènements enregistrés, etc.) et de l’adapter en conséquence. Les évènements critiques pour la sécurité doivent être journalisés et gardés pendant au moins un an (ou plus en fonction des obligations légales du secteur d’activités). Une étude contextuelle du système d’information doit être effectuée et les éléments suivants doivent être journalisés : >> pare-feu : paquets bloqués ; >> systèmes |  |  |  |  |
| 37 | Définir et appliquer une politique de sauvegarde des composants critiques | /Standard Suite à un incident d’exploitation ou en contexte de gestion d’une intrusion, la disponibilité de sauvegardes conservées en lieu sûr est indispensable à la poursuite de l’activité. Il est donc fortement recommandé de formaliser une politique de sauvegarde régulièrement mise à jour. Cette dernière a pour objectif de définir des exigences en matière de sauvegarde de l’information, des logiciels et des systèmes. Cette politique doit au moins intégrer les éléments suivants : >> la liste des données jugées vitales pour l’organisme et les serveurs concernés ; >> les différents types de sauvegarde (par exemple le mode hors ligne) ; >> la fréquence des sauvegardes ; >> la procédure d’administration et d’exécution des sauvegardes ; >> les informations de stockage et les restrictions d’accès aux sauvegardes ; >> les procédures de test de restauration ; >> la destruction des supports ayant contenu les sauvegardes. Les tests de restauration peuvent être réalisés de plusieurs manières : > |  |  |  |  |
| 38 | Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives asso | /Renforcé La réalisation d’audits réguliers (au moins une fois par an) du système d’information est essentielle car elle permet d’évaluer concrètement l’efficacité des mesures mises en oeuvre et leur maintien dans le temps. Ces contrôles et audits permettent également de mesurer les écarts pouvant persister entre la règle et la pratique. Ils peuvent être réalisés par d’éventuelles équipes d’audit internes ou par des sociétés externes spécialisées. Selon le périmètre à contrôler, des audits techniques et/ou organisationnels seront effectués par les professionnels mobilisés. Ces audits sont d’autant plus nécessaires que l’entité doit être conforme à des réglementations et obligations légales directement liées à ses activités. À l’issue de ces audits, des actions correctives doivent être identifiées, leur application planifiée et des points de suivi organisés à intervalles réguliers. Pour une plus grande efficacité, des indicateurs sur l’état d’avancement du plan d’action pourront être in |  |  |  |  |
| 39 | Désigner un référent en sécurité des systèmes d’information et le faire connaître auprès du personne | /Standard Toute entité doit disposer d’un référent en sécurité des systèmes d’information qui sera soutenu par la direction ou par une instance décisionnelle spécialisée selon le niveau de maturité de la structure. Ce référent devra être connu de tous les utilisateurs et sera le premier contact pour toutes les questions relatives à la sécurité des systèmes d’information : >> définition des règles à appliquer selon le contexte ; >> vérification de l’application des règles ; >> sensibilisation des utilisateurs et définition d’un plan de formation des acteurs informatiques ; >> centralisation et traitement des incidents de sécurité constatés ou remontés par les utilisateurs. Ce référent devra être formé à la sécurité des systèmes d’information et à la gestion de crise. Dans les entités les plus importantes, ce correspondant peut être désigné pour devenir le relais du RSSI. Il pourra par exemple signaler les doléances des utilisateurs et identifier les thématiques à aborder dans le cadre d |  |  |  |  |
| 40 | Définir une procédure de gestion des incidents de sécurité | /Standard Le constat d’un comportement inhabituel de la part d’un poste de travail ou d’un serveur (connexion impossible, activité importante, activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation, multiples alertes de l’antivirus, etc.) peut alerter sur une éventuelle intrusion. Une mauvaise réaction en cas d’incident de sécurité peut faire empirer la situation et empêcher de traiter correctement le problème. Le bon réflexe est de déconnecter la machine du réseau, pour stopper l’attaque. En revanche, il faut la maintenir sous tension et ne pas la redémarrer, pour ne pas perdre d’informations utiles pour l’analyse de l’attaque. Il faut ensuite prévenir la hiérarchie, ainsi que le référent en sécurité des systèmes d’information. Celui-ci peut prendre contact avec un prestataire de réponse aux incidents de sécurité (PRIS) afin de faire réaliser les opérations techniques nécessaires (copie physique du disque, analyse de la mémoire |  |  |  |  |
| 41 | Mener une analyse de risques formelle | /Renforcé Chaque entité évolue dans un environnement informationnel complexe qui lui est propre. Aussi, toute prise de position ou plan d’action impliquant la sécurité du système d’information doit être considéré à la lumière des risques pressentis par la direction. En effet, qu’il s’agisse de mesures organisationnelles ou techniques, leur mise en oeuvre représente un coût pour l’entité qui nécessite de s’assurer qu’elles permettent de réduire au bon niveau un risque identifié. Dans les cas les plus sensibles, l’analyse de risque peut remettre en cause certains choix passés. Ce peut notamment être le cas si la probabilité d’apparition d’un événement et ses conséquences potentielles s’avèrent critiques pour l’entité et qu’il n’existe aucune action préventive pour le maîtriser. La démarche recommandée consiste, dans les grandes lignes, à définir le contexte, apprécier les risques et les traiter. L’évaluation de ces risques s’opère généralement selon deux axes : leur probabilité d’apparit |  |  |  |  |
| 42 | Privilégier l’usage de produits et de services qualifiés par l’ANSSI | /Renforcé La qualification prononcée par l’ANSSI offre des garanties de sécurité et de confiance aux acheteurs de solutions listées dans les catalogues de produits et de prestataires de service qualifiés que publie l’agence. Au-delà des entités soumises à réglementation, l’ANSSI encourage plus généralement l’ensemble des entreprises et administrations françaises à utiliser des produits qu’elle qualifie, seul gage d’une étude sérieuse et approfondie du fonctionnement technique de la solution et de son écosystème. S’agissant des prestataires de service qualifiés, ce label permet de répondre aux enjeux et projets de cybersécurité pour l’ensemble du tissu économique français que l’ANSSI ne saurait adresser seule. Évalués sur des critères techniques et organisationnels, les prestataires qualifiés couvrent l’essentiel des métiers de la sécurité des systèmes d’information. Ainsi, en fonction de ses besoins et du maillage national, une entité pourra faire appel à un Prestataire d’audit de la s |  |  |  |  |

# Activité 2 (Source de risque)

## Activité 2.a (Identifier les sources de risques et les objectifs)

Sources de risque et objectifs visés

| **Type d'ttaquant** | **Profil d'attaquant** | **Description source de risque** | **Objectif visé** | **Description de l'objectif** |
| --- | --- | --- | --- | --- |
| Organisation idéologique | Amateur | Desc SR | MonOOV | Desc OV |
| Individu isolé | Le voisin | Des SR | Voler le mot de passe | Desc OV |
| Organisation structurée | Anonymous | Groupe de hacker très bien organisé | Se faire connaitre | Faire le buzz |
| Organisation idéologique | Anonymous | Groupe structuré de hacker | Attaquer le capitalisme | Objectif faire tomber les grands sociétés commerciales |

**Activité 2 (Source de risque)**

## Activité 2.b (Évaluer les couples sources de risque/objectifs visés)

Évaluation des sources de risques

${p\_srov2}

**Activité 2 (Source de risque)**

## Activité 2.c (Sélectionner les couples SR/OV retenus pour la suite de l’analyse)

Choix des sources de risque

| **Profil d'attaquant** | **Description source du risque** | **Objectif visé** | **Description de l'objectif** | **Motivation** | **Ressources** | **Activité** | **Mode opératoire** | **Secteur d'activité** | **Arsenal d'attaque** | **Fait d'armes** | **Pertinence** | **Choix P1/P2** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Amateur | Desc SR | MonOOV | Desc OV | 1 | 1 | 1 |  |  |  |  | Faible | P2 |
| Le voisin | Des SR | Voler le mot de passe | Desc OV | 1 | 1 | 1 |  |  |  |  | Faible | P2 |
| Anonymous | Groupe de hacker très bien organisé | Se faire connaitre | Faire le buzz | 3 | 3 | 3 |  |  |  |  | Élevée | P1 |
| Anonymous | Groupe structuré de hacker | Attaquer le capitalisme | Objectif faire tomber les grands sociétés commerciales | 3 | 3 | 3 |  |  |  |  | Élevée | P1 |

**Activité 2 (Source de risque)**

Activité 2.c (Sélectionner les couples SR/OV retenus pour la suite de l’analyse)

Cartographie des "Source de risque / Objectif visé"

${Cartographie1}

# **Activité 3 (Scénarios stratégiques)**

## Activité 3.a (Construire la cartographie des menaces numériques de l'écosystème et sélectionner les parties prenantes critiques)

Création des seuils (q\_seuil)

Seuil de danger : ${danger}

Seuil de contrôle : ${contrôle}

Seuil de veille : ${veille}

**Activité 3 (Scénarios stratégiques)**

Activité 3.a (Construire la cartographie des menaces numériques de l'écosystème et sélectionner les parties prenantes critiques)

Parties prenantes

${r\_partie\_prenante1}

Parties prenantes internes

${Cartographie2}

Parties prenantes externes

${Cartographie3}

**Activité 3 (Scénarios stratégiques)**

## Activité 3.b (Élaborer des scénarios stratégiques)

Liste des évènements redoutés établis à l'atelier 1.c

${ m\_evenement\_redoute}

**Activité 3 (Scénarios stratégiques)**

Activité 3.b (Élaborer des scénarios stratégiques)

Liste des couples sources de risques / objectifs visés retenus établis à l'atelier 2

${p\_srov4}

**Activité 3 (Scénarios stratégiques)**

Activité 3.b (Élaborer des scénarios stratégiques)

Scénarios stratégiques

${s\_scenario\_strategique1}

**Activité 3 (Scénarios stratégiques)**

Activité 3.b (Élaborer des scénarios stratégiques)

Chemins d'attaque

${t\_chemin\_d\_attaque\_strategique}

**Activité 3 (Scénarios stratégiques)**

## Activité 3.c (Définir des mesures de sécurité sur l'écosystème)

Liste des parties prenantes établis à l'atelier 3.a

${r\_partie\_prenante2}

**Activité 3 (Scénarios stratégiques)**

Activité 3.c (Définir des mesures de sécurité sur l'écosystème)

Liste des scénarios stratégiques établis à l'atelier 3.b

${s\_scenario\_strategique2}

# Activité 4 (Scénarios opérationnels)

## Activité 4.a (Élaborer les scénarios opérationnels)

Liste des scénarios stratégiques établis lors de l'atelier 3.b

${s\_scenario\_strategique3}

**Activité 4 (Scénarios opérationnels)**

## Activité 4.b (Évaluer la vraisemblance des scénarios opérationnels)

Niveaux des échelles de vraisemblance

${da\_echelle}

**Activité 4 (Scénarios opérationnels)**

Activité 4.b (Évaluer la vraisemblance des scénarios opérationnels)

Niveaux des échelles de vraisemblance

${u\_scenario\_operationnel}

# Activité 5 (Traitement du risque)

## Activité 5.a (Réaliser une synthèse des scénarios de risque)

Cartographie du risque initial

${Cartographie4}

**Activité 5 (Traitement du risque)**

## Activité 5.b (Décider de la stratégie de traitement du risque et définir les mesures de sécurité)

Plan d'amélioration continue de la sécurité

${za\_traitement\_de\_securite}

**Activité 5 (Traitement du risque)**

## Activité 5.c (Évaluer et documenter les risques résiduels)

Évaluation et documentation des risques résiduels

$ {x\_revaluation\_du\_risque}