GUIDE PRATIQUE RGPD

SÉCURITÉ DES DONNÉES PERSONNELLES

Version 2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

L'objectif de ce guide est d'accompagner les organismes dans la mise en place de mesures de sécurité pour assurer la protection des données personnelles qu'ils traitent.

Il s'adresse notamment aux délégués à la protection des données (DPD), aux responsables de la sécurité des systèmes d'information (RSSI) et aux informaticiens. Les juristes en protection de la vie privée pourront également y trouver des éléments utiles.

Ce guide est un outil vivant qui est enrichi des pratiques à l'état de l'art et des éléments de doctrine de la Commission nationale de l'informatique et des libertés (CNIL) sur la question de la sécurité des données.

Un journal des modifications est disponible sur le site de la CNIL pour aider les acteurs à repérer les évolutions à prendre en compte afin d'adapter leur niveau de sécurité.

TABLE DES MATIÈRES

AVANT-PROPOS

La sécurité est un élément essentiel de la protection des données personnelles. Elle s'impose à tout responsable de traitement et sous-traitant à travers l'article 32 du règlement général sur la protection des données[1] (RGPD). En principe, chaque traitement doit faire l'objet d'un ensemble de mesures de sécurité décidées en fonction du contexte, à savoir « ***des précautions utiles, au regard de la nature des données et des risques*** *présentés par le traitement* » (article 121 de la loi Informatique et Libertés[2]). Le RGPD précise que la protection des données personnelles nécessite de prendre les « *mesures techniques et organisationnelles appropriées afin de garantir un* ***niveau de sécurité adapté au risque*** » pour les droits et libertés des personnes physiques, notamment leur vie privée.

Pour évaluer les mesures à mettre en place, deux approches complémentaires sont à déployer :

- **la mise en place d'un socle de sécurité** reprenant les bonnes pratiques issues d'années de capitalisation d'hygiène et de sécurité informatique (ex. : règlementations, normes, guides). Ce socle vise à répondre aux risques les plus courants ;
- **l'analyse des risques[3] pour les personnes** concernées par le traitement qui vise à identifier et évaluer les risques spécifiques au traitement. Une telle analyse permet d'étayer la prise de décision objective sur le traitement de ces risques et la détermination de mesures nécessaires et adaptées au contexte.

Il est cependant difficile, pour les non-spécialistes de la sécurité informatique, de mettre en œuvre une telle démarche et de s'assurer que le niveau de sécurité des traitements dont ils sont responsables est suffisant.

Pour aider dans la mise en conformité, ce guide présente un ensemble de préconisations regroupées par fiches thématiques. Chaque fiche est structurée en trois sections :

- les **précautions élémentaires**, qui reprennent les bonnes pratiques essentielles ;
- les **mauvaises pratiques tendancielles**, qui devraient être évitées ;
- les **mesures complémentaires**, pour aller plus loin[4].

Chaque fiche peut être lue séparément des autres : des renvois sont indiqués quand une autre fiche apporte plus de précisions sur un élément.

1 « Le règlement général sur la protection des données - RGPD », cnil.fr

2 « La loi Informatique et Libertés », cnil.fr

3 Elle est en particulier indispensable lorsque le traitement doit faire l'objet d'une analyse d'impact relative à la protection des données ou AIPD (voir « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) », cnil.fr).

4 Ces mesures pourront avec le temps et la pratique devenir des précautions élémentaires.

FICHE 1 - PILOTER LA SÉCURITÉ DES DONNÉES

Mettre en place et maintenir dans la durée la protection des données personnelles exigée par le RGPD et les cadres sectoriels.

L'intégration de la protection des données personnelles dans les processus de décision de l'organisme permet d'en assurer la prise en compte dans la durée et aux moments clés d'arbitrages des budgets et des projets.

Les précautions élémentaires

- **Impliquer la direction** et formaliser des objectifs généraux en matière de sécurité et de protection des données personnelles, validés par la direction de l'organisme.
- **Recenser** (à travers le registre[5]) **les traitements de données personnelles**, automatisés ou non, les données traitées (ex. : fichiers clients, contrats) et les supports sur lesquels ces traitements reposent :
  - les matériels (ex. : serveurs, ordinateurs portables, disques durs) ;
  - les logiciels (ex. : systèmes d'exploitation, logiciels métier) ;
  - les ressources d'informatique en nuage (*cloud*) utilisés (ex. : SaaS, PaaS, IaaS) ;
  - les canaux de communication logiques ou physiques (ex. : connexions filaires, Wi-Fi, Internet, échanges verbaux, coursiers) ;
  - les supports papier (ex. : documents imprimés, photocopies) ;
  - les locaux et installations physiques où se situent les éléments précédemment cités (ex. : locaux informatiques, bureaux).

  Formaliser des schémas d'interconnexions et de flux de données entre les différents composants des systèmes d'information. Le registre et les schémas doivent être mis à jour lors de chaque modification structurelle des traitements ou des composants des systèmes d'information.
- **Définir un plan d'action relatif à la sécurité informatique et mettre en œuvre les mesures techniques et organisationnelles définies** pour assurer la protection des données. Pour ce faire, deux approches complémentaires peuvent être mises en œuvre : d'une part, mettre en place les précautions élémentaires listées dans le présent guide (voir la check-list d'évaluation) et, d'autre part, compléter par des mesures spécifiques identifiées à l'aide d'analyses de risques[6] (voir la fiche n°20 - Analyse de risques). Toute nouvelle mesure décidée doit intégrer le plan d'action dont l'avancement est suivi régulièrement.
- **Contrôler périodiquement l'effectivité des mesures** techniques et organisationnelles pour s'assurer qu'elles remplissent bien l'objectif poursuivi (ex. : par la mise en place d'indicateurs). Vérifier en priorité les mesures mises en œuvre pour corriger des vulnérabilités identifiées ou pour prévenir des incidents qui se sont déjà produits.
- **Assurer un suivi avec la direction** en termes de gestion de risques informatiques à travers une revue de direction au moins annuelle. Elle doit permettre d'établir une synthèse et de prendre des décisions considérant :

5 « Le registre des activités de traitement », cnil.fr

6 L'article 35 du RGPD impose de mener une analyse d'impact relative à la protection des données (AIPD) pour certains types de traitements (voir « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) », cnil.fr).

- l'évolution du contexte, des enjeux et des attentes des parties prenantes (ex. : clients, partenaires, autorités de contrôle) ;
- le changement des objectifs et missions de l'organisme ;
- l'évolution de la menace numérique ;
- l'essor de nouvelles technologies ou solutions de sécurité ;
- les évolutions des systèmes d'information et des traitements de données ;
- l'évolution des risques sur la sécurité des données et la vie privée ;
- l'avancement du plan d'action juridique (ex. : mise en conformité des contrats) et technique (mesures de sécurité) ;
- les incidents et violations rencontrés, avec leur impact sur l'organisme et les personnes concernées ;
- les demandes et plaintes reçues et traitées concernant les données personnelles.

• **Améliorer la protection des données personnelles dans le temps**. La revue de direction doit notamment permettre de décider de l'allocation des moyens humains et budgétaires nécessaires aux mesures à mettre en place et à l'amélioration continue de la sécurité.

Ce qu'il ne faut pas faire

- Considérer la sécurité comme un problème accessoire pouvant être pris en compte a posteriori, une fois les traitements de données déjà opérationnels.
- Se concentrer sur des mesures avancées sans avoir mis en place les précautions élémentaires.
- Se limiter à des actions ponctuelles et ne pas considérer le traitement de données dans son ensemble (ex. : collecte, partenaires, fin de vie des données) pour décider des mesures de sécurité à mettre en place.
- Se reposer uniquement sur des mesures techniques sans les accompagner de mesures organisationnelles en cohérence.
- Définir un plan d'action sans attribuer d'échéance et de responsable de mise en œuvre à chaque action.
- Déléguer la gestion de toute la sécurité informatique à un fournisseur.

POUR ALLER PLUS LOIN

- Afin d'assurer le suivi de la sécurité et de la protection des données au quotidien, il est très utile (voire obligatoire selon la nature de l'organisme) de **nommer une personne responsable de la sécurité des systèmes d'information (RSSI) et un délégué à la protection des données**[7] **(DPD)**. Ils doivent :
  - avoir la capacité de **rapporter directement au niveau le plus élevé de la direction** ;
  - **disposer des ressources nécessaires et des conditions de travail** pour exercer leurs missions ;
  - **être impliqués** (eux-mêmes ou leur équipe) systématiquement et en amont dans les réflexions sur les questions relatives à leur champ de compétences afin d'assurer une sécurité des systèmes d'information et la protection des données personnelles **dès la conception et par défaut**.
- Les objectifs généraux en matière de protection des données personnelles peuvent être consignés dans une politique générale de protection des données, portée par la direction et diffusée à l'ensemble des acteurs (personnels, sous-traitants, partenaires). Cette politique peut ensuite être précisée à un niveau opérationnel en politiques thématiques et procédures détaillées pour décliner au contexte d'activité de l'organisme les mesures de protection des données personnelles.
- **Les audits de sécurité sont un moyen essentiel pour évaluer le niveau de sécurité des systèmes sur lesquels reposent le(s) traitement(s) de données personnelles.** Réalisés de façon périodique, ils permettent de prendre en compte les évolutions du traitement et des menaces. Chaque audit doit donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.
- Afin de structurer la gouvernance dans la durée, il est possible de mettre en place un système de management reposant sur une démarche d'amélioration continue. La norme internationale ISO/IEC 27701[8] décrit les processus et les mesures organisationnelles et techniques permettant de mettre en place un système de management de la protection de la vie privée (PIMS, en anglais), en s'appuyant sur le système de management de la sécurité de l'information (SMSI) porté par la norme ISO/IEC 27001.
- L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié son propre guide[9] des bonnes pratiques en termes de sécurité informatique.

7 « Devenir délégué à la protection des données », cnil.fr

8 « L'ISO 27701, une norme internationale pour la protection des données personnelles », cnil.fr

9 « Guide d'hygiène informatique », cyber.gouv.fr

LES UTILISATEURS

FICHE 2 - DÉFINIR UN CADRE POUR LES UTILISATEURS

Donner une force contraignante aux principales règles d'usage des outils informatiques.

Les utilisateurs ont un usage souvent quotidien de l'outil informatique. Leurs pratiques peuvent avoir un impact direct sur la sécurité des données personnelles et doivent donc être encadrées.

Les précautions élémentaires

- **Rédiger une charte informatique et lui donner une force contraignante** (ex. : annexion au règlement intérieur).
- **Inclure dans la charte** au moins les éléments suivants :

1. Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.
2. Le champ d'application de la charte, qui inclut notamment :
   - les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme ;
   - les moyens d'authentification utilisés par l'organisme et la politique de mots de passe que l'utilisateur doit respecter ;
   - les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment de :
     - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique, toute perte ou vol de matériel et, de manière générale, tout dysfonctionnement ;
     - ne jamais confier son mot de passe (ou équivalent) à un tiers ;
     - ne pas installer, copier, modifier, détruire des logiciels et leur paramétrage sans autorisation ;
     - verrouiller (ou éteindre) son ordinateur dès que l'on quitte son poste de travail ;
     - ne pas accéder, tenter d'accéder à des informations ou les supprimer si cela ne relève pas des tâches incombant à l'utilisateur ;
     - respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.
3. Les modalités d'utilisation des moyens informatiques et de télécommunication mis à disposition comme :
   - le poste de travail ;
   - les équipements nomades (notamment dans le cadre du télétravail) ;
   - les espaces de stockage individuel ;
   - les réseaux locaux ;
   - les conditions d'utilisation des dispositifs personnels ;
   - l'accès à Internet ;
   - la messagerie électronique ;
   - la téléphonie.

4. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de :
   - systèmes automatiques de filtrage ;
   - systèmes automatiques dédiés à la traçabilité des actions ;
   - systèmes de gestion du poste de travail.
5. Les responsabilités et sanctions encourues en cas de non-respect de la charte.

Ce qu'il ne faut pas faire

- Ne pas donner de force contraignante à la charte ou ne pas l'appliquer et la faire appliquer en cas de manquement.
- Ne pas tenir compte des pratiques réelles des usagers, de leurs attentes et de leurs besoins en définissant les règles d'usage des moyens informatiques : l'informatique fantôme (ou « *shadow IT* » en anglais) révèle parfois des besoins essentiels non pourvus par l'organisme ou un dysfonctionnement structurel.
- Ne pas accompagner les usagers dans leurs pratiques.

POUR ALLER PLUS LOIN

- Prévoir la signature d'un **engagement de confidentialité** (voir exemple de clause ci-dessous), ou prévoir dans les contrats de travail une **clause de confidentialité spécifique** concernant les données personnelles.
- Prévoir une charte spécifique pour les administrateurs qui détaille les exigences complémentaires que cette population particulièrement à risque doit respecter.

Exemple de clause d'engagement de confidentialité pour les personnes ayant vocation à manipuler des données personnelles

Je soussigné/e Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément à l'article 32 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes à l'état de l'art et aux règles internes dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :
- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes à l'état de l'art et aux règles internes dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes à l'état de l'art et aux règles internes pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, après la cessation de mes fonctions, quelle qu'en soit la cause et tant que les données n'auront pas été rendues publiques par la Société, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.
J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la règlementation en vigueur, notamment au regard des articles 226-13 et 226-16 à 226-24 du code pénal.

Fait à xxx, le xxx, en xxx exemplaires

Nom :
Signature :

FICHE 3 – IMPLIQUER ET FORMER LES UTILISATEURS

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée.

Les erreurs humaines et les attaques par ingénierie sociale sont à l'origine d'un nombre important d'incidents de sécurité. Les solutions techniques ne sont pas suffisantes pour assurer la protection des données personnelles détenues par un organisme.

Les précautions élémentaires

- **Sensibiliser les utilisateurs (aussi bien internes qu'externes à l'organisme) travaillant avec des données personnelles aux risques liés aux libertés et à la vie privée des personnes**, les informer des mesures prises pour traiter ces risques et des conséquences potentielles en cas de manquement. Concrètement, il peut s'agir :
  - d'organiser des séances de sensibilisation sur les risques, les principaux types d'attaques (ex. : hameçonnage ou « *phishing* », rançongiciel ou « *ransomware* », usurpation d'identité), la vigilance nécessaire (ex. : avant d'ouvrir une pièce jointe ou de cliquer sur un lien dans un message, lorsqu'on répond au téléphone) et la conduite à tenir en cas d'incident ou de suspicion (mesures de protection et d'alerte) ;
  - de faire des rappels réguliers et en fonction de l'actualité de l'organisme (ex. : tentative de hameçonnage récente, arrivée d'un nouveau prestataire) des consignes.
- Déployer différentes campagnes de sensibilisation dont **le contenu et le langage sont adaptés aux fonctions des destinataires.** Par exemple, les ressources humaines doivent être sensibilisées aux données qu'elles manipulent et les employés qui interviennent à l'extérieur, aux risques particuliers du nomadisme.
- S'assurer que les personnels en charge de traitements de données personnelles (ex. : ceux en charge du traitement de réclamations ou de documents administratifs) ont bien assimilé les bonnes pratiques relatives à la protection des données personnelles à mettre en œuvre au quotidien (ex. : évaluation des connaissances).
- Former les personnels en charge des outils informatiques (ex. : ceux en charge de la conception et de la maintenance) à la sécurité informatique et à la protection des données personnelles.
- **Documenter les procédures d'exploitation**, les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur un traitement de données personnelles, qu'il s'agisse d'une opération d'administration ou de la simple utilisation d'une application, doit être expliquée dans un langage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuvent se référer.

Ce qu'il ne faut pas faire

- Imposer des outils informatiques sans accompagner leur adoption par les équipes.
- Ne pas imposer de session obligatoire sur la protection des données personnelles à tout nouvel arrivant, quand l'activité principale de l'organisme traite des données personnelles (ex. : établissement de santé, service client).
- Sous-estimer l'impact positif que des collaborateurs bien sensibilisés peuvent avoir sur la sécurité informatique de l'organisme.
- Ne pas veiller à la sensibilisation des prestataires extérieurs (par action directe ou par engagement contractuel) quand leur impact sur la sécurité des données peut être aussi important que celui des collaborateurs internes.

POUR ALLER PLUS LOIN

- Mettre en place une politique et des outils de **classification de l'information** définissant plusieurs niveaux (ex. : public, interne, confidentiel) et imposant un marquage des documents, des supports et des e-mails contenant des données confidentielles.
- Ajouter une mention visible et explicite sur chaque page des documents papier ou électroniques qui contiennent des données sensibles[10].
- Organiser des **exercices et des simulations d'incidents de sécurité informatique** ou de crises (avec l'organisation préalable et l'encadrement nécessaires à tout exercice de sécurité). Ces exercices permettent de vérifier la bonne prise en compte des consignes et l'efficacité des procédures en place en matière de gestion des incidents et de crise. La consolidation des retours d'expérience permet d'identifier les messages à renforcer et les procédures à améliorer.

10 Les données sensibles sont décrites à l'article 6 de la loi Informatique et Libertés et à l'article 9 du RGPD.

FICHE 4 - AUTHENTIFIER LES UTILISATEURS

Reconnaître les utilisateurs pour pouvoir, ensuite, leur donner les accès nécessaires.

Avant toute utilisation des moyens informatiques, un utilisateur doit être doté d'un **identifiant qui lui est propre** et doit **s'authentifier** afin de permettre de contrôler son identité et ses accès aux données dont il a besoin.

Les mécanismes permettant de réaliser l'authentification des personnes sont catégorisés selon qu'ils font intervenir :

- **un facteur de connaissance** (ce que l'on sait), par exemple un mot de passe ;
- **un facteur de possession** (ce que l'on a), par exemple une carte à puce ;
- **un facteur inhérent** (ce que l'on est), par exemple une empreinte digitale ou une manière de frapper au clavier[11]. Pour rappel, le traitement de données biométriques visant à identifier un individu automatiquement et de manière unique à partir de ses caractéristiques physiques, physiologiques ou comportementales est un traitement de données sensibles donnant lieu à l'application de l'article 9 du RGPD[12].

L'authentification d'un utilisateur est qualifiée de **multifacteur** lorsqu'elle a recours à une combinaison **d'au moins deux** facteurs de catégories distinctes. Elle est dite **robuste** si elle repose sur un mécanisme cryptographique dont les paramètres et la sécurité sont jugés robustes (ex. : clé cryptographique).

Les précautions élémentaires

- **Définir un identifiant unique par utilisateur et interdire les comptes partagés** entre plusieurs utilisateurs. Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, exiger une validation de la hiérarchie, mettre en œuvre des moyens pour tracer les actions associées à ces identifiants et renouveler le mot de passe dès qu'une personne n'a plus besoin d'accéder au compte.
- **Respecter la recommandation de la CNIL[13] dans le cas d'une authentification des utilisateurs basée sur des mots de passe,** notamment en appliquant les règles suivantes :
  - **stocker uniquement l'empreinte des mots de passe, obtenue selon des techniques à l'état de l'art ;**
  - ne pas demander le renouvellement périodique des mots de passe pour les simples utilisateurs (au contraire des administrateurs) ;
  - obliger l'utilisateur à **changer**, dès sa première connexion, **tout mot de passe attribué automatiquement ou par un administrateur** lors de la création du compte ou d'un renouvellement du mot de passe ;

11 La biométrie comportementale (ex. : frappe au clavier) est moins mature que la biométrie physiologique (ex. : empreinte digitale).

12 En matière d'authentification sur le lieu de travail, cela se traduit par l'obligation, pour tout responsable de traitement souhaitant mettre en œuvre un tel traitement, de se conformer aux dispositions du règlement type relatif à l'accès par authentification biométrique sur les lieux de travail (voir « Le contrôle d'accès biométrique sur les lieux de travail », cnil.fr).

13 « Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité », cnil.fr

- imposer une **complexité du mot de passe** en fonction des cas d'usage :
  - **par défaut, entropie**[14] (imprédictibilité théorique) **minimale de 80 bits** (ex. : 12 caractères minimum comportant des majuscules, des minuscules, des chiffres et des caractères spéciaux ; 14 caractères minimum comportant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire) ;
  - entropie de 50 bits (ex. : 8 caractères minimum de 3 types différents ; 16 chiffres) dans le cas où des mesures complémentaires sont en place (restriction de l'accès au compte telle qu'une temporisation de l'accès après plusieurs échecs, la mise en place de « Captcha » ou le blocage du compte après 10 échecs) ;
  - entropie de 13 bits (ex. : 4 chiffres) dans le cas d'un matériel détenu par l'utilisateur (ex. : carte SIM, dispositif contenant un certificat) avec blocage au bout de 3 échecs.

- **Accompagner les utilisateurs pour le choix d'un mot de passe robuste :**
  - en sensibilisant sur les **moyens mnémotechniques**[15] ;
  - en incitant à l'utilisation de **gestionnaires de mots de passe**[16] et en formant à leur utilisation :
    - il permet d'enregistrer de façon sécurisée autant de mots de passe que nécessaire tout en n'exigeant la mémorisation que d'un seul mot de passe maître ;
    - le mot de passe maître doit par conséquent être particulièrement robuste ;
    - une attention particulière doit être apportée au choix de la solution.
- **Communiquer sur les pratiques interdites**[17] (ex. : communiquer son mot de passe à une autre personne, utiliser un mot de passe pouvant être déduit du contexte dans lequel il est utilisé, enregistrer les mots de passe dans un navigateur sans mot de passe maître). **Un mot de passe respectant l'entropie exigée peut toujours être facilement utilisé par un attaquant en cas de mauvaises pratiques**.

Ce qu'il ne faut pas faire

- Utiliser les mots de passe par défaut des équipements et logiciels.
- Conserver les mots de passe en clair et non une empreinte cryptographique.
- Utiliser, pour la génération de l'empreinte des mots de passe à stocker, une fonction cryptographique de hachage obsolète, telle que MD5 ou SHA-1 (voir la fiche n°21 - Chiffrement, hachage, signature), ou conçue en interne qui est, par conséquent, non reconnue ou éprouvée.
- Empêcher l'usage de la fonction « Coller » ou de l'auto-complétion dans les formulaires pour ne pas impacter l'utilisation d'un gestionnaire de mots de passe.

14 L'entropie, appliquée à un mot de passe, correspond à sa capacité de résistance à une attaque par force brute. À titre d'exemple, pour le code secret d'une carte bancaire, le nombre de combinaisons possibles est égal à 10 (chiffres possibles) à la puissance 4 (10^4). En binaire, pour obtenir un nombre de combinaisons équivalent, il faut utiliser 13 bits, car 2 (bits possibles) à la puissance 13 (2^{13}) vaut 8 192, ce qui est du même ordre de grandeur que 10^4. On parle alors d'une entropie de 13 bits.

15 « Générer un mot de passe solide », cnil.fr

16 « 5 arguments pour adopter le gestionnaire de mots de passe », cnil.fr

17 « Les conseils de la CNIL pour un bon mot de passe », cnil.fr

POUR ALLER PLUS LOIN

- **Privilégier l'authentification multifacteur** lorsque cela est possible, en particulier lorsque la connexion est accessible depuis l'extérieur du réseau de l'organisme.
- **Limiter le nombre de tentatives d'accès** aux comptes utilisateurs sur les postes de travail et bloquer l'accès au compte temporairement ou non, lorsque sa limite est atteinte.
- **Imposer, pour les administrateurs, une entropie des mots de passe plus élevée et un renouvellement** selon une périodicité pertinente et raisonnable.
- Mettre en œuvre des moyens techniques pour **faire respecter les règles relatives à l'authentification** (ex. : blocage du compte en cas de non-renouvellement du mot de passe d'un administrateur).
- La CNIL met à disposition sur son site web un outil[18] pour calculer la complexité des mots de passe demandés aux utilisateurs, selon chaque cas d'usage (mot de passe seul, avec restriction d'accès ou avec un matériel détenu par la personne).
- Éviter, si possible, que les identifiants (ou « *logins* ») des utilisateurs et ceux des administrateurs soient ceux des comptes définis par défaut par les éditeurs de logiciels et désactiver les comptes par défaut.
- **Stocker les mots de passe de façon sécurisée** transformés (« *hash* ») avec une fonction spécifiquement conçue à cette fin et utilisant toujours un sel ou une clé[19] (voir la fiche n°21 - Chiffrement, hachage, signature). Une clé ne doit pas être stockée dans la même base de données que les empreintes générées.
- L'ANSSI a publié avec la collaboration de la CNIL[20] des recommandations relatives à l'authentification multifacteur et aux mots de passe. Se référer également aux guides[21] publiés par l'ANSSI pour aider les développeurs et administrateurs dans leurs choix d'algorithmes cryptographiques, de dimensionnement et d'implémentation.
- Pour les autorités administratives, les annexes du référentiel général de sécurité (RGS)[22] s'appliquent, notamment les annexes B1 et B2 concernant respectivement les mécanismes cryptographiques et la gestion des clés utilisées.

18 « Vérifier sa politique de mots de passe », cnil.fr

19 On appelle « sel » l'aléa utilisé lorsqu'il est différent pour chaque mot de passe stocké et « clé » lorsque l'aléa utilisé est commun à la transformation d'un ensemble de mots de passe (ex. : pour toute une base de données).

20 « Recommandations relatives à l'authentification multifacteur et aux mots de passe », cyber.gouv.fr

21 « Mécanismes cryptographiques », cyber.gouv.fr

22 « Le référentiel général de sécurité version 2.0 : les documents », cyber.gouv.fr

FICHE 5 - GÉRER LES HABILITATIONS

Limiter les accès aux seules données dont un utilisateur a besoin.

Respecter le principe de moindre privilège, à travers la gestion des profils d'habilitation, permet de limiter les conséquences d'une usurpation de comptes ou d'une erreur de manipulation.

Les précautions élémentaires

- **Définir des profils d'habilitation** dans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions.
- **Faire valider toute demande d'habilitation** par un responsable (ex. : supérieur hiérarchique, chef de projet).
- **Supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique** (ex. : changement de mission ou de poste)**, ainsi qu'à la fin de leur contrat.**
- **Réaliser une revue régulière, au moins annuelle, des habilitations** afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur. Les métiers devraient être impliqués dans cette revue afin qu'ils s'assurent de la légitimité opérationnelle des droits attribués.

Ce qu'il ne faut pas faire

- Créer ou utiliser des comptes partagés par plusieurs personnes sans tracer ces exceptions aux règles de sécurité, sans les faire valider par les responsables appropriés et sans les revoir régulièrement.
- Donner des droits d'administrateurs à des utilisateurs n'en ayant pas besoin.
- Accorder à un utilisateur plus de privilèges que nécessaire.
- Oublier de retirer des autorisations temporaires accordées à un utilisateur (ex. : pour un remplacement).
- Oublier de supprimer les comptes utilisateurs des personnes ayant quitté l'organisation ou ayant changé de fonction.

POUR ALLER PLUS LOIN

- Établir, documenter et réexaminer régulièrement **une politique de contrôle d'accès** en rapport avec les traitements mis en œuvre par l'organisation qui doit inclure :
  - les procédures à appliquer systématiquement à l'arrivée ainsi qu'au départ ou au changement d'affectation d'une personne ayant accès à des données personnelles ;
  - les conséquences prévues pour les personnels en cas de non-respect des mesures de sécurité (ex. : utilisation abusive d'un droit d'accès légitime) ;
  - les mesures prévues permettant de restreindre et de contrôler l'attribution et l'utilisation des accès au traitement (voir la fiche n°16 - Tracer les opérations).

MON INFORMATIQUE, MES ÉQUIPEMENTS

FICHE 6 - SÉCURISER LES POSTES DE TRAVAIL

Prévenir les accès frauduleux, l'exécution de programmes malveillants (ex. : virus) ou la prise de contrôle à distance, notamment via Internet.

Les risques d'intrusion dans les systèmes informatiques sont multiples et les postes de travail constituent un des principaux points d'entrée.

Les précautions élémentaires

- Prévoir un mécanisme de **verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné.
- Installer un **pare-feu** (« *firewall* ») logiciel sur le poste et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.
- Utiliser des **antivirus régulièrement mis à jour.**
- **Déployer les mises à jour de sécurité au plus tôt**, le cas échéant après les avoir testées. Les mises à jour venant corriger des failles critiques publiques doivent d'autant plus être installées sans délais.
- Limiter les droits des utilisateurs au strict minimum en fonction de leurs besoins sur les postes de travail.
- **Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau interne de l'organisme** plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation.
- **Effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation** à une autre personne.
- Pour les **supports amovibles** (ex. : clés USB, disques durs externes) :
  - sensibiliser les utilisateurs aux risques liés à l'utilisation de supports amovibles, en particulier s'ils proviennent de l'extérieur ;
  - **limiter la connexion de supports amovibles** à l'indispensable ;
  - désactiver l'exécution automatique (« *autorun* ») depuis les supports amovibles.
- Pour l'**assistance sur les postes de travail** :
  - les outils d'administration à distance doivent **recueillir l'accord** de l'utilisateur avant toute intervention sur son poste (ex. : en répondant à un message s'affichant à l'écran, à l'occasion d'un rendez-vous accepté) ;
  - l'utilisateur doit également pouvoir **constater si la prise de main à distance est en cours** et quand elle se termine (ex. : affichage d'un message à l'écran).

Ce qu'il ne faut pas faire

- Utiliser des systèmes d'exploitation dont le support n'est plus assuré par l'éditeur.
- Donner des privilèges, en local comme sur le réseau, aux utilisateurs n'ayant pas une fonction le justifiant (ex. : administrateurs).

POUR ALLER PLUS LOIN

- **N'autoriser que l'exécution d'applications téléchargées** provenant de sources sûres (liste blanche).
- **Limiter l'usage** d'applications nécessitant des droits de niveau administrateur pour leur exécution.
- Fournir un environnement sécurisé (ex. : environnement virtualisé temporaire) pour la réalisation d'opérations nécessaires comportant un risque particulier (ex. : navigation sur un site qui n'est pas de confiance).
- Mettre en place une solution d'analyse et de **décontamination des supports amovibles** avant chaque utilisation. L'ANSSI a publié un guide[23] pour aider dans le choix de ce type de solutions.
- **En cas de compromission d'un poste, rechercher la source ainsi que toute trace d'intrusion** dans le système d'information de l'organisme pour détecter la compromission d'autres éléments.
- **Effectuer une veille de sécurité sur les logiciels et matériels utilisés dans le système d'information de l'organisme**. Le CERT-FR, centre gouvernemental français de veille, d'alerte et de réponse aux attaques informatiques, publie sur son site web[24] des alertes et des avis sur les vulnérabilités découvertes dans des logiciels et matériels et donne, lorsque cela est possible, des moyens pour s'en prémunir.
- Déployer les **mises à jour critiques des systèmes d'exploitation** sans délai (le cas échéant après les avoir testées) en programmant une vérification automatique hebdomadaire.
- Prévoir une politique des mises à jour fonctionnelles.
- Fixer les postes de travail à du mobilier spécifique ou difficilement déplaçable (ex. : utilisation de câbles antivol).
- Diffuser à tous les utilisateurs **la conduite à tenir et la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un évènement inhabituel** touchant aux systèmes d'information et de communication de l'organisme.
- Consulter la page[25] du CERT-FR sur les bons réflexes en cas d'intrusion sur un système d'information.

23 « Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés) », cyber.gouv.fr

24 « CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques », cert.ssi.gouv.fr

25 « Les bons réflexes en cas d'intrusion sur un système d'information », cert.ssi.gouv.fr

FICHE 7 - SÉCURISER L'INFORMATIQUE MOBILE

Anticiper l'atteinte à la sécurité des données à l'extérieur des locaux, dont le vol ou la perte d'un équipement mobile.

La multiplication des pratiques de travail hors des locaux de l'organisme (ex. : déplacements, télétravail) et d'utilisation de l'équipement personnel des utilisateurs comporte des risques spécifiques liés à l'usage d'ordinateurs portables, de clés USB ou encore de smartphones : il est indispensable de les encadrer.

Les précautions élémentaires

- **Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles** (ex. : vol de matériel, risques liés à la connexion aux réseaux et équipements non maîtrisés, notamment publics, usage d'équipements personnels) et aux procédures prévues pour les limiter.
- **Prévoir un contrôle d'accès** par des dispositifs d'authentification adaptées (ex. : certificat électronique, carte à puce). Tous les flux d'information devraient être chiffrés (ex. : VPN pour les accès externes).
- Mettre à disposition des utilisateurs **des espaces de stockage partagé accessibles en nomadisme.** Leur recommander d'y stocker toutes leurs données pour se prémunir contre la perte ou le vol du matériel.
- **Prévoir des moyens de chiffrement des postes nomades et supports de stockage amovibles** (ex. : ordinateur portable, clé USB, disque dur externe, CD-R, DVD-RW) tels que :
  - le chiffrement du disque dur (de nombreux systèmes d'exploitation intègrent une telle fonctionnalité) ;
  - le chiffrement fichier par fichier ;
  - la création de conteneurs (dossier susceptible de contenir plusieurs fichiers) chiffrés.
- **Concernant les *smartphones*,** en plus du code PIN de la carte SIM, **activer le verrouillage automatique du terminal et exiger un secret pour le déverrouiller** (ex. : mot de passe, schéma).
- **Informer les utilisateurs** de la personne à contacter en cas de perte ou de vol de leur matériel.
- **Évaluer les risques spécifiques à l'utilisation d'équipements personnels par les utilisateurs** (pratique du « *bring your own device* » ou BYOD) **et ne les autoriser qu'en fonction des risques identifiés**. Les données et les applications accessibles sur ces appareils non maîtrisés par l'organisme doivent être limitées en fonction de leur criticité. Les responsabilités de chacun et les précautions à respecter doivent être formalisées dans la charte informatique (voir la fiche n°2 - Définir un cadre pour les utilisateurs).

Ce qu'il ne faut pas faire

- Utiliser comme outil de sauvegarde ou de synchronisation les services *cloud* installés par défaut sur un appareil sans analyse approfondie de leurs conditions d'utilisation et des engagements de sécurité pris par les fournisseurs de ces services. Ceux-ci ne permettent généralement pas de respecter les préconisations données dans la fiche n°14 : Gérer la sous-traitance.
- Prévoir des mesures de sécurité (ex. : par le paramétrage d'un système de gestion des appareils mobiles ou MDM, « *mobile device management* ») qui entravent l'utilisation d'un équipement personnel dans le cadre privé (BYOD) au motif qu'il est utilisé dans le cadre professionnel (ex. : interdire l'installation d'applications sur l'appareil).
- Accéder à des éléments relevant de la vie privée des personnes stockés dans l'espace personnel d'un équipement personnel utilisé dans le cadre professionnel (BYOD).

POUR ALLER PLUS LOIN

- Voir la fiche dédiée[26] à l'utilisation d'équipement personnel par les utilisateurs sur le site de la CNIL.
- **Mettre en place un système de gestion des appareils mobiles** (MDM ou « *mobile device management* »), y compris pour les appareils personnels utilisés dans le cadre professionnel (BYOD) si la pratique est autorisée, afin d'uniformiser les configurations et de maîtriser le niveau de sécurité des appareils qui se connectent au réseau de l'organisme.
- **Fournir un filtre de confidentialité** pour les écrans des postes utilisés dans des lieux publics.
- Sensibiliser sur les mauvaises pratiques dans les lieux publics :
  - **ne pas laisser d'équipements ou de documents sans surveillance** ;
  - ne pas discuter (ex. : conversation en groupe ou au téléphone) d'informations sensibles (ex. : données personnelles, informations pouvant dévoiler des failles de sécurité).
- **Limiter le stockage des données** sur les postes nomades au strict nécessaire, en particulier lors de l'usage d'équipements personnels, et éventuellement l'interdire lors de déplacements à l'étranger[27].
- **Prévoir des mécanismes de protection contre le vol** (ex. : câble de sécurité, marquage visible du matériel) **et de limitation de ses impacts** (ex. : verrouillage automatique, chiffrement, effacement à distance). En cas d'utilisation d'un mécanisme d'effacement, ses modalités d'utilisation par l'employeur sur l'équipement personnel d'un employé (BYOD) doivent être intégrées à la charte informatique (voir la fiche n°2 - Définir un cadre pour les utilisateurs).
- Cloisonner les parties d'un équipement personnel ayant vocation à être utilisées dans un cadre professionnel.

26 « BYOD : quelles sont les bonnes pratiques ? », cnil.fr

27 « Bonnes pratiques à l'usage des professionnels en déplacement », cyber.gouv.fr

FICHE 8 - PROTÉGER LE RÉSEAU INFORMATIQUE

Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en œuvre.

Le réseau interne interconnecte l'ensemble des composants des systèmes d'information d'un organisme et dispose souvent de points de connexion avec l'extérieur. Il s'agit tout autant d'un point d'entrée que d'un support de propagation des attaques. Il est donc primordial de sécuriser le réseau interne.

Les précautions élémentaires

- **Limiter les accès Internet** en bloquant les services non nécessaires (ex. : VoIP, pair à pair).
- **Gérer les réseaux Wi-Fi.** Ils doivent utiliser un chiffrement à l'état de l'art (WPA3 ou WPA2 en respectant les recommandations de l'ANSSI sur la configuration de ce dernier[28]) et les réseaux ouverts aux invités doivent être séparés du réseau interne.
- **Imposer un VPN pour l'accès à distance** avec, si possible, une authentification robuste de l'utilisateur (ex. : carte à puce, mot de passe à usage unique basé sur le temps (TOTP)).
- **S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet.** Les opérations d'administration et de maintenance doivent tout particulièrement s'effectuer à travers un VPN.
- Privilégier le protocole SSH (correctement configuré) ou un accès physique direct pour l'administration des équipements réseau.
- **Limiter les flux réseau au strict nécessaire** en filtrant les flux entrants/sortants sur les équipements (ex. : pare-feux, serveurs proxy). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports.
- **Cloisonner le réseau** pour réduire l'impact en cas de compromission. On peut au minimum **distinguer un réseau interne sur lequel aucune connexion venant d'Internet n'est autorisée et un réseau DMZ** (« *demilitarized zone* ») **accessible depuis Internet**, en les séparant par des passerelles (« *gateway* »).

Ce qu'il ne faut pas faire

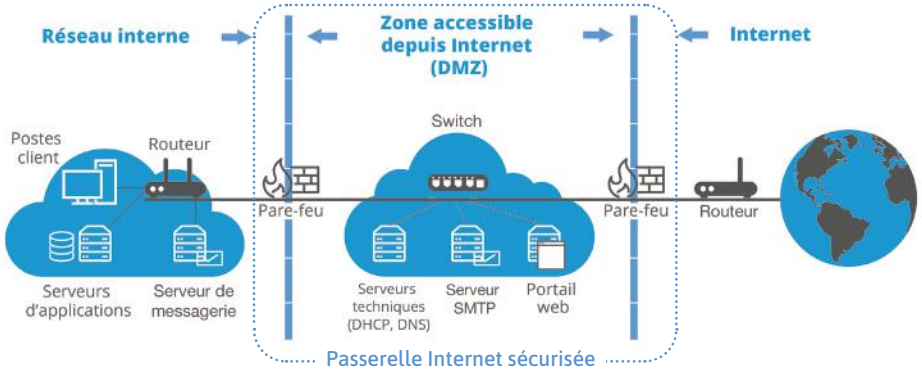
- Utiliser le protocole Telnet pour la connexion aux équipements actifs du réseau (ex. : pare-feux, routeurs, passerelles).
- Mettre à disposition des utilisateurs un accès Internet non filtré.
- Mettre en place un réseau Wi-Fi utilisant un chiffrement WEP.

28 « Sécuriser les accès Wi-Fi », cyber.gouv.fr

POUR ALLER PLUS LOIN

- Les opérations d'administration et de maintenance devraient être effectuées depuis des équipements sous maîtrise exclusive du responsable de traitement ou de ses sous-traitants.
- **On peut mettre en place l'identification automatique de matériel** en configurant une authentification des matériels (protocole 802.1X) ou, au minimum, en définissant une liste blanche, tenue à jour, des identifiants des cartes réseau (adresses MAC) afin d'interdire la connexion d'un dispositif non répertorié.
- **Des systèmes de détection d'intrusion** (IDS) **et de prévention d'intrusion** (IPS) peuvent analyser le trafic réseau pour détecter des attaques, voire y répondre. **Informer les utilisateurs** de la mise en place de tels systèmes dans la charte informatique (voir la fiche n°2 - Définir un cadre pour les utilisateurs), après information et consultation des instances représentatives du personnel.
- **L'ANSSI a publié des bonnes pratiques**[29], par exemple pour l'interconnexion d'un système d'information à Internet[30] (desquelles sont inspirées le schéma ci-dessous), le choix des pare-feux[31] ou le déploiement du protocole 802.1X[32].

Exemple de mise en œuvre d'une DMZ



29 « Publications de l'ANSSI », cyber.gouv.fr

30 « Recommandations relatives à l'interconnexion d'un SI à Internet », cyber.gouv.fr

31 « Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet », cyber.gouv.fr

32 « Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux », cyber.gouv.fr

FICHE 9 - SÉCURISER LES SERVEURS

Renforcer les mesures de sécurité appliquées aux serveurs.

La sécurité des serveurs doit être une priorité car ils centralisent un grand nombre de données et hébergent les services permettant d'y accéder et de les manipuler.

Les précautions élémentaires

- **Désinstaller ou désactiver les services et interfaces inutiles.**
- **Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.** Utiliser des comptes utilisateurs sans privilèges pour les opérations courantes.
- **Adopter une politique spécifique de mots de passe** pour les administrateurs. Changer les mots de passe, au minimum, lors de chaque départ d'un administrateur et en cas de suspicion de compromission.
- **Installer les mises à jour critiques** sans délai (le cas échéant après les avoir testées), en particulier les correctifs de sécurité, que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire.
- **Utiliser des logiciels de détection et de suppression de programmes malveillants** (ex. : antivirus) régulièrement mis à jour.
- **Utiliser des comptes nominatifs** pour l'accès aux bases de données et créer des comptes techniques spécifiques à chaque application.
- **Effectuer des sauvegardes et vérifier régulièrement leur intégrité et la capacité de les restaurer** (voir la fiche n°17 - Sauvegarder).
- **Mettre en œuvre le protocole TLS** (en remplacement de SSL[33]), ou un protocole assurant le chiffrement et l'authentification, au minimum pour tout échange de données sur Internet et vérifier sa bonne mise en œuvre par des outils appropriés[34].
- Ne pas autoriser les algorithmes de chiffrement obsolètes dans les communications avec le serveur.
- **Mettre en place un système de journalisation des évènement**s (voir la fiche n°16 - Tracer les opérations).

Ce qu'il ne faut pas faire

- Traiter des données personnelles sur des serveurs obsolètes et ne pas prévoir le remplacement de ces derniers.
- Utiliser des protocoles d'échange de données non sécurisés (ex. : authentification en clair, flux en clair).
- Utiliser les serveurs pour d'autres fonctions que celles auxquelles ils sont dédiés, notamment pour naviguer sur des sites web ou accéder à une messagerie électronique.
- Placer les bases de données sur un serveur directement accessible depuis Internet.
- Utiliser des comptes génériques (c'est-à-dire partagés entre plusieurs utilisateurs).

33 Le protocole TLS est parfois appelé, à tort, SSL ou SSL/TLS. Le protocole SSL, prédécesseur de TLS, est aujourd'hui obsolète et à proscrire.

34 Pour TLS, il existe plusieurs outils à cette fin (ex. : « SSL Server Test », ssllabs.com, « SSL-Tools », ssl-tools.net).

POUR ALLER PLUS LOIN

- Tout système traitant des données sensibles[34] doit être mis en œuvre dans un **environnement dédié** (isolé logiquement).
- **Les opérations d'administration des serveurs devraient se faire via un réseau dédié et isolé**, accessible après une authentification robuste (voir la fiche n°5 - Gérer les habilitations) permettant une traçabilité renforcée (voir la fiche n°16 - Tracer les opérations).
- En plus des flux extérieurs, **les flux internes devraient être chiffrés** autant que possible (ex. : à l'aide des protocoles TLS, IPsec ou SSH).
- Isoler les serveurs obsolètes mais essentiels et limiter le traitement de données personnelles dessus dans l'attente de leur remplacement par un système à jour.
- S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser des **outils de détection des vulnérabilités** (logiciels de scans de vulnérabilités tels que nmap[36], nessus[37] ou nikto[38]) ou audits pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité. Des systèmes de détection et prévention des attaques sur des systèmes ou serveurs critiques peuvent aussi être utilisés.
- Restreindre les accès physiques et interdire les accès logiques à distance aux ports de diagnostic et de configuration.
- La version 1.3 de TLS est à privilégier ou, à défaut, la version 1.2 en respectant les recommandations publiées par l'ANSSI sur le sujet[39].
- **L'ANSSI a publié diverses recommandations**[40] parmi lesquelles la sécurisation de l'administration des systèmes d'information[41] et la mise en place de cloisonnement système[42].

35 Les données sensibles sont décrites à l'article 6 de la loi Informatique et Libertés et à l'article 9 du RGPD.

36 « Nmap », nmap.org

37 « Tenable Nessus », tenable.com

38 « Nikto2 », cirt.net

39 « Recommandations de sécurité relatives à TLS », cyber.gouv.fr

40 « Publications de l'ANSSI », cyber.gouv.fr

41 « Recommandations relatives à l'administration sécurisée des SI », cyber.gouv.fr

42 « Recommandations pour la mise en place de cloisonnement système », cyber.gouv.fr

FICHE 10 - SÉCURISER LES SITES WEB

S'assurer que les bonnes pratiques minimales sont appliquées aux sites web.

Tout site web doit garantir son identité aux terminaux s'y connectant et la confidentialité des informations transmises..

Les précautions élémentaires

- **Sécuriser les flux d'échange de données** par l'utilisation de TLS :
  - **obtenir des certificats** aux niveaux adaptés (domaine, organisation ou étendu) auprès d'une autorité de certification et les gérer de manière adéquate ;
  - mettre en œuvre le protocole **TLS** (en remplacement de SSL[43]) sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre ;
  - **rendre l'utilisation de TLS obligatoire** pour toutes les pages d'authentification ou sur lesquelles sont affichées ou transmises des données personnelles.
- **Limiter les ports de communication** strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports.
- **Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées**. En particulier, limiter l'utilisation des comptes administrateur aux équipes en charge de l'informatique interne et ce, uniquement pour les actions d'administration qui le nécessitent.
- Implémenter les options « *HttpOnly* » et « *Secure* » dans tous les cookies utilisés.
- **Si des cookies non nécessaires au service sont utilisés, recueillir le consentement** de l'internaute après information de celui-ci et avant le dépôt du cookie.
- **Limiter le nombre de composants mis en œuvre**, en effectuer une veille régulière et les mettre à jour.
- **Limiter les informations renvoyées lors de la création d'un compte utilisateur ou lors de la réinitialisation d'un mot de passe**, afin de ne pas renseigner un attaquant sur l'existence – ou non – d'un compte associé à un identifiant (ex. : adresse de messagerie électronique).
- **Adopter les bonnes pratiques pour le développement informatique** (voir la fiche n°11 - Encadrer les développements informatiques). En particulier, **se prémunir contre les attaques les plus courantes sur les sites web référencées dans le Top 10 OWASP**[44] (ex. : injections SQL[45], injections de code indirecte (« *cross-site scripting* » ou XSS)[46], manipulations d'URL[47]).

43 Le protocole TLS est parfois appelé, à tort, SSL ou SSL/TLS. Le protocole SSL, prédécesseur de TLS, est aujourd'hui obsolète et à proscrire.

44 L'OWASP (Open web application security project) publie régulièrement une liste des dix risques les plus critiques pour les applications web (voir « OWASP Top Ten », owasp.org).

45 « SQL Injection », owasp.org

46 « Cross Site Scripting (XSS) », owasp.org

47 « Path Traversal », owasp.org

Ce qu'il ne faut pas faire

- Faire transiter des données personnelles dans une URL (ex. : identifiants, mots de passe).
- Utiliser des services non sécurisés (ex. : authentification en clair, flux en clair).
- Utiliser les serveurs hébergeant des sites web comme des postes de travail (ex. : navigation sur des sites web, accès à une messagerie électronique).
- Placer les bases de données sur un serveur directement accessible depuis Internet.
- Utiliser des comptes utilisateurs génériques (c'est-à-dire partagés entre plusieurs utilisateurs).

POUR ALLER PLUS LOIN

- Concernant la mise en œuvre de cookies, il est conseillé de consulter le dossier dédié sur le site de la CNIL[48].
- De manière générale, respecter les niveaux L1 et L2 des recommandations produites par l'OWASP[49].S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser **des outils de détection des vulnérabilités** (logiciels de scans de vulnérabilité tels que OWASP ZAP[50], nmap[51] ou nikto[52]) pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité. Des systèmes de détection et de prévention des attaques sur des systèmes ou serveurs critiques peuvent aussi être utilisés. Ces tests doivent être menés de façon régulière et avant toute mise en production d'une nouvelle version logicielle.
- **L'ANSSI a publié sur son site[53] des recommandations spécifiques** pour mettre en œuvre TLS[54] ou pour sécuriser un site web[55].

48 « Site web, cookies et autres traceurs », cnil.fr
49 « OWASP MAS Checklist », mas.owasp.org
50 « Zed Attack Proxy (ZAP) », zaproxy.org
51 « Nmap », nmap.org
52 « Nikto2 », cirt.net
53 « Publications de l'ANSSI », cyber.gouv.fr
54 « Recommandations de sécurité relatives à TLS », cyber.gouv.fr
55 « Sécuriser un site web », cyber.gouv.fr

FICHE 11 - ENCADRER LES DÉVELOPPEMENTS INFORMATIQUES

Intégrer la sécurité et la protection des données personnelles au plus tôt dans les projets.

La protection des données personnelles doit être intégrée dans le cycle de développement informatique dès la phase de conception et pour les configurations par défaut afin d'offrir aux personnes concernées une meilleure maîtrise de leurs données et de limiter les erreurs, pertes, modifications non autorisées, ou mauvais usages de celles-ci dans les applications.

Les précautions élémentaires

- **Intégrer la protection des données, y compris ses exigences en termes de sécurité des données, dès la conception** de l'application ou du service. Ces exigences peuvent se traduire par divers choix d'architecture (décentralisée ou centralisée), de fonctionnalités (ex. : anonymisation à bref délai, minimisation des données), de technologies (ex. : chiffrement des communications), etc.
- Utiliser des composants (ex. : bibliothèques) et outils **sécurisés et reconnus par la communauté**.
- Mettre en œuvre des mesures contre les attaques courantes qui visent les bases de données (ex. : injections de code SQL, scripts).
- **Pour tout développement à destination du grand public, mener une réflexion sur les paramètres influant sur le respect de la vie privée**, et notamment sur le paramétrage par défaut.
- **Éviter le recours à des zones de texte libre ou de commentaires**, sources de collecte de données personnelles supplémentaires non nécessaires ou disproportionnées.
- **Réaliser des tests complets** (ex. : unitaires, d'intégration, fonctionnels, de sécurité) avant la mise à disposition ou la mise à jour d'un produit. Lors d'une mise à jour, s'assurer que les tests utilisés sont toujours adaptés.
- Effectuer les développements informatiques et les tests dans un environnement informatique distinct de celui de la production (ex. : sur des ordinateurs ou des machines virtuelles différents) et sur des données fictives ou anonymisées.
- **Veiller à l'absence de secrets (d'authentification ou de chiffrement)** lors du dépôt de code dans un outil de gestion de versions (ex. : Git ou svn). **Changer les secrets lors du passage en production.**
- **Effectuer un test de non-régression et/ou une revue de code avant tout passage en production d'une mise à jour** pour éviter l'apparition de sources de violation de données personnelles.

Ce qu'il ne faut pas faire

- Utiliser des données personnelles réelles pour les phases de développement et de test. Des jeux fictifs doivent être utilisés autant que possible.
- Développer une application puis réfléchir dans un second temps aux mesures de sécurité ou de protection des données personnelles à mettre en place.

POUR ALLER PLUS LOIN

- La CNIL a publié un **guide RGPD**[56] **spécifiquement à destination des équipes de développement** pour les aider à mettre en conformité leurs développements informatiques avec la règlementation concernant la protection des données personnelles.
- **Mettre en place une défense en profondeur** des systèmes, c'est-à-dire une combinaison de plusieurs mesures de sécurité et contrôles (ex. : contrôler les données entrées dans un formulaire en ligne mais également protéger les requêtes en base de données). En particulier, les mesures en place sur la partie « *front* » d'une application peuvent être contournées et devraient être renforcées par des mesures sur la partie « *back* ».
- Le développement doit imposer des **formats de saisie et d'enregistrement des données qui minimisent les données collectées**. Par exemple, s'il s'agit de collecter uniquement l'année de naissance d'une personne, le champ du formulaire correspondant ne doit pas permettre la saisie du mois et du jour de naissance. Cela peut se traduire notamment par la mise en œuvre d'un menu déroulant limitant les choix pour un champ du formulaire.
- Un article dédié aux zones de texte libre ou de commentaires est accessible sur le site de la CNIL[57].
- Les conventions ou règles de codage et la documentation sont essentielles pour maintenir l'application ou le service dans le temps sans introduire de nouvelles vulnérabilités et pour corriger efficacement les dysfonctionnements.
- Les formats de données doivent être compatibles avec la mise en œuvre de la durée de conservation choisie. Par exemple, si un document numérique doit être conservé 20 ans, il pourrait être pertinent de privilégier des formats ouverts, davantage susceptibles d'être maintenus sur le long terme.
- La **création et la gestion de profils utilisateur** donnant des droits d'accès aux données variant en fonction des catégories d'utilisateurs doivent être intégrées dès la phase de conception.
- Les tests menés sur les données fictives ou anonymisées ne sont parfois pas suffisants pour s'assurer du bon fonctionnement d'un nouveau service ou d'une nouvelle fonctionnalité. Il est alors possible de tester dans un environnement de pré-production avec des données réelles. L'environnement de pré-production doit être configuré et sécurisé au même niveau que l'environnement de production lui-même et le nouveau service ou sa mise à jour doit avoir déjà subi l'ensemble des tests (unitaires, d'intégration et fonctionnels) dans les environnements de développement et de test.
- Selon la nature de l'application, il peut être nécessaire d'assurer son intégrité par le recours à des signatures de code exécutable garantissant qu'il n'a subi aucune altération.

56 « Guide RGPD de l'équipe de développement », lincnil.github.io

57 « Zones bloc note et commentaires : les bons réflexes pour ne pas déraper », cnil.fr

FICHE 12 - PROTÉGER LES LOCAUX

Renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux.

L'accès aux locaux doit être contrôlé pour éviter ou ralentir un accès direct, non autorisé, que ce soit aux fichiers papier ou aux matériels informatiques, notamment aux serveurs. Les locaux doivent également être protégés contre les autres types de menaces (ex. : incendie, inondation).

Les précautions élémentaires

- Restreindre les accès aux locaux au moyen de portes verrouillées.
- Installer des **alarmes anti-intrusion** et vérifier leur bon fonctionnement périodiquement.
- **Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies** et les inspecter annuellement.
- Protéger les clés permettant l'accès aux locaux ainsi que les codes d'alarme.
- **Distinguer les zones des bâtiments selon les risques** (ex. : prévoir un contrôle d'accès dédié pour la salle informatique).
- Tenir à jour une liste des personnes ou catégories de personnes autorisées à pénétrer dans chaque zone et faire une revue périodique de cette liste.
- **Établir les règles et moyens de contrôle d'accès** des visiteurs, au minimum en faisant **accompagner les visiteurs en dehors des zones d'accueil du public**[58] par une personne appartenant à l'organisme.
- Protéger l'accès au réseau (ex. : prises dans les bureaux, baies de brassage) et ne permettre qu'aux équipements autorisés de s'y connecter.
- Protéger physiquement les matériels informatiques par des moyens spécifiques (ex. : système anti-incendie dédié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique, redondance de système de climatisation).

Ce qu'il ne faut pas faire

- Sous-dimensionner ou négliger l'entretien de l'environnement des salles informatiques (ex. : climatisation, onduleur). Une panne sur ces installations a souvent comme conséquence l'arrêt des machines ou l'ouverture des accès aux salles (pour favoriser la circulation d'air) qui neutralise de fait des éléments concourant à la sécurité physique des locaux.
- Laisser visibles (ex. : écran du secrétariat lisible facilement par les visiteurs, salle de réunion dont l'écran est visible de l'extérieur) ou accessibles (ex. : documents critiques imprimés posés à la vue de tous dans les zones d'accueil du public) des données qui devraient rester confidentielles.

58 Depuis leur entrée, pendant leur visite et jusqu'à leur sortie des locaux.

POUR ALLER PLUS LOIN

- Conserver une trace des accès aux salles ou bureaux susceptibles de contenir du matériel traitant des données personnelles pouvant avoir un impact négatif grave sur les personnes concernées en cas d'incident. **Informer les utilisateurs** de la mise en place d'un tel système, après information et consultation des instances représentatives du personnel.
- S'assurer que seul le personnel dûment habilité est admis dans les zones à accès restreint.
  Par exemple :
  - à l'intérieur des zones à accès règlementé, exiger **le port d'un moyen d'identification visible** (ex. : badge) pour toutes les personnes ;
  - les visiteurs (ex. : personnel en charge de l'assistance technique) ne doivent avoir qu'un accès limité. La date et l'heure de leur arrivée et de leur départ doivent être consignées ;
  - réexaminer et mettre à jour régulièrement les permissions d'accès aux zones sécurisées et les supprimer si nécessaire.

MA MAÎTRISE DES DONNÉES

FICHE 13 - SÉCURISER LES ÉCHANGES AVEC L'EXTÉRIEUR

Renforcer la sécurité de toute transmission de données personnelles.

Sans mesure complémentaire, les canaux de transmission de données grand public (ex. : messagerie électronique, messagerie instantanée, plateforme de dépôt de fichiers) **constituent rarement un moyen de communication sûr** pour transmettre des données personnelles. Une simple erreur d'inattention peut conduire des personnes non habilitées à prendre connaissance de données personnelles, ce qui porte atteinte au droit à la vie privée des personnes concernées. En outre, les entités ayant accès aux serveurs par lesquels transite l'information peuvent avoir accès à leur contenu ou à des métadonnées.

Les précautions élémentaires

- **Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers** (ex. : clé USB, disque dur portable, disque optique).
- **Lors d'un envoi via un réseau :**
  - **chiffrer les pièces** sensibles à transmettre. À ce sujet, il convient de se référer aux préconisations de la fiche n°21 - Chiffrement, hachage, signature ;
  - utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers (ex. : **SFTP** ou **HTTPS**), en utilisant **les versions les plus récentes des protocoles** ;
  - **assurer la confidentialité des secrets** (ex. : clé de chiffrement, mot de passe) en les transmettant via un canal distinct des données protégées (ex. : envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).
- Ouvrir un fichier venant de l'extérieur seulement si l'expéditeur est connu et après soumission à une **analyse antivirus**.
- En cas d'utilisation du **fax**, mettre en place les mesures suivantes :
  - installer le fax dans un local physiquement contrôlé et uniquement accessible au personnel habilité ;
  - faire afficher l'identité du fax destinataire lors de l'émission des messages ;
  - doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;
  - préenregistrer dans le carnet d'adresses des fax les numéros des destinataires potentiels (si la fonction existe).

Ce qu'il ne faut pas faire

- Transmettre des fichiers contenant des données personnelles en clair via des messageries et autres plateformes grand public.
- Ne pas prévoir la suppression (de préférence automatique) des fichiers transmis à l'aide d'une plateforme de transfert de fichiers.

POUR ALLER PLUS LOIN

- Utiliser des algorithmes à clé publique, lorsque les différents acteurs ont mis en place une **infrastructure de gestion de clés publiques** pour garantir la confidentialité et l'intégrité des communications, ainsi que l'authentification de l'émetteur.
- Faire **signer électroniquement les données** par l'émetteur avant leur envoi afin de garantir qu'il est à l'origine de la transmission (voir la fiche n°21 - Chiffrement, hachage, signature).
- Utiliser un **serveur de dépôt de fichiers temporaires** peut également être approprié. Dans ce cas, s'assurer de :
  - paramétrer une durée limitée de mise à disposition des fichiers ;
  - restreindre l'accès aux fichiers aux seuls destinataires dûment autorisés ;
  - chiffrer les fichiers avant de les déposer sur le service si la solution utilisée ne prévoit pas cette possibilité de manière intégrée.
- Certains outils et solutions de communication protègent aussi les métadonnées liées aux éléments échangés et peuvent être utilisés lorsque celles-ci présentent une sensibilité particulière.
- Pour les systèmes les plus sensibles, cantonner les fichiers venant de l'extérieur à des zones isolées du reste du système pour éviter la propagation de logiciels malveillants.

FICHE 14 - GÉRER LA SOUS-TRAITANCE

Encadrer la sécurité des données avec les sous-traitants.

Les traitements de données réalisés par un sous-traitant[59] pour le compte du responsable de traitement doivent bénéficier de garanties suffisantes, notamment en matière de sécurité. Le responsable de traitement doit avoir connaissance du détail des mesures de sécurité mises en œuvre par ses sous-traitants pour pouvoir démontrer sa conformité[60].

Les précautions élémentaires

- **Faire appel uniquement à des sous-traitants présentant des garanties suffisantes** (notamment en termes de connaissances spécialisées, de fiabilité et de ressources).
- **Prévoir un contrat avec les sous-traitants**[61], qui définit notamment l'objet, la durée, la finalité du traitement ainsi que les obligations des parties, notamment en termes de sécurité. S'assurer qu'il contient en particulier des dispositions fixant :
  - la répartition des responsabilités et des obligations en matière de **confidentialité des données personnelles** confiées ;
  - des **contraintes minimales en matière d'authentification** des utilisateurs ;
  - **les conditions de restitution et de destruction des données** en fin du contrat ;
  - **les règles de gestion et de notification des incidents**. Celles-ci devraient comprendre une information du responsable de traitement en cas de découverte de faille de sécurité ou d'incident de sécurité et cela dans les plus brefs délais lorsqu'il s'agit d'une violation de données personnelles[62] ;
  - l'assistance que doit fournir le sous-traitant pour garantir le respect des obligations de sécurité[63] ;
  - la revue régulière des mesures de sécurité et, le cas échéant, les conditions de leur révision.
- **Prévoir les moyens permettant de vérifier l'effectivité des garanties offertes par le sous-traitant** en matière de protection des données (ex. : audits de sécurité, visite des installations). Ces garanties incluent notamment :
  - le chiffrement des données selon leur sensibilité ou, à défaut, l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées si cela n'est pas nécessaire à l'exécution de son contrat ;
  - le chiffrement des transmissions de données (ex. : connexion de type HTTPS, mise en place de VPN) ;
  - des garanties en matière de protection du réseau, de traçabilité, de gestion des habilitations, d'authentification, de pratiques d'administration, d'audits, etc.

---

59 Entendu au sens du RGPD.

60 Articles 5.2 et 24.1 du RGPD.

61 La Commission européenne a publié des clauses contractuelles types sur lesquelles ce contrat peut reposer (voir « Clauses contractuelles types entre responsable de traitement et sous-traitant », cnil.fr).

62 Un incident de sécurité est caractérisé de « violation de données à caractère personnel » lorsqu'il touche à des données personnelles.

63 Se référer à l'article 32 du RGPD et au §41 des lignes directrices 07/2020 adoptées par le Comité européen à la protection des données (CEPD).

Ce qu'il ne faut pas faire

- Entamer la prestation de sous-traitance sans avoir signé avec le prestataire un contrat reprenant les exigences posées par l'article 28 du RGPD.
- Avoir recours à des services de *cloud* sans garantie quant à la localisation géographique effective des données et sans s'assurer des conditions légales et des éventuelles formalités pour les transferts de données en dehors de l'Union européenne.

POUR ALLER PLUS LOIN

- La CNIL a publié un guide à destination des sous-traitants[64].
- Consulter et mettre en œuvre les dispositions de l'article 28 du RGPD.
- Apporter une attention particulière au choix d'un fournisseur de service *cloud* (voir la fiche n°22 - *Cloud* : Informatique en nuage).
- Toute la chaine de sous-traitance (sous-traitants des sous-traitants) devrait être considérée et non seulement les sous-traitants directs.
- Lors du choix d'un sous-traitant, l'obtention d'une certification est un premier indice pour évaluer sa fiabilité. Par exemple, la norme internationale ISO/IEC 27001 impose des mesures organisationnelles et techniques pour la mise en place d'un système de management de la sécurité de l'information (SMSI), tandis que la norme ISO/IEC 27701[65] concerne le système de management de la protection de la vie privée (PIMS en anglais).
- Concernant les données de santé, un hébergeur doit disposer d'une certification d'hébergeur de données de santé (HDS)[66]. L'Agence du numérique en santé (ANS) publie la liste des hébergeurs certifiés[67]. À noter que la certification a progressivement remplacé l'agrément HDS depuis 2018 et que certains hébergeurs disposent encore d'un agrément[68] valide.
- Le cas échéant, exiger la communication par le prestataire de ses certifications et en vérifier le périmètre.

64 « Règlement européen sur la protection des données : un guide pour accompagner les sous-traitants », cnil.fr

65 « L'ISO 27701, une norme internationale pour la protection des données personnelles », cnil.fr

66 « HDS - Certification Hébergeur de Données de Santé », esante.gouv.fr

67 « Liste des hébergeurs certifiés », esante.gouv.fr

68 « Liste des hébergeurs agréés », esante.gouv.fr

FICHE 15 - ENCADRER LA MAINTENANCE ET LA FIN DE VIE DES MATÉRIELS ET LOGICIELS

Garantir la sécurité des données à tout moment du cycle de vie des matériels et des logiciels.

Les opérations de support doivent être encadrées pour maîtriser l'accès aux données par les prestataires. Les données doivent être préalablement effacées des matériels destinés à être mis au rebut.

Les précautions élémentaires

- **Enregistrer les interventions** de maintenance **dans une main courante**.
- **Ouvrir les accès nécessaires** à la télémaintenance **à la demande** du prestataire, pour une durée adaptée à l'intervention et définie à l'avance. Ces accès doivent être refermés à l'issue de cette durée.
- Insérer des clauses de sécurité dans les contrats de maintenance effectuée par des prestataires pour encadrer leurs accès aux systèmes d'information (voir l'exemple de clause ci-contre).
- **Encadrer par un responsable de l'organisme les interventions par des tiers.**
- **Ne pas laisser seul un intervenant extérieur**, notamment dans les salles sensibles (ex. : salle serveur).
- **Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers** ou en fin du contrat de location.

Ce qu'il ne faut pas faire

- Installer des applications pour la télémaintenance ayant des vulnérabilités connues (ex. : applications qui ne chiffrent pas les communications).
- Réutiliser, revendre ou jeter des supports ayant contenu des données personnelles sans que les données n'aient été supprimées de façon sécurisée.
- Laisser un accès complet ou permanent aux systèmes pour la télémaintenance.

POUR ALLER PLUS LOIN

- Rédiger et mettre en œuvre une procédure de suppression sécurisée des données.
- Utiliser des logiciels dédiés à la suppression de données sans destruction physique qui ont été qualifiés ou certifiés. L'ANSSI accorde des certifications de premier niveau[69] à des logiciels de ce type.
- Mettre en place des outils de surveillance en temps réel (ex. : sessions « 4 yeux ») ou a posteriori (ex. : enregistrement) des interventions de télémaintenance par des tiers[70].
- L'ANSSI dédie un chapitre de son guide[71] concernant l'administration sécurisée à la maintenance par des tiers.

69 « Découvrir les solutions certifiées », cyber.gouv.fr

70 Tout comme les systèmes de journalisation, de tels dispositifs doivent être mis en place dans le respect des dispositions légales applicables et en informant les personnes concernées.

71 « Recommandations relatives à l'administration sécurisée des SI », cyber.gouv.fr

Exemple de clause pouvant être utilisé en cas de maintenance par un tiers :

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à X.

En cas de télémaintenance permettant l'accès à distance aux fichiers de X, Y ne pourra intervenir qu'après autorisation d'accès délivrée par X. L'accès devra être fermé au terme de chaque intervention de Y.

[*Formulation alternative selon la nature de la maintenance :*

En cas de télémaintenance permettant l'accès à distance aux fichiers de X, Y ne pourra intervenir qu'après information délivrée à X, permettant à ce dernier d'identifier et de surveiller les accès à son système d'information.

]

Des registres seront établis sous les responsabilités respectives de X et Y, mentionnant les date et nature détaillée des interventions de télémaintenance ainsi que les noms de leurs auteurs.

Note : une telle clause de maintenance doit nécessairement être couplée à celle traitant de la confidentialité pour la sous-traitance.

SE PRÉPARER À UN INCIDENT

FICHE 16- TRACER LES OPÉRATIONS

Tracer les opérations pour la détection d'anomalies, de dysfonctionnements ou d'incidents et disposer des informations utiles à leur traitement ou en cas de contentieux.

Afin de pouvoir **identifier un accès frauduleux** ou une **utilisation abusive** de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Les traces alors collectées sont également des éléments de preuve utiles pour la démonstration de la conformité[72].

Les précautions élémentaires

- **Prévoir un système de journalisation** (c'est-à-dire un enregistrement dans des fichiers journaux ou « *logs* ») des activités métier des utilisateurs (traces applicatives), des interventions techniques (y compris par les administrateurs), des anomalies et des évènements liés à la sécurité (traces techniques ou « système »).
- **Conserver ces évènements sur une période glissante comprise entre six mois et un an** (sauf, par exemple, en cas d'obligation légale portant sur cette durée de conservation, de besoin de gestion des contentieux, de contrôle interne ou encore d'un besoin identifié d'analyse post-incident).
- **Effectuer, pour les traces applicatives, un enregistrement des opérations de création, consultation, partage, modification et suppression** des données en conservant l'identifiant de l'auteur, la date, l'heure et la nature de l'opération ainsi que la référence des données concernées (pour en éviter la duplication).
- **Informer les utilisateurs**, par exemple lors de l'authentification ou de l'accès au système, de la mise en place du dispositif de journalisation, après information et consultation des instances représentatives du personnel.
- **Protéger les équipements de journalisation et les informations journalisées** pour empêcher les opérations non autorisées (ex. : en les rendant inaccessibles aux personnes dont l'activité est journalisée), les mésusages par des comptes habilités (ex. : en mettant en place une charte d'utilisation ou des alertes spécifiques) et l'écrasement des traces générées par les applicatifs concernés.
- S'assurer du bon fonctionnement du système de journalisation **en intégrant les équipements dans un outil de supervision et vérifier régulièrement la présence de journaux exploitables**.
- **S'assurer que les sous-traitants sont contractuellement tenus** de mettre en œuvre la journalisation conformément aux présentes recommandations et de notifier dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement.
- **Analyser de manière active, en temps réel ou à court terme, les traces collectées pour être en mesure de détecter la survenue d'un incident** (voir la fiche n°19 - Gérer les incidents et les violations).

72 Articles 5.2 et 24.1 du RGPD.

Ce qu'il ne faut pas faire

- Dupliquer et conserver de manière excessive les données personnelles concernées par le traitement au sein des journaux (ex. : y enregistrer les mots de passe ou leur empreinte (ou « *hash* ») lors de l'authentification des utilisateurs).
- Utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique (ex. : utiliser les traces pour compter les heures travaillées est un détournement de finalité, puni par la Loi).
- Conserver les traces sans limite de durée.

POUR ALLER PLUS LOIN

- Voir la recommandation de la CNIL relative à la journalisation[73].
- **Faire participer l'utilisateur à la surveillance des opérations** faites sur son compte et ses données (ex. : proposer un récapitulatif des trois dernières connexions). Privilégier une surveillance automatique des journaux, couplée à une configuration adaptée des alertes.
- **Mettre en place une enclave de collecte** centralisant les journaux d'évènements de l'ensemble du système d'information afin d'empêcher toute altération de ceux-ci.
- L'ANSSI a publié des recommandations sur la mise en place d'un système de journalisation[74] et plus spécifiquement des recommandations en environnement Active Directory[75].

73 « La CNIL publie une recommandation relative aux mesures de journalisation », cnil.fr

74 « Recommandations de sécurité pour l'architecture d'un système de journalisation », cyber.gouv.fr

75 « Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory », cyber.gouv.fr

FICHE 17 - SAUVEGARDER

Effectuer des sauvegardes régulières pour limiter l'impact d'une disparition ou d'une altération non désirée de données.

Des copies de sauvegarde doivent être réalisées et testées régulièrement pour être disponibles en cas de besoin.

Les précautions élémentaires

- **Effectuer des sauvegardes fréquentes des données**, que celles-ci soient sous forme papier ou électronique. Il peut être opportun de prévoir des sauvegardes incrémentales[76] quotidiennes et des sauvegardes complètes à intervalles réguliers.
- Stocker au moins une sauvegarde sur un site géographiquement distinct du site d'exploitation.
- **Isoler au moins une sauvegarde hors ligne**, déconnectée du réseau de l'entreprise.
- **Protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation** (ex. : en chiffrant les sauvegardes, en prévoyant un stockage dans un lieu sécurisé, en encadrant contractuellement une prestation d'externalisation des sauvegardes).
- Chiffrer le canal de transmission, si celui-ci n'est pas interne à l'organisme, lorsque les sauvegardes sont transmises par le réseau.
- Tester régulièrement l'intégrité des sauvegardes et la capacité de les restaurer.

Ce qu'il ne faut pas faire

- Assurer un niveau de sécurité moins élevé sur le système de sauvegardes (ex. : ne pas sauvegarder le système lui-même) que sur les autres systèmes d'information.
- Conserver les sauvegardes sur les mêmes systèmes que les données sauvegardées sans les isoler. Une menace (ex. : rançongiciel) pourrait alors s'attaquer aussi bien aux données qu'à leurs sauvegardes.
- Conserver les sauvegardes au même endroit que les machines hébergeant les données. Un sinistre majeur intervenant à cet endroit aurait comme conséquence une perte définitive des données.
- Ne jamais vérifier si les sauvegardes sont exploitables et se rendre compte que ce n'est pas le cas le jour où elles sont nécessaires.

POUR ALLER PLUS LOIN

- Protéger au moins une sauvegarde (ex. : celle qui est géographiquement distincte du site d'exploitation) dans des coffres ignifugés et étanches.
- Si les exigences sur la disponibilité des données et des systèmes sont élevées, il est conseillé de mettre en place une réplication des données vers un site secondaire.
- Il est conseillé d'appliquer la règle dite « 3 – 2 – 1 », état de l'art en matière de sauvegarde, qui consiste à disposer de 3 copies des donnés, stocker sur 2 supports différents, dont 1 hors ligne.
- L'ANSSI a publié des recommandations[77] sur la sauvegarde des systèmes d'information.

76 Une sauvegarde incrémentale consiste à n'enregistrer que les modifications faites par rapport à une précédente sauvegarde.

77 « Sauvegarde des systèmes d'information », cyber.gouv.fr

FICHE 18 - PRÉVOIR LA CONTINUITÉ ET LA REPRISE D'ACTIVITÉ

Prévoir un fonctionnement dégradé des systèmes d'information et être capable de les redémarrer sans impacter la sécurité des données.

Pour limiter le temps d'indisponibilité du système, il faut anticiper les incidents les plus courants. Assurer la continuité d'activité consiste à prévoir des moyens de continuer de fonctionner, en général de manière dégradée, malgré des dysfonctionnements. La reprise d'activité, quant à elle, englobe toutes les actions nécessaires pour relancer un système arrêté.

Les précautions élémentaires

- **Rédiger un plan de continuité (PCA) et de reprise (PRA) d'activité informatique** même sommaire, incluant la liste des intervenants. Le niveau de protection des données ne devrait pas être réduit par les modes de fonctionnement prévu.
- **S'assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d'incident**.
- **Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité**.
- À propos des matériels :
  - utiliser un onduleur pour protéger le matériel servant aux traitements essentiels ;
  - prévoir une redondance matérielle des équipements de stockage (ex. : au moyen d'une technologie RAID[78]).

Ce qu'il ne faut pas faire

- Se considérer à l'abri.
- Réduire le niveau de sécurité des données lors de la mise en place d'une procédure dégradée, sans prendre en compte les nouveaux risques générés pour maintenir l'activité.
- Ne pas prévoir de retour à la normale.
- Ne pas tester les mesures de continuité ou de reprise d'activité en amont.

POUR ALLER PLUS LOIN

- Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a publié un guide[79] concernant l'établissement d'un plan de continuité d'activité ou de reprise d'activité.
- Définir une organisation de gestion de crise.
- Réaliser des exercices avec toutes les parties prenantes pour vérifier l'efficacité et l'assimilation des procédures mises en place.
- Des tests ciblés sur certains composants ou parties du système peuvent être privilégiés pour limiter l'impact sur la production. Cependant, la continuité et la reprise des éléments les plus critiques doivent être testées de temps en temps. Un test de l'arrêt complet du système d'information doit également être envisagé.

78 RAID (« *redondant array of independant disk* ») désigne des techniques de répartition de données sur plusieurs supports de stockage (ex. : disques durs) afin de prévenir la perte de données consécutive à la panne d'un des supports.

79 « Bienvenue sur le guide de la continuité d'activité », guide-continuite-activite.sgdsn.gouv.fr .

FICHE 19 - GÉRER LES INCIDENTS ET LES VIOLATIONS

Prévoir les procédures pour gérer les incidents et réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).

Il convient d'être préparé à l'éventualité d'un incident pour intervenir à temps et de manière appropriée, en intégrant l'objectif de limiter les effets pour les personnes dont les données sont concernées. Le responsable de traitement peut être amené à notifier la CNIL ou informer les personnes concernées de l'incident en fonction du risque pour celles-ci.

Les précautions élémentaires

- **Analyser régulièrement les traces collectées** (voir la fiche n°16 - Tracer les opérations).
- S'assurer que **les gestionnaires du dispositif de gestion des traces** (qu'ils soient internes ou externes) **notifient le responsable de traitement, dans les plus brefs délais, en cas d'anomalie ou d'incident de sécurité**.
- Diffuser à tous les utilisateurs, internes comme externes, **la conduite à tenir et la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un évènement inhabituel** touchant aux systèmes d'information et de communication de l'organisme. **Sensibiliser les utilisateurs** à l'importance de signaler tout évènement suspect.
- Établir des procédures détaillant les dispositifs de génération et de remontée des alertes des différentes sources (ex. : automatiques, par les utilisateurs), leur traitement et les actions à mener en cas d'incident avéré (ex. : personnes à contacter, actions pour circonscrire l'incident en fonction de sa nature). Inclure la gestion des violations de données dans le processus de gestion des incidents. **Définir des critères de qualification d'un incident en violations de données**.
- **Évaluer le risque, pour les personnes, engendré par la violation** en tenant compte de la gravité et de la probabilité des conséquences que la violation pourrait avoir sur leurs droits et libertés.
- **Tenir un registre interne de toutes les violations de données personnelles**.
- **Notifier[80] à la CNIL, dans les 72 heures (tel que prévu par le RGPD), les violations présentant un risque pour les droits et libertés des personnes et**, en cas de de risque élevé et sauf exception prévue par le RGPD[81], **informer les personnes concernées** pour qu'elles puissent en limiter les conséquences[82].

Ce qu'il ne faut pas faire

- Attendre que les personnes concernées ou des tiers détectent un incident et le signalent.
- Omettre l'analyse des risques qu'une violation de données personnelles pourrait avoir pour les droits et libertés des personnes.
- Attendre d'avoir des informations précises pour notifier la CNIL alors qu'il est clairement établi qu'une violation s'est produite. Les notifications de données peuvent être transmises en deux temps : une initiale, dans les 72h, puis une complémentaire ensuite si nécessaire.

80 La procédure de notification est détaillée sur le site de la CNIL (voir « Notifier une violation de données personnelles », cnil.fr).

81 Articles 33 et 34 du RGPD.

82 L'obligation de notification de violation de données personnelles ne dédouane pas le responsable de ses potentielles autres obligations de remontée d'incident (voir « Notifications d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ? », cnil.fr).

POUR ALLER PLUS LOIN

- Privilégier une **surveillance automatique des journaux**, couplée à une configuration adaptée des alertes.
- Mettre en place une formation obligatoire à tout le personnel sur l'identification et la notification de violations ainsi que la conduite à tenir dans ce cas.
- Le CEPD[83] a publié des lignes directrices[84] détaillant 18 exemples de violations de données, rédigées à partir de cas pratiques rencontrés par les autorités de protection des données européennes.
- Le groupe de travail (dit « article 29 ») qui a précédé le CEPD sur la protection des données a également publié des lignes directrices[85] sur la notification de violations de données personnelles pour accompagner les organismes dans la mise en œuvre de leurs obligations.
- En cas d'incident ou pour s'y préparer, consulter le site d'assistance et prévention en sécurité numérique[86].

83 Comité européen à la protection des données.

84 « Lignes directrices 01/2021 Exemples concernant la notification de violations de données à caractère personnel », edpb.europa.eu

85 « Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) », ec.europa.eu

86 « Assistance et prévention du risque numérique au service des publics », cybermalveillance.gouv.fr

FOCUS

FICHE 20 – ANALYSE DE RISQUES

Identifier les risques et évaluer leur vraisemblance et leur gravité pour mettre en place les mesures de sécurité appropriées.

En parallèle de la mise en conformité aux précautions élémentaires présentées dans ce guide, il est pertinent, voire obligatoire selon la criticité des traitements, de réaliser des analyses de risques relative à la protection des données. Ces analyses permettent de décider des mesures de sécurité complémentaires, adaptées au contexte, permettant de limiter l'impact sur les personnes concernées par le traitement.

Les précautions élémentaires

- Identifier les traitements de données personnelles pour lesquels **une analyse d'impact relative à la protection des données (AIPD)[87] doit obligatoirement être menée selon le RGPD[88]**. Une AIPD comporte non seulement une partie dédiée à la réflexion sur les risques, objet de la présente fiche, mais également une partie dédiée au volet juridique des traitements de données personnelles.
- Mener une analyse de risques[89], même minimale, selon les trois étapes suivantes :

1. Recenser les traitements de données personnelles, automatisés ou non, les données traitées (ex. : fichiers clients, contrats) et les supports sur lesquels ces traitements reposent :
- les matériels (ex. : serveurs, ordinateurs portables, disques durs) ;
- les logiciels (ex. : systèmes d'exploitation, logiciels métier) ;
- les ressources d'informatique en nuage (*cloud*) utilisés (ex. : SaaS, PaaS, IaaS) ;
- les canaux de communication logiques ou physiques (ex. : fibre optique, Wi-Fi, Internet, échanges verbaux, coursiers) ;
- les supports papier (ex. : documents imprimés, photocopies) ;
- les locaux et installations physiques où se situent les éléments précédemment cités (ex. : locaux informatiques, bureaux).

Cette étape mérite d'être menée indépendamment de toute analyse de risques (voir la fiche n°1 - Piloter la sécurité des données).

2. Apprécier les risques engendrés par chaque traitement :

a. Identifier les impacts potentiels sur les droits et libertés des personnes concernées, pour les trois évènements redoutés suivants :
- **accès illégitime à des données** (ex. : usurpation d'identité consécutive à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise) ;
- **modification non désirée de données** (ex. : accusation à tort d'une personne d'une faute ou d'un délit suite à la modification de journaux d'accès) ;
- **disparition temporaire ou définitive de données** (ex. : non-détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).

87 « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) », cnil.fr

88 Article 35 du RGPD.

89 Le vocabulaire utilisé dans la description suivante est tiré des guides AIPD publiés par la CNIL (voir « Les guides AIPD (analyse d'impact relative à la protection des données) », cnil.fr).

b. **Identifier les sources de risques** (qui ou qu'est-ce qui pourrait être à l'origine de chaque évènement redouté ?), en prenant en compte des sources humaines internes et externes (ex. : administrateur informatique, utilisateur, attaquant externe, concurrent) ainsi que des sources non humaines internes et externes (ex. : eau, épidémie, matériaux dangereux, virus informatique non ciblé).

c. **Identifier les menaces** (qu'est-ce qui pourrait permettre que chaque évènement redouté survienne ?). Ces menaces surviennent sur les supports identifiés précédemment (matériels, logiciels, canaux de communication, supports papier, etc.), qui peuvent être :
   - utilisés de manière inadaptée (ex. : abus de droits, erreur de manipulation) ;
   - modifiés (ex. : piégeage logiciel ou matériel ou « *keylogger* », installation d'un logiciel malveillant) ;
   - perdus (ex. : vol d'un ordinateur portable, perte d'une clé USB) ;
   - observés (ex. : observation d'un écran dans un train, géolocalisation d'un matériel) ;
   - détériorés (ex. : vandalisme, dégradation du fait de l'usure naturelle) ;
   - surchargés (ex. : unité de stockage pleine, attaque par déni de service).

d. **Déterminer les mesures existantes ou prévues** qui permettent de réduire chaque risque (ex. : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation).

e. **Estimer la gravité** (impact ou préjudice potentiel pour les personnes concernées) **et la vraisemblance** (probabilité qu'ils se réalisent) des risques, au regard des éléments précédents (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale).

Le tableau suivant peut être utilisé pour formaliser cette réflexion :

Évènement redouté	Impacts sur les personnes	Principales sources de risques	Principales menaces	Mesures existantes ou prévues	Gravité pour les personnes	Vraisem-blance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

3. **Mettre en œuvre et vérifier les mesures prévues.** Si les mesures existantes et prévues sont jugées appropriées, il convient de s'assurer qu'elles soient appliquées et contrôlées (voir la fiche n°1 - Piloter la sécurité des données). Sinon, des mesures supplémentaires doivent être identifiées et mises en œuvre pour réduire la gravité et/ou la vraisemblance des risques associés.

- **Revoir régulièrement l'analyse de risques** et, en particulier, en cas de modification du système ou du contexte du traitement.

Ce qu'il ne faut pas faire

- Oublier l'impact pour les personnes et seulement considérer l'impact pour l'organisme.
- Omettre une partie du traitement (ex. : collecte, partenaires, fin de vie des données) pour mener l'analyse.
- Ajuster les échelles de vraisemblance et de gravité pendant l'analyse au lieu de les définir en amont, en prenant en compte le contexte de l'organisme.

POUR ALLER PLUS LOIN

- Le RGPD introduit les **analyses d'impact relatives à la protection des données** (AIPD) et précise que celles-ci doivent au moins contenir « *une description [...] des opérations [...] et des finalités du traitement [...], une évaluation de la nécessité et de la proportionnalité [...], une évaluation des risques [...] et les mesures envisagées pour faire face aux risques [...] et visant à apporter la preuve du respect du règlement* » (article 35.7).
- La CNIL a publié des guides[90] permettant de mener une AIPD. La CNIL a également publié un logiciel pour faciliter la conduite et la formalisation d'AIPD[91].
- La CNIL a également publié des listes de traitements pour lesquels une AIPD est requise[92] ou non[93].
- **Les audits de sécurité sont un moyen essentiel pour évaluer le niveau de sécurité des systèmes sur lesquels reposent les(s) traitement(s) de données personnelles**. Réalisés de façon périodique, ils permettent de prendre en compte les évolutions du traitement et des menaces. Chaque audit doit donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.
- **L'étude des risques sur la sécurité de l'information[94] peut être menée en même temps que l'étude des risques sur la vie privée**. Ces approches sont compatibles.
- L'étude des risques permet de déterminer des mesures de sécurité à mettre en place. Il est nécessaire de **prévoir un budget** pour leur mise en œuvre.

90 « Les guides AIPD (analyse d'impact relative à la protection des données) », cnil.fr

91 « Outil PIA : téléchargez et installez le logiciel de la CNIL », cnil.fr

92 « Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise », cnil.fr

93 « Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse n'est pas requise », cnil.fr

94 Par exemple à l'aide de la méthode EBIOS RM (voir « La méthode EBIOS Risk Manager », cyber.gouv.fr), la méthode de gestion des risques publiée par l'ANSSI, agence rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN). EBIOS est une marque déposée du SGDSN.

FICHE 21 - CHIFFREMENT, HACHAGE, SIGNATURE

Assurer l'intégrité, la confidentialité et l'authenticité d'une information.

Les **fonctions de hachage** permettent d'assurer **l'intégrité des données. Les signatures numériques,** en plus d'assurer l'intégrité, permettent de vérifier l'authenticité de l'identité du signataire et d'assurer la non-répudiation. Enfin, **le chiffrement**[95] permet de garantir **la confidentialité** d'un message.

Les précautions élémentaires

- **Utiliser un algorithme reconnu et sûr,** par exemple, les algorithmes suivants :
  - SHA-2[96] ou SHA-3[97] comme familles de fonctions de hachage ;
  - bcrypt, scrypt, Argon2 ou PBKDF2 pour stocker les mots de passe ;
  - AES[98] avec un mode de construction approprié (CCM, GCM, ou EAX) ou ChaCha20[99] (avec Poly1305) pour le chiffrement symétrique ;
  - RSA-OAEP[100], ECIES-KEM[101] ou DLIES-KEM[101] pour le chiffrement asymétrique ;
  - RSA-SSA-PSS[100] ou ECDSA[102] pour les signatures.
- **Utiliser des tailles de clés suffisantes** :
  - pour AES, les clés de 128, 192 ou 256 bits sont considérées comme suffisantes ;
  - pour les algorithmes basés sur RSA, il est recommandé d'utiliser des modules et exposants secrets d'au moins 2 048 bits ou 3 072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65 536 bits.
- **Appliquer les recommandations d'utilisation appropriées**, en fonction de l'algorithme utilisé. Les erreurs d'implémentation ont un impact important sur la sécurité du mécanisme cryptographique.
- **Protéger les clés secrètes,** au moins par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr.
- **Rédiger une procédure indiquant la manière dont les clés et certificats vont être gérés** en prenant en compte les cas d'oubli du mot de passe de déverrouillage.

95 Parfois improprement appelé cryptage.

96 Comme défini dans le standard NIST FIPS 180-4.

97 Comme défini dans le NIST FIPS 202.

98 Comme défini dans le NIST FIPS 197.

99 Comme défini dans la RFC 8439.

100 Comme définis dans le standard RSA PKCS#1 v2.2.

101 Comme définis dans la norme ISO/IEC 18033-2.

102 Comme défini dans le NIST FIPS 186-5.

Ce qu'il ne faut pas faire

- Utiliser des algorithmes obsolètes, comme les chiffrements DES et 3DES ou les fonctions de hachage MD5 et SHA-1.
- Confondre fonction de hachage et de chiffrement et considérer qu'une fonction de hachage seule est suffisante pour assurer la confidentialité d'une donnée. Bien que les fonctions de hachage soient des fonctions « à sens unique », c'est-à-dire des fonctions difficiles à inverser, une donnée peut être retrouvée à partir de son empreinte. En effet, ces fonctions étant rapides à l'exécution, il est souvent possible de tester automatiquement toutes les possibilités et ainsi de reconnaître l'empreinte.
- Hacher les mots de passe sans faire intervenir un sel[103].

POUR ALLER PLUS LOIN

- Voir la page dédiée sur le site de la CNIL[104].
- L'ANSSI a publié des **guides**[105] pour aider **les développeurs et administrateurs dans leurs choix d'algorithmes cryptographiques, de dimensionnement et d'implémentation**.
- Lors de la réception d'un certificat électronique, **vérifier que le certificat** contient une indication d'usage conforme à ce qui est attendu, qu'il **est valide et non révoqué, et qu'il possède une chaîne de certification correcte** à tous les niveaux.
- **Utiliser des logiciels ou des bibliothèques cryptographiques ayant fait l'objet de vérifications par des tierces parties à l'expertise avérée.**
- Différentes solutions de chiffrement peuvent être utilisées, telles que :
  - les solutions certifiées ou qualifiées par l'ANSSI[106] ;
  - le logiciel VeraCrypt, permettant la mise en œuvre de conteneurs[107] chiffrés ;
  - le logiciel GNU Privacy Guard, permettant la mise en œuvre de la cryptographie asymétrique (signature et chiffrement)[108].
- Pour les autorités administratives, les annexes du référentiel général de sécurité (RGS)[109] s'appliquent, notamment les annexes B1 et B2 concernant respectivement les mécanismes cryptographiques et la gestion des clés utilisées.

103 On appelle « sel » un aléa différent utilisé pour chaque mot de passe stocké.
104 « Comprendre les grands principes de la cryptologie et du chiffrement », cnil.fr
105 « Mécanismes cryptographiques », cyber.gouv.fr
106 « Visa de sécurité », cyber.gouv.fr
107 Par conteneur, il faut comprendre un fichier susceptible de contenir plusieurs autres fichiers.
108 « The Gnu Privacy Guard », gnupg.org
109 « Le référentiel général de sécurité version 2.0 : les documents », cyber.gouv.fr

FICHE 22 – *CLOUD* : INFORMATIQUE EN NUAGE

Sécuriser les données et les traitements dans un environnement *cloud*.

Le recours à l'informatique en nuage (*cloud*) est perçu comme un moyen plus rapide et flexible de déployer des nouveaux services. Cependant, les risques spécifiques liés au recours au *cloud* doivent être pris en compte lors de la mise en œuvre d'un traitement de données. Le fournisseur du service *cloud* doit présenter des garanties suffisantes pour assurer la mise en œuvre de mesures de sécurité. Toutefois, le client a également un rôle à jouer pour sécuriser ses données et ses traitements dans le *cloud*, non seulement pour les protéger de tiers malveillants mais également du fournisseur lui-même.

Les précautions élémentaires

- **Cartographier les données et les traitements dans le *cloud*** et maintenir à jour cette cartographie. Inventorier également les services *cloud* utilisés (y compris les applications SaaS). Identifier les ressources *cloud* non utilisées ou non surveillées, et le cas échéant, les retirer.
- Évaluer les besoins en sécurité des traitements mis en œuvre puis choisir :
  - **le mode de déploiement des services** (public, privé, hybride, communautaire, multicloud) adapté ;
  - son fournisseur après avoir **évalué le niveau de sécurité proposé** (notamment en termes de sauvegarde, redondance, chiffrement, sécurité physique, sécurité de la maintenance) par rapport à des spécifications de sécurité *cloud* reconnues.
- **Prendre en compte les services *cloud* dans l'analyse de risques** (voir la fiche n°20 - Analyse de risques), mais également dans les PCA/PRA (voir la fiche n°18 - Prévoir la continuité et la reprise d'activité), tout en tenant compte de ses spécificités.
- **Formaliser les obligations de sécurité et la répartition des responsabilités entre le fournisseur et le client dans un contrat** (voir la fiche n°14 - Gérer la sous-traitance).
- Vérifier que tous **les acteurs impliqués** dans la fourniture du service *cloud* **maintiennent le niveau de sécurité recherché** (le fournisseur lui-même ainsi que ses éventuels prestataires).
- **Configurer les outils de sécurité mis à disposition par le fournisseur le cas échéant** (ex. : chiffrement, gestion des accès et des identités, pare-feu, outil anti-DDoS) en respectant la politique interne de sécurité des systèmes d'information.
- Appliquer les **précautions élémentaires** du présent guide aux traitements dans le *cloud*. En particulier :
  - **chiffrer les données au repos et en transit et avoir une gestion des clés cryptographiques appropriée** (voir la fiche n°21 - Chiffrement, hachage, signature). Il est à noter que l'utilisation des services de gestion de clefs proposés par le fournisseur de service implique que ce dernier a la capacité d'accéder aux données ;
  - **attribuer méticuleusement les accès et autorisations** aux seules personnes habilitées à accéder aux ressources (données et applications) dans le *cloud* et appliquer le principe de moindre privilège (voir la fiche n°5 - Gérer les habilitations) ;
  - **authentifier les utilisateurs pour les accès aux services dans le *cloud*** (voir la fiche n°4 - Authentifier les utilisateurs) et n'accorder que les habilitations nécessaires (voir la fiche n°5 - Gérer les habilitations) ;

- **configurer les permissions liées aux ressources dans le *cloud* ;**
- **réaliser des sauvegardes** (voir la fiche n°17 - Sauvegarder) et **vérifier que le fournisseur dispose bien de lieux de sauvegarde géographiquement éloignés des centres de données**.

Ce qu'il ne faut pas faire

- Migrer toutes ses données et traitements dans le *cloud*, sans identifier les données qui ne devraient pas faire l'objet d'un traitement dans le *cloud*, en raison de leur sensibilité.
- Négliger les aspects liés à la sécurité dans la sélection du fournisseur de service *cloud*.
- Présumer que l'obligation de sécurité dans le *cloud* incombe uniquement au fournisseur.
- Avoir un niveau de sécurité plus bas que si les traitements avaient été effectués en local.
- Ne pas considérer les données de télémétrie et de diagnostic ou les données d'usage collectées par le fournisseur dans l'analyse de risques.
- Croire que le chiffrement côté serveur permet de garantir la confidentialité envers le fournisseur.
- Ne pas configurer ou mal configurer les outils de sécurité mis à disposition par le fournisseur[110].
- Partager des moyens d'authentification (ex. : identifiants ou clés d'accès en clair codées en dur dans les fichiers du code source des applications ou des scripts exécutés dans le *cloud*).
- Avoir recours à des services de *cloud* sans garantie quant à la localisation géographique effective des données et sans s'assurer des conditions légales et des éventuelles formalités pour les transferts de données en dehors de l'Union européenne.
- Avoir une stratégie de sauvegarde dans le même centre de données où sont hébergées les données.
- Signer un contrat indiquant que le fournisseur de *cloud* peut accéder aux données et aux systèmes pour certains besoins (y compris sécurité ou obligation légale), sans autorisation du client.

110 « Violation du trimestre : les défauts de configuration des espaces de stockage dans le cloud public », cnil.fr

POUR ALLER PLUS LOIN

- **Auditer régulièrement la sécurité du fournisseur**.
- **Privilégier des fournisseurs adhérant à des codes de conduite RGPD**[111] et s'assurer que ces codes de conduite contiennent des exigences spécifiques en matière de sécurité et des précisions sur les obligations règlementaires spécifiques au *cloud*. Voir notamment les codes approuvés par les autorités après avis du Comité européen à la protection des données (CEPD) : le code CISPE[112] ou le code EU Cloud[113].
- Envisager le recours à un fournisseur qualifié SecNumCloud[114] par l'ANSSI pour le traitement des données d'une sensibilité particulière. La règle R9 de la doctrine « *cloud* au centre »[115] impose le recours à un tel prestataire pour certains acteurs.
- Recourir à un fournisseur certifié hébergeur de données de santé[116] (HDS) pour le traitement de données de santé conformément à l'Article L1111-8 du code de la santé publique. L'Agence du numérique en santé (ANS) publie la liste des hébergeurs certifiés[117]. À noter que la certification a progressivement remplacé l'agrément HDS depuis 2018 et que certains hébergeurs disposent encore d'un agrément[118] valide.
- Consulter la communication[119] sur les pratiques de chiffrement dans le *cloud* public.
- Consulter la communication[120] sur les outils pour la sécurité d'applications web dans le *cloud*.

111 « Ce qu'il faut savoir sur le code de conduite », cnil.fr
112 « La CNIL approuve le premier code de conduite européen dédié aux fournisseurs de services d'infrastructure *cloud* (IaaS) », cnil.fr
113 « EU Cloud COC », eucoc.cloud
114 « L'ANSSI actualise le référentiel SecNumCloud », cyber.gouv.fr
115 « Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre ») », legifrance.gouv.fr
116 « HDS - Certification Hébergeur de Données de Santé », esante.gouv.fr
117 « Liste des hébergeurs certifiés », esante.gouv.fr
118 « Liste des hébergeurs agréés », esante.gouv.fr
119 « Les pratiques de chiffrement dans l'informatique en nuage (cloud) public », cnil.fr
120 « Les outils de sécurisation d'applications web dans l'informatique en nuage (cloud) », cnil.fr

FICHE 23 – APPLICATIONS MOBILES : CONCEPTION ET DÉVELOPPEMENT

Appliquer les principes de sécurité de base au développement des applications mobiles.

Les applications mobiles sont l'un des principaux moyens d'accès à des contenus et des services numériques et impliquent pour la plupart le traitement de données personnelles. Il est nécessaire pour les éditeurs de sécuriser ces traitements et d'offrir la meilleure transparence possible aux utilisateurs.

Les précautions élémentaires

- **Minimiser les traitements de données personnelles mis en œuvre** en s'assurant que chaque type de données collectées est bien nécessaire au fonctionnement de l'application.
- Choisir, lors de leur sélection, les permissions pertinentes au fonctionnement de l'application et impliquant le minimum de collecte supplémentaire, voire proposer des alternatives à l'utilisateur ne reposant pas sur des permissions (ex. : la géolocalisation permet de simplifier une recherche géographique, mais peut être remplacée par la saisie manuelle de l'adresse).
- **Sécuriser les communications**, au moins avec les serveurs, en les encapsulant dans un canal TLS, en respectant le guide TLS de l'ANSSI[121].
- **Stocker les secrets cryptographiques par empaquetage** au moyen d'API permettant l'utilisation des suites cryptographiques incluses dans le téléphone, en privilégiant les protections matérielles telles que le « *Hardware Keystore* »[122] d'Android ou la « *Secure Enclave* »[123] d'Apple.
- **Prendre en compte la possibilité que le système d'exploitation effectue des sauvegardes automatiques des données personnelles**, quelles qu'elles soient. Désactiver les sauvegardes non souhaitées ou procéder à un chiffrement des données sans inclure la clé de chiffrement dans les sauvegardes.
- **Recourir à un moyen d'authentification correspondant au niveau de sécurité recherché** lorsqu'une authentification est nécessaire (ex. : si une personne doit être authentifiée avec certitude, ne pas recourir à un moyen d'authentification biométrique si le dispositif utilisé permet l'enregistrement de gabarits biométriques de plusieurs personnes).

121 « Recommandations de sécurité relatives à TLS », cyber.gouv.fr

122 « Keystore soutenu par le matériel », source.android.com

123 « Secure Enclave », support.apple.com

Ce qu'il ne faut pas faire

- Contractualiser avec un développeur pour la réalisation d'une application sans formaliser avec lui les objectifs et les mesures techniques attendus en termes de sécurité des données et sans préciser que ces exigences sont applicables aux sous-traitants ultérieurs (voir la fiche n°14 - Gérer la sous-traitance).
- Intégrer ou laisser à son sous-traitant la latitude d'intégrer dans son application des éléments de code extérieurs (ou SDK), y compris ceux proposés par les éditeurs des systèmes d'exploitation mobiles, sans s'assurer qu'ils respectent eux-mêmes les précautions de sécurité à l'état de l'art.

POUR ALLER PLUS LOIN

- De manière générale, respecter les niveaux L1 et L2 des recommandations produites par l'OWASP[124].
- **Le modèle de sécurité des applications mobiles ne devrait pas se reposer sur l'intégrité du terminal (via une attestation mise à disposition par le système d'exploitation)**, sauf dans certains cas justifiés. Le service devrait être conçu de manière à maintenir le niveau de sécurité même avec des terminaux considérés corrompus. **Les bonnes pratiques en termes d'API** (voir la fiche n°25 - API : Interfaces de programmation applicative) **devraient être appliquées pour sécuriser les serveurs utilisés par l'application et les protéger contre des éventuelles tentatives d'abus**.
- Privilégier le traitement et le stockage des données de l'utilisateur directement sur son terminal.
- Il est souhaitable que **l'éditeur d'une application mette en place un processus de validation de toutes les modifications apportées au traitement mis en œuvre, notamment en termes de sécurité**, afin d'éviter que des évolutions (ex. : opérations de maintenance, modification de composants externes) ne viennent impacter la sécurité globale du traitement.
- Il est important de mettre en œuvre des processus qui assurent le maintien de la sécurité de l'application au cours du temps, notamment :
  - en adoptant une méthodologie d'intégration et de déploiement continus (CI/CD en anglais) pour permettre des mises à jour fréquentes des applications, notamment en cas de mise à jour de sécurité ;
  - en informant les utilisateurs de la disponibilité de mises à jour critiques (ex. : un bandeau d'information), **voire en bloquant certaines fonctionnalités au niveau du serveur pour les versions non sécurisées de l'application** ;
  - en maintenant **la vigilance relative aux éléments externes intégrés dans les applications**, notamment face au risque d'évolution malveillante dans les SDKs ou les bibliothèques utilisés, via des pratiques de sécurisation de la chaîne d'approvisionnement (ou « *supply-chain security* ») tel que décrit dans les analyses de l'ANSSI[125] ;
  - en s'assurant que le niveau de sécurité attendu puisse rester le même, le plus longtemps possible, indépendamment de la version de l'OS utilisée. De sorte qu'un utilisateur qui ne souhaiterait ou ne pourrait pas accéder à un appareil récent puisse bénéficier d'un niveau de sécurité suffisant.

124 Open web application security project (voir « OWASP MAS Checklist », mas.owasp.org).

125 « Chaine d'attaque sur les prestataires de service et les bureaux d'étude : un nouveau rapport d'analyse de la menace », cyber.gouv.fr

FICHE 24 – INTELLIGENCE ARTICIFICIELLE : CONCEPTION ET APPRENTISSAGE

Se doter des ressources et outils nécessaires pour développer un système d'IA robuste, fiable et performant.

Qu'il s'agisse de l'entraînement d'un nouveau modèle ou de l'intégration d'un modèle existant dans un logiciel ou un écosystème d'applications, le développement d'un système d'intelligence artificielle (IA) nécessite la mise en œuvre de certaines mesures de sécurité spécifiques. **Le volume important de données d'entraînement**, tout comme la **complexité de ces systèmes**, augmentent la surface d'attaque et le risque de défaillance pouvant avoir des conséquences graves **sur la fiabilité du système.** Cette fiche énumère plusieurs recommandations **d'ordre technique et organisationnel** permettant d'atteindre un premier niveau de sécurité.

Les précautions élémentaires

- Constituer une **équipe de développement aux compétences pluridisciplinaires** (analyse et ingénierie des données, interface et expérience utilisateur, contrôle qualité, administration des infrastructures informatiques, équipes métier), veiller à sa formation sur les bonnes pratiques de sécurité et sensibiliser aux vulnérabilités propres à l'IA.
- Mettre en œuvre une procédure obligatoire pour le développement et l'intégration continus, reposant sur des **tests exhaustifs et robustes, des accès soumis à habilitation et à une authentification adaptée aux profils** (voir la fiche n°4 - Authentifier les utilisateurs), notamment pour les modifications apportées au code de production (voir la fiche n°11 - Encadrer les développements informatiques).
- **Vérifier la qualité des données et des annotations, la présence possible de biais, la fiabilité des sources de données**, notamment afin d'éviter que les données ne puissent être manipulées par un tiers (ex. : empoisonnement).
- **Éviter les copies, partielles ou totales, des bases de données** et en restreindre l'accès et l'utilisation aux seules personnes habilitées pour des cas le nécessitant. **Recourir à des données fictives ou de synthèse** dans les autres cas, comme pour les tests de sécurité, l'intégration, ou pour certains audits.
- **Construire un recueil documentaire** à l'intention des développeurs et des utilisateurs du système, portant notamment sur :
  - la conception du système, et notamment les données et modèles utilisés ainsi que les analyses ayant conduit à leur sélection et à leur validation, et les résultats de ces analyses ;
  - le fonctionnement du système durant tout son cycle de vie, ses performances, l'analyse de ses biais et les résultats obtenus, ses conditions d'utilisations et limitations d'usage, comme les cas où la performance peut être insuffisante ;
  - les équipements matériels nécessaires pour l'utilisation du système, la latence attendue ou encore la capacité maximale pour les systèmes accessibles en SaaS.

126 Les attaques par inversion de modèle visent à reconstituer les données ayant servi pour l'apprentissage du système.

- **Vérifier la légitimité des utilisateurs** du système lorsque celui-ci est rendu disponible en tant que service, afin d'éviter une tentative d'attaque telle qu'une **attaque par inversion de modèle**[126] **ou par déni de service**.
- **Prévoir un plan d'audit du système**, portant sur les éléments logiciels, matériels, et sur les mesures organisationnelles telles que **les procédures de supervision humaine du système d'IA**.

Ce qu'il ne faut pas faire

- Entraîner un modèle sur des données **dont la source est inconnue ou n'est pas fiable, ou dont la qualité, et notamment celle de l'annotation, n'a pas été vérifiée**.
- Déployer, partager, diffuser ou rendre accessible un modèle **sans vérifier la qualité des sorties**, et en particulier **l'absence de sorties problématiques** (ex : contenus haineux) **et de données personnelles**, hormis à des fins de tests et d'audit.
- Utiliser un système **sans en connaître les limitations**, ou **sans évaluer les conséquences d'une erreur ou d'un biais**.

POUR ALLER PLUS LOIN

- La CNIL a publié un ensemble de fiches[127] concernant la phase de développement des systèmes d'IA impliquant des données personnelles.
- Les modèles d'attaques sur les systèmes d'IA sont divers et encore peu connus. Le Laboratoire d'innovation numérique de la CNIL (LINC) a publié un premier article recensant ces attaques[128] ainsi qu'un second recensant les bonnes pratiques de sécurité pour s'en prémunir[129] (comme l'apprentissage fédéré, ou la confidentialité différentielle).
- La collecte de données personnelles peut être minimisée grâce à des techniques d'augmentation ou de synthèse de données, ou encore en concentrant la collecte sur des données de qualité.
- Les données utilisées lors de la phase de déploiement peuvent évoluer au cours du temps, et perdre en qualité pour plusieurs raisons (ex. : détérioration d'un capteur, dérive ou empoisonnement des données). Ces évolutions doivent être surveillées.
- Le résultat fourni par le système peut être accompagné d'informations permettant à l'utilisateur de l'interpréter et d'identifier une éventuelle erreur (ex. : score de confiance, carte de saillance).
- Des mesures, telles que des filtres sur les sorties, l'apprentissage par renforcement à partir de la rétroaction humaine (« *reinforcement learning from human Feedback* » ou RLHF) ou encore le tatouage numérique (« *watermarking* ») du contenu généré, permettent de sécuriser les contenus produits par le système.

127 « Les fiches pratiques IA », cnil.fr

128 « Petite taxonomie des attaques des systèmes d'IA », linc.cnil.fr

129 « Sécurité des systèmes d'IA, les gestes qui sauvent », linc.cnil.fr

FICHE 25 - API : INTERFACES DE PROGRAMMATION APPLICATIVE

Veiller à sécuriser des données partagées via l'implémentation d'une API.

Le recours à des interfaces de programmation applicative (API en anglais) constitue une bonne pratique pour de nombreux cas d'usages d'échange de données personnelles, dans la mesure où les API peuvent contribuer à fiabiliser, minimiser et sécuriser ces échanges. La gestion des API doit, pour ce faire, s'inscrire dans la politique de sécurité des systèmes d'information et faire l'objet d'une coordination entre fournisseurs et consommateurs d'API.

Les précautions élémentaires

- Identifier les acteurs et leur **rôle fonctionnel** (détenteur de données, gestionnaire d'API, réutilisateur[130]) afin d'organiser le périmètre d'attribution de chacun en matière **d'accès aux API et aux données**.
- Limiter le partage aux **données strictement nécessaires**, uniquement aux **personnes et pour les finalités prévues**, en application du principe de minimisation.
- Créer une séparation entre les appels aux fonctions courantes de l'API et ceux dédiés à son administration, pour lesquels une authentification robuste apparaît nécessaire.
- Disposer de **journaux pertinents** afin de tracer les échanges (voir la fiche n°16 - Tracer les opérations) et de détecter et réagir en cas d'une utilisation détournée de l'API, d'accès illégitime aux données, d'un dépassement de la capacité d'accès ou de tout autre comportement inhabituel (voir la fiche n°19 - Gérer les incidents et les violations).
- **Maintenir à jour la documentation**. Celle-ci doit inclure le **format des requêtes et des données** concernées par le partage afin de limiter le risque d'une erreur d'interprétation.

Ce qu'il ne faut pas faire

- Conserver **actives les anciennes versions d'une API** qui ne permettent pas le maintien du niveau de sécurité attendu.
- Négliger la sécurité des **clés d'accès aux API**, alors que des solutions de sécurisation des secrets, tel qu'un coffre-fort numérique, existent.

130 Le réutilisateur de données est tout organisme envisageant d'accéder ou recevant des données par voie d'API en vue de les exploiter pour son propre compte.

POUR ALLER PLUS LOIN

- Avant le mise en production d'une API, vérifier sa résistance aux risques publiés par l'OWASP dans son **Top 10 API**[131].
- Voir la recommandation de la CNIL[132] relative au partage sécurisé de données par API.
- L'implémentation de l'API doit être mise en œuvre dans le respect de mesures de sécurité standards telles que la mise en place d'un **mécanisme d'authentification adapté** (voir la fiche n°4 - Authentifier les utilisateurs), la gestion périodique des habilitations (voir la fiche n°5 - Gérer les habilitations) ou encore le **chiffrement des communications** à l'état de l'art.
- Une version « bac à sable » de l'API devrait être mise à disposition afin de permettre des expérimentations et de tester les résultats attendus à partir de données fictives.

131 « OWASP API Security Top 10 », owasp.org

132 « API : les recommandations de la CNIL sur le partage de données », cnil.fr

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE MON ORGANISME

Avez-vous pensé à... ?

FICHES		MESURES	
1	Piloter la sécurité des données	Faire de la sécurité un enjeu partagé et porté par l'équipe dirigeante	☐
		Évaluer régulièrement l'efficacité des mesures de sécurité mises en œuvre et adopter une démarche d'amélioration continue	☐
2	Définir un cadre pour les utilisateurs	Rédiger une charte informatique comprenant les modalités d'utilisation des systèmes informatiques, les règles de sécurité et les moyens d'administration en place	☐
		Donner une force contraignante à la charte et y rappeler les sanctions encourues en cas de non-respect	☐
3	Impliquer et former les utilisateurs	Sensibiliser les personnes manipulant les données	☐
		Adapter le contenu des sensibilisations à la population ciblée et à leurs tâches	☐
4	Authentifier les utilisateurs	Octroyer un identifiant (« *login* ») unique à chaque utilisateur	☐
		Adopter une politique de mot de passe conforme aux recommandations de la CNIL	☐
		Obliger l'utilisateur à changer le mot de passe attribué automatiquement ou par un administrateur	☐
5	Gérer les habilitations	Définir des profils d'habilitation	☐
		Supprimer les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
6	Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session	☐
		Installer et configurer un pare-feu (« *firewall* » en anglais) logiciel	☐
		Utiliser des antivirus régulièrement mis à jour	☐
		Recueillir l'accord de l'utilisateur avant toute intervention sur son poste	☐
7	Sécuriser l'informatique mobile	Sensibiliser les utilisateurs aux risques spécifiques du nomadisme	☐
		Prévoir des moyens de chiffrement des équipements mobiles	☐
		Exiger un secret pour le déverrouillage des smartphones	☐
8	Protéger le réseau informatique	Limiter les flux réseau au strict nécessaire	☐
		Sécuriser les réseaux Wi-Fi, notamment en mettant en œuvre le protocole WPA3	☐
		Sécuriser les accès distants des appareils informatiques nomades par VPN	☐
		Cloisonner le réseau, entre autres en mettant en place une DMZ (zone démilitarisée)	☐
9	Sécuriser les serveurs	Désinstaller ou désactiver les services et interfaces inutiles	☐
		Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installer sans délai les mises à jour critiques après les avoir testées le cas échéant	☐

FICHES		MESURES	
10	Sécuriser les sites web	Sécuriser les flux d'échange des données	☐
		Vérifier qu'aucun secret ou donnée personnelle ne passe par les URL	☐
		Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu	☐
11	Encadrer les développements informatiques	Prendre en compte la protection des données personnelles dès la conception	☐
		Proposer des paramètres respectueux de la vie privée par défaut	☐
		Réaliser des tests complets avant la mise à disposition ou la mise à jour d'un produit	☐
		Utiliser des données fictives ou anonymisées pour le développement et les tests	☐
12	Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées	☐
		Installer des alarmes anti-intrusion et les vérifier périodiquement	☐
13	Sécuriser les échanges avec l'extérieur	Chiffrer les données avant leur envoi	☐
		S'assurer qu'il s'agit du bon destinataire	☐
		Transmettre le secret lors d'un envoi distinct et via un canal différent	☐
14	Gérer la sous-traitance	Prévoir des clauses spécifiques dans les contrats des sous-traitants	☐
		Prévoir les conditions de restitution et de destruction des données	☐
		S'assurer de l'effectivité des garanties prévues (ex. : audits de sécurité, visites)	☐
15	Encadrer la maintenance et la fin de vie des matériels et des logiciels	Enregistrer les interventions de maintenance dans une main courante	☐
		Encadrer les interventions de tiers par un responsable de l'organisme	☐
		Effacer les données de tout matériel avant sa mise au rebut	☐
16	Tracer les opérations	Prévoir un système de journalisation	☐
		Informer les utilisateurs de la mise en place du système de journalisation	☐
		Protéger les équipements de journalisation et les informations journalisées	☐
		Analyser régulièrement les traces pour détecter la survenue d'un incident	☐
17	Sauvegarder	Effectuer des sauvegardes régulières	☐
		Protéger les sauvegardes, autant pendant leur stockage que leur convoyage	☐
		Tester régulièrement la restauration des sauvegardes et leur intégrité	☐

FICHES		MESURES	
18	Prévoir la continuité et la reprise d'activité	Prévoir un plan de continuité et de reprise d'activité	☐
		Effectuer des exercices régulièrement	☐
19	Gérer les incidents et les violations	Traiter les alertes remontées par le système de journalisation	☐
		Prévoir les procédures et les responsabilités internes pour la gestion des incidents, dont la procédure de notification aux régulateurs des violations de données personnelles	☐
20	Analyse de risques	Mener une analyse de risques, même minimale, sur les traitements de données envisagés	☐
		Suivre au cours du temps l'avancement du plan d'action décidé à l'issue de l'analyse de risques	☐
		Revoir régulièrement l'analyse de risques	☐
21	Chiffrement, hachage, signature	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées	☐
		Conserver les secrets et les clés cryptographiques de manière sécurisée	☐
22	*Cloud* : Informatique en nuage	Inclure les services *cloud* dans l'analyse de risques	☐
		Évaluer la sécurité mise en place par le fournisseur	☐
		Veiller à la répartition des responsabilités de sécurité dans le contrat	☐
		Assurer le même niveau de sécurité dans le *cloud* que sur site	☐
23	Applications mobiles : Conception et développement	Prendre en compte les spécificités de l'environnement mobile pour réduire les données personnelles collectées et limiter les permissions demandées	☐
		Encapsuler les communications dans un canal TLS	☐
		Utiliser les suites cryptographiques du système d'exploitation et les protections matérielles des secrets	☐
24	Intelligence artificielle : Conception et apprentissage	Adopter les bonnes pratiques de sécurité applicables au développement informatique	☐
		Veiller à la qualité et l'intégrité des données utilisées pour l'apprentissage et l'inférence	☐
		Documenter le fonctionnement et les limitations du système	☐
25	API : Interfaces de programmation applicative	Organiser et documenter la sécurité des accès aux API et aux données	☐
		Limiter le partage des données uniquement aux personnes et aux finalités prévues	☐

Commission nationale de l'informatique et des libertés
3, Place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

Mars 2024

www.cnil.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS