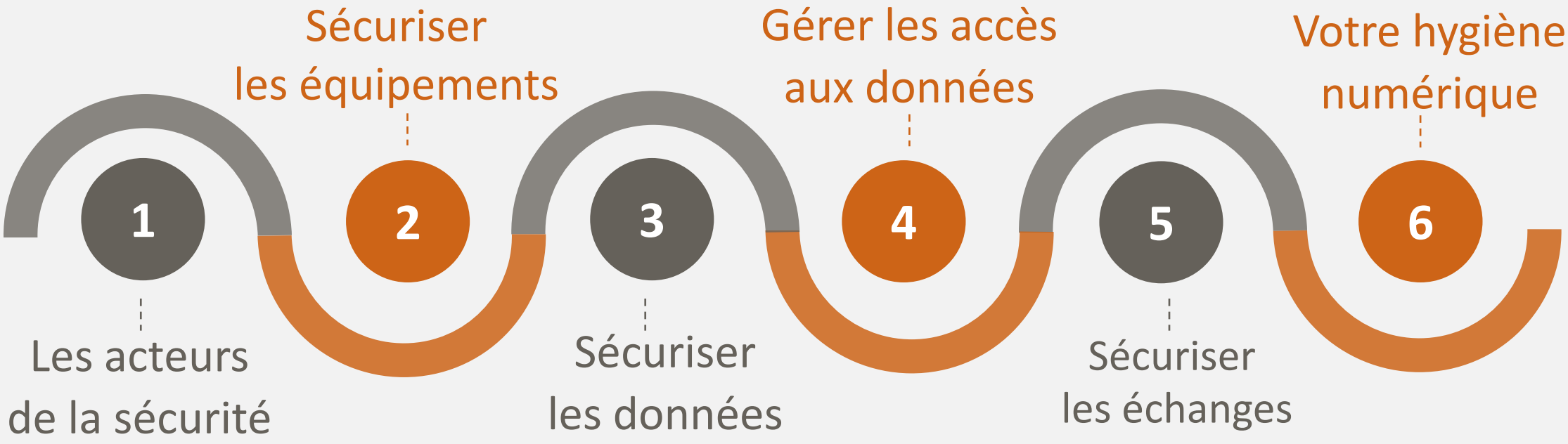
Mate-SHS
Ethique et SHS

Garantir la sécurité et la confidentialité des données

Le 25 mai 2023 - Sophie Corré


Sécuriser
les équipements
Gérer les accès
aux données
Votre hygiène
numérique
1
2
3
4
5
6
Les acteurs
de la sécurité
Sécuriser
les données
Sécuriser
les échanges

Les acteurs de la sécurité

- Les acteurs ayant des missions dans la sécurité des systèmes d'information (SSI)

  ✓ L'**ANSSI** (l'autorité nationale) assure la sécurité des administrations françaises
  ✓ Les responsables sécurité (**RSSI**)
  ✓ Au sein de chaque unité CNRS, désignation d'un(e) chargée(e) de la sécurité des systèmes d'information (**CSSI**)

  Définissent et appliquent une politique de sécurité (**PSSI**)

- **Recommandations, guides, fiches pratiques disponibles en ligne**

  ✓ CNIL (données personnelles)
  ✓ Cybermalveillance.gouv.fr
  ✓ MOOC de l'ANSSI : SecNumAcadémie [9]

- Dans tout projet, la sécurité et la protection des données doivent être pensées dès la conception : **privacy by design**

Sécuriser les équipements

- **Ordinateurs (fixes et portables) fournis par l'établissement/laboratoire** (1)
  - ✓ Authentification à l'ouverture de session
  - ✓ Anti-virus de votre établissement/laboratoire (décontamination des supports amovibles)
  - ✓ Système et applications à jour
  - ✓ Verrouillage automatique de sa session en cas de non-utilisation du poste
  - ✓ Maintenance assurée par le service informatique de votre établissement/laboratoire

- **Chiffrement** (4) **des disques durs** : Veracrypt, Filevault, Bitlocker, PrimX ZoneCentral, dmcrypt
  - ✓ HDD interne/externe, clé usb, tablette, smartphone
  - ✓ Se faire accompagner par son informaticien (séquestre du mot de passe/clé de secours)
  - ✓ Associée à une sauvegarde maitrisée de ses données

- Dictaphone :
  - ✓Privilégier un dictaphone chiffrant en cas de déplacement
  - ✓Purger les données collectées une fois transférées vers son espace de stockage sécurisé

- **Tablette, smartphone :** limiter le stockage au strict nécessaire, secret pour déverrouiller

Sécuriser les données

- **Le stockage sécurisé de vos données sur un serveur institutionnel**
  - ✓ Plusieurs solutions à votre disposition : Scout (pour les toulousains, UT), Sharedocs (IR* Huma-Num), Huma-Num Box (IR* Huma-Num), MyCore (CNRS), Resana (DINUM), etc.
  - ✓ Règle de **sauvegarde 3-2-1**
  - ✓ Tracer les accès aux données avec un système de journalisation

- **Chiffrement des fichiers** : conteneurs veracrypt/zed! (données avec une sensibilité particulière)

- Hébergement, à minima en Europe, au mieux en France

Gérer les accès aux données

L'accès aux données doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées.

Une organisation doit être pensée pour :

- ✓ Définir un **identifiant unique** à chaque collaborateur
- ✓ Définir **quels collaborateurs peuvent accéder à quelles données** (droit de lecture et/ou modification et/ou suppression et/ou téléchargement, …)
- ✓ Organiser vos dossiers pour prendre en compte cet aspect de sécurité
- ✓ **Revue régulière des droits** (départs, nouvelles affectations, changement de rôle) : désactiver des accès, modifier des droits, …

Sécuriser les échanges

- **Mail institutionnel** dans vos échanges

- Chiffrer les documents avant de les transférer à un tiers
- Utiliser un **canal distinct** : envoi du fichier par mail et du mot de passe par sms
- Utiliser un serveur de dépôt de fichiers temporaires : durée limitée, chiffrement de bout en bout comme **Filesender**

- **Logiciel d'enquête en ligne Limesurvey de votre établissement**
  - ✓ Possibilité d'activer le chiffrement de son enquête au niveau de la base de données (si data sensibles)
  - ✓ Désactiver le questionnaire dés la fin de la collecte

- Visio-conférence
  - ✓ Entretiens individuels : Rendez-vous de RENATER
  - ✓ De groupe : BBB (BigBlueButton)
  - ✓ Enregistrement avec OBS Studio

Hygiène numérique

- Complexité des mots de passe [8]
  - ✓ 12 caractères avec majuscules, minuscules, chiffres et caractères spéciaux
  - ✓ 14 caractères avec majuscules, minuscules, chiffres
  - ✓ 1 mot de passe unique pour une application
  - ✓ Tester la robustesse de votre mot de passe

- Gestionnaire de mots de passe [7]
  - ✓ Chiffrement des mots de passe
  - ✓ Protégé dans un coffre-fort numérique
  - ✓ Recommandations : Keepass (Windows), KeepassXC (Windows & Mac os X)

- Navigation sur Internet [13]
  - ✓ Choisir son navigateur (Firefox conseillé)
  - ✓ Utiliser la navigation privée

Hygiène numérique

- Vigilance vis-à-vis du phishing par email

- Dissocier vos données professionnelles de vos données privées [12]

  Votre messagerie personnelle est généralement bien moins sécurisée que votre messagerie professionnelle. Ne pas paramétrer de transfert de l'un vers l'autre : privilégier l'utilisation d'un client de messagerie (Thunderbird) où les 2 comptes sont configurés en IMAP. Cela amène de la souplesse et respecte le cloisonnement pro/perso.

- WIFI public [11]

  ✓ Eviter d'utiliser les wifi publics (restauration rapide, aéroports...).

  ✓ Les universités mondiales mettent à disposition Eduroam qui est sécurisé (avec chiffrement WPA2).

  ✓ Usage systématique du VPN (suivant votre établissement)

Sources

(1) Recherche scientifique (hors santé) : les mesures de sécurité et de confidentialité. (2022, janvier 31). CNIL. Page consultée le 10:46, mai 23, 2023 à partir de https://www.cnil.fr/fr/recherche-scientifique-hors-sante/mesures-de-securite-et-de-confidentialite.

(2) La CNIL publie une nouvelle version de son guide de la sécurité des données personnelles. (2023, avril 03). CNIL. Page consultée le 11:30, mai 24, 2023 à partir de https://www.cnil.fr/fr/la-cnil-publie-une-nouvelle-version-de-son-guide-de-la-securite-des-donnees-personnelles

(3) Guide pratique RGPD | Sécurité des données personnelles. (2023, mars). CNIL. Page consultée le 11:32, mai 24, 2023 à partir de https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_des_donnees_personnelles-2023.pdf

(4) Chiffrement vs cryptage : quelles différences ?. PRIM'X. Page consultée le 11:33, mai 24, 2023 à partir de https://www.primx.eu/fr/abc-chiffrement/chiffrement-vs-cryptage-quelles-differences/

(5) Guide de la sécurité des données personnelles. CNIL. Page consultée le 11:35, mai 24, 2023 à partir de https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

(6) Guide RGPD de l'équipe de développement. CNIL. Page consultée le 11:37, mai 24, 2023 à partir de https://lincnil.github.io/Guide-RGPD-du-developpeur/#Fiche_n%C2%B01%C2%A0:_Identifier_les_donn%C3%A9es_%C3%A0_caract%C3%A8re_personnel

(7) 5 arguments pour adopter le gestionnaire de mots de passe. (2018, octobre 03). CNIL. Page consultée le 11:39, mai 24, 2023 à partir de https://www.cnil.fr/fr/5-arguments-pour-adopter-le-gestionnaire-de-mots-de-passe

(8) Vérifier sa politique de mots de passe. (2022, octobre 17). CNIL. Page consultée le 11:40, mai 24, 2023 à partir de https://www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe

(9) Bienvenue sur le MOOC de l'ANSSI. ANSSI. Page consultée le 11:42, mai 24, 2023 à partir de https://secnumacademie.gouv.fr/

(10) Assistance et prévention du risque numérique au service des publics. Cybermalveillance.gouv.fr. Page consultée le 11:43, mai 24, 2023 à partir de https://www.cybermalveillance.gouv.fr/

(11) Utiliser un Wi-Fi public ? Voici 4 précautions à prendre…. (2017, octobre 25). CNIL. Page consultée le 16:06, mai 24, 2023 à partir de https://www.cnil.fr/fr/utiliser-un-wi-fi-public-voici-4-precautions-prendre

Sources

12) Apprendre à séparer ses usages pro-perso. (2019, novembre 22). Cybermalveillance.gouv.fr. Page consultée le 16:12, mai 24, 2023 à partir de https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso.
13) Cartographie des outils et pratiques de protection de la vie privée. (2018, avril 11). LINC. Page consultée le 16:15, mai 24, 2023 à partir de https://www.cnil.fr/fr/une-cartographie-des-outils-et-pratiques-de-protection-de-la-vie-privee.

Merci de votre attention