1. DOCUMENTATION EXTERNE

Document :

GEN GTA 02 : Guide Technique d'Accréditation – Systèmes d'information dématérialisés

Révision ou Version

- Version 00

Date de publication

- 16/11/2020

Evaluation

- Faite le : 20/11/2020
- Par : STI

2. EVALUATION

Evolution :

A retenir

Cartographie des systèmes d'information

Intérêt de formaliser la cartographie des systèmes d'information

- **La maîtrise du système d'information** : la cartographie permet de disposer d'une vision commune et partagée du système d'information au sein de l'organisme. C'est un outil indispensable au pilotage de l'évolution du système d'information. Elle facilite également la capitalisation d'expérience et la prise de décision grâce à un langage simple et visuel ;
- **La protection et défense du système d'information** : la cartographie permet d'identifier les systèmes les plus critiques et les plus exposés, d'anticiper les chemins d'attaque possibles sur ces systèmes et de mettre en place des mesures adéquates pour assurer leur protection. Elle permet de réagir plus efficacement en cas d'incident ou d'attaque numérique ;
- **La disponibilité du système d'information** : la cartographie permet d'identifier les activités clefs de l'organisme afin d'en assurer la disponibilité (via par exemple un Plan de Continuité d'Activité - PCA ou un Plan de Reprise d'Activité - PRA) et s'impose comme un outil indispensable à la gestion de crise, qu'elle soit numérique ou non.

Pour établir sa cartographie, l'organisme peut suivre les étapes suivantes :

- **Etape 1 – initier la démarche de cartographie** : définir les enjeux de la cartographie, les acteurs à mobiliser, le périmètre du système d'information à représenter, le niveau de détail de l'inventaire et les types de vues à réaliser, les différentes itérations et le calendrier associé ;
- **Etape 2 – définir le modèle de cartographie** : recenser toutes les informations disponibles en rassemblant les inventaires et schémas de représentation du système d'information déjà constitués. Définir le modèle de représentation de la cartographie et des différentes vues ainsi qu'une nomenclature pour les différents objets ;
- **Etape 3 – construire sa cartographie** : en mettant à jour, le cas échéant, les informations recensées. Représenter les différentes vues de la cartographie selon le modèle choisi ;
- **Etape 4 – pérenniser sa cartographie** : diffuser et promouvoir la cartographie au sein de l'organisme. Mettre en place un processus de mise à jour de la cartographie et la gouvernance associée.

Concepts de sécurité de l'information

Pour évaluer la sécurité de son système d'information, l'organisme peut suivre les étapes suivantes :

- **Etape 1** – identifier les failles du système d'information, par exemple en s'appuyant sur la cartographie ;
- **Etape 2** – recenser les informations traitées par l'organisme, via son système d'information. Identifier, parmi les informations recensées, celles qui doivent être sécurisées, par exemple, *via* une analyse de risques (voir § 7.3.1 item « Apprécier et gérer les risques inhérents au système d'information ») ;
- **Etape 3** – analyser, selon les critères DICP, chaque information qui doit être sécurisée ;

- **Etape 4** – si nécessaire, mettre en place les actions de sécurisation des informations.

Pilote du système d'information

Approche PDCA

- PLAN : Identifier les actions à mener
  Les sources possibles d'identification des actions à mener sont :
  - - Les besoins de l'organisme et de ses clients,
  - - Les exigences normatives et règlementaires,
  - - La gestion des risques inhérents au système d'information.

- DO : Sélectionner et mettre en œuvre les dispositifs de maîtrise
- CHECK : Surveiller le système d'information
  - Superviser
  - Auditer
  - réagir.
- ACT : Mettre à jour et améliorer le système d'information

Thématiques importantes vis-à-vis de l'accréditation

- Confidentialité des données
- Intégrité des données
- Disponibilité des données
- Archivage électronique
- Validation du système d'information
- Prestataires externes / services supports
- Comptes rendu des prestations accréditées
  Quelques exemples :
  - Authentification de la personne autorisant le compte rendu de la prestation par l'utilisation
  - Protection du contenu du compte rendu en utilisant un format possédant une clef de chiffrement.
  - Transmission des comptes rendus par messagerie électronique sécurisée (existe en santé) ou non, *via* un coffre-fort numérique, *via* un serveur de résultats sécurisé, *via* un réseau en utilisant un protocole qui garantit la confidentialité et l'authentification du serveur distant
  - Transmission des comptes rendus *via* l'intégration directe des résultats dans le système d'information du client ou de l'autorité.
  - Lorsque les modalités de diffusion ne sont pas réputées sécurisées par une tierce partie (par exemple, l'ANSSI), une convention de preuve peut être signée avec les clients. Cette convention de preuve formalise généralement :
    1. le mode de transmission,
    2. la liste des adresses mails, des adresses serveurs, des numéros de Fax (etc.),
    3. les rôles et responsabilités de chacun vis-à-vis de la confidentialité,
    4. les modalités de réalisation des dossiers tests pour vérifier l'intégrité des données et
    5. la bonne réception par les destinataires identifiés par le client,
    6. le cas échéant, les modalités de signature électronique des documents.

Impact

- /