Audit de la sécurité de la base de données INFOSTAR
Office fédéral de la justice et Centre de service informatique du Département fédéral de justice et police

L'essentiel en bref

Infostar est le registre centralisé pour la saisie électronique des événements d'état civil (naissance, mariage, décès, etc.), mis à disposition des cantons par la Confédération depuis 2005. Il compte près de 1200 utilisateurs répartis dans 142 offices de l'état civil. L'application est exploitée par l'Unité Infostar de l'Office fédéral de la justice (OFJ) et le Centre de service informatique du Département fédéral de justice et police (CSI-DFJP). Un projet de modernisation à hauteur de quelque 23,7 millions de francs est en cours, son achèvement était initialement prévu pour 2023.

Dans cet audit, le Contrôle fédéral des finances (CDF) examine si la sécurité de l'information est assurée dans le cadre de l'exploitation de l'application actuelle. Il vérifie aussi si les lacunes de sécurité sont corrigées dans le projet de modernisation et si la collaboration dans le processus de traitement des cyberincidents fonctionne.

Les bases de la sécurité de l'information sont globalement posées dans le cadre de l'exploitation de l'application actuelle et du projet de modernisation, notamment par leur intégration dans l'infrastructure standard du CSI-DFJP. Des lacunes sont toutefois constatées : la documentation de sécurité et l'analyse des risques de l'application doivent être mises à jour. Le projet « Infostar New Generation » est dans une passe difficile, des aménagements dans l'organisation et la planification sont à apporter et la démarche de test est à améliorer. Enfin, les bases du processus de traitement des cyberincidents sont posées, mais une opérationnalisation renforcée et une meilleure communication sont nécessaires.

Application actuelle : une exploitation stable mais une documentation de sécurité périmée

Par son intégration dans l'infrastructure standard du CSI-DFJP, l'application actuelle bénéficie d'une architecture de sécurité éprouvée. L'authentification des utilisateurs, des droits d'accès, un trafic crypté des informations, des redondances sont, entre autres, mis en œuvre. Des comités d'architecture en suivent l'évolution de manière continue.

Les activités d'exploitation applicative et technique sont décrites et appliquées adéquatement. La gestion des utilisateurs, des protections contre les logiciels malveillants, des sauvegardes de sécurité, la surveillance de l'infrastructure et des tests périodiques de sa solidité sont notamment assurés par des experts en la matière. L'exploitation de la solution actuelle est stable, mais sa maintenance est rendue difficile par la complexité de ses programmes.

La gouvernance de la sécurité est en place, les rôles sont définis, pourvus, et clairement délimités entre intervenants. Toutefois, alors qu'Infostar a des besoins accrus en termes de protection de l'information, la documentation de sécurité est largement périmée. Les responsables peuvent ainsi être amenés à sous-estimer les risques auxquels la solution fait face. Les documents de sécurité doivent être mis à jour et une analyse des risques résiduels doit être entreprise et validée.

Une modernisation en difficulté, une organisation de projet et des tests à améliorer

Lancé en 2018, le projet de modernisation d'Infostar est en cours. Les travaux doivent permettre de bénéficier des évolutions techniques et d'apporter des réponses aux difficultés rencontrées dans les activités de maintenance. Le projet est mené selon une méthodologie agile sous la responsabilité de l'OFJ, qui assure notamment la définition des besoins métier. Le CSI-DFJP est en charge de la réalisation.

Le projet fait face depuis plusieurs mois à des difficultés, un fort taux de rotation du personnel est constaté et le poste de chef de projet est pourvu ad interim. Les responsables ont conscience de la situation délicate et ont défini des mesures immédiates. Une nouvelle organisation a été mise en place, des profils sont recherchés sur le marché de l'emploi. Des retards et des dépassements de coûts sont ainsi prévisibles. Le CDF renonce à émettre une recommandation sur ce point, mais demande que la nouvelle organisation prévoie une intégration renforcée des spécialistes de la sécurité et de l'exploitation.

La nouvelle application est réalisée dans le cadre de l'architecture standard du CSI-DFJP. Elle bénéficie donc des solides composantes de sécurité qui y sont mises en œuvre. Le CDF note toutefois que la démarche de test au sein du projet n'est pas encore entièrement aboutie. Il demande en particulier que la profondeur des tests, leur automatisation, les non-régressions et le traitement des défauts soient repensés.

Traitement des cyberincidents et gestion de la continuité : une intégration à renforcer

Les bases du traitement des cyberincidents sont adéquatement définies. Les rôles et responsabilités dans ce domaine sont exercés activement au CSI-DFJP. Les processus sont décrits, mais les bénéficiaires de prestations ne sont pas assez impliqués dans la mise en œuvre de ces processus. Le Centre de service doit améliorer ce point. Il doit aussi réexaminer s'il est opportun d'élaborer des modèles de réponse selon les types d'incidents. Lors de l'audit, les modalités de la gestion de crise étaient en cours de mise à jour, le CDF renonce donc à émettre une recommandation.

Les systèmes de gestion et de remontée des incidents sont mis en œuvre, de même que les points de contact et les voies de signalement. Lors du déroulement d'un incident, les actions et décisions sont documentées. Les outils de surveillance sont en place, les événements sont journalisés et peuvent être analysés au moyen d'utilitaires.

Les modalités de la gestion de la continuité des activités sont définies dans le giron de chaque unité administrative, mais le CDF voit le risque qu'elles soient insuffisamment intégrées. Il conseille à l'OFJ d'organiser pour Infostar des exercices de gestion de la continuité intégrant bénéficiaires et fournisseurs de prestations. Le but est d'améliorer la coordination entre les parties prenantes et de reconnaître les éventuelles faiblesses dans le processus.