Politique en matière de sécurité de l'information

Objectif stratégique

Garantir la sécurité de l'information constitue une priorité et un objectif important pour le Comité général de gestion et le Comité de direction de l'INAMI qui s'engagent dans ce sens. La responsabilité en incombera à l'Administrateur général. Le domaine stratégique « Amélioration de la gestion des données » figurant dans le Contrat administration en témoigne.

Système de gestion de la sécurité de l'information

Le système de gestion de la sécurité de l'information de l'INAMI garantit la confidentialité, l'intégrité et la disponibilité de toutes les données traitées par l'Institut dans tous les processus de travail des services opérationnels et dans tous les processus de support des services généraux. L'INAMI s'engage à améliorer en permanence ce système de gestion.

Cet engagement repose sur l'application d'une gestion de risques qui tient compte de manière structurelle des dangers et des opportunités engendrés par l'évolution des technologies, de la législation ou d'autres facteurs environnementaux.

ISO 27001

L'INAMI met en place les processus requis en vue d'assurer la concordance du SGSI (système de gestion de la sécurité de l'information décrit dans le Manuel SGSI) par rapport à la norme ISO standard 27001, l'implémentation des mesures de contrôle nécessaires conformément au respect de la déclaration d'applicabilité et l'organisation des actions nécessaires à la réalisation des objectifs mentionnés ci-après.

RIZIV - INAMI

Objectifs de la Sécurité de l'information

La politique en matière de sécurité de l'information est conforme aux normes minimales fixées par la Banque-carrefour de la sécurité sociale.

L'INAMI prévoit l'organisation et l'encadrement nécessaires permettant la mise en œuvre du SGSI.

Pour l'ensemble des processus faisant partie du scope du SGSI, une analyse de risques a été effectuée selon une méthode documentée.

Pour tous les contrôles sélectionnés dans le cadre de la déclaration d'applicabilité, l'objectif à atteindre est le niveau de maturité 3.

Le Comité pour la sécurité de l'information joue un rôle actif dans le cadre du soutien, de l'exécution et de l'amélioration continue de la politique en matière de sécurité de l'information dont il assure la responsabilité.

Le conseiller Sécurité de l'information est responsable de la maintenance du SGSI et en fait régulièrement rapport au Comité pour la sécurité de l'information.

La confidentialité, l'intégrité et la disponibilité de l'information est garantie.

Les aspects relatifs à la sécurité sont repris, en fonction de leur pertinence, dans les descriptions de fonctions, les déclarations de confidentialité, les contrats conclus avec des tiers.

Les ressources de l'entreprise sont répertoriées et la sécurisation est conforme à la classification des données traitées.

La mise à disposition des informations s'effectue au moyen d'un système de gestion des utilisateurs et des accès.

La politique en matière de sécurité de l'information est traduite en directives de sécurité à respecter obligatoirement, qui seront communiquées aux collaborateurs.

Les dispositifs et procédures requis sont mis en place de sorte que les activités de support du Service ICT puissent garantir la sécurité des données en conformité avec le SGSI.

Lors du développement ou de l'acquisition des systèmes d'information, les mesures de sécurité adéquates seront intégrées, à dater du début de la phase projet et pour la durée totale de l'usage opérationnel.

Des accords en matière de sécurité sont intégrés dans une convention, en concertation avec les fournisseurs.

Les infractions à la politique de sécurité sont rapportées, examinées et traitées au moyen d'un processus de gestion des incidents.

Le SGSI est en adéquation avec le contexte légal en vigueur et est soumis, à intervalles réguliers, à un audit interne.