RIZIV - INAMI

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.

Objectifs de la Sécurité de l'information

RIZIV-INAMI veille à ce que cette politique de sécurité de l'information soit revue tous les trois ans - ou en cas de changement majeur - en tenant compte des normes minimales de la Banque Carrefour de la Sécurité Sociale et de la stratégie de l'organisme.

Afin de réduire les risques de sécurité de l'information, RIZIV-INAMI procède régulièrement à des évaluations des risques de sécurité de l'information et traite les risques en conséquence conformément à la méthodologie établie.

Pour s'assurer que tous les employés de RIZIV-INAMI comprennent le besoin de sécurité de l'information, les employés reçoivent régulièrement une formation de sensibilisation à la sécurité de l'information.

Pour assurer la confidentialité, l'intégrité et la disponibilité de tous les actifs couverts par le ISMS, RIZIV-INAMI doit documenter et mettre en œuvre un ensemble approprié de contrôles de sécurité de l'information dans des politiques, des normes et des procédures, dérivées d'audits, d'examens d'incidents, d'évaluations des risques, etc. qui doit être mis à la disposition et communiqué à tous les employés.

Afin d'assurer le respect de la sécurité de l'information, des exigences contractuelles, légales et réglementaires, RIZIV-INAMI intègre les exigences applicables dans sa stratégie et ses opérations quotidiennes.

Afin d'améliorer en permanence l'adéquation, l'adéquation et l'efficacité du ISMS, le CISO procède au moins une fois par an à des revues de direction, en tenant compte :

Le statut des actions des revues de direction précédentes.

- Changements pertinents pour le ISMS.
- Retour d'expérience sur les non-conformités et actions correctives, résultats de surveillance et de mesure, résultats d'audit, réalisation des objectifs.
- Commentaires des parties intéressées.
- Résultat de l'évaluation des risques et de l'état du traitement des risques.
- Possibilités d'amélioration continue.

Les violations de la politique de sécurité sont signalées, font l'objet d'une enquête et sont traitées par le biais d'un processus de gestion des incidents.