Politique du Système de Gestion de Sécurité des Informations - SGSI

La Direction Générale de COSTAISA convient que le développement des activités d'affaires de l'Organisation requiert de garantir, à tout moment, la confidentialité, l'intégrité et la disponibilité des informations objet de traitement au sein de l'Organisation.

Afin de garantir la qualité et l'excellence du traitement des informations, nous avons développé et implanté un Système de Gestion de la Sécurité des Informations (ci-après, SGSI), qui constitue le cadre de référence afin de parvenir à respecter cet engagement.

La portée du SGSI couvre les processus sous-jacents du service d'Exploitation en s'axant sur certains des processus les plus importants, grâce auxquels ils offrent des services à leurs clients : Service de Chaman, Gestion administrative des clients, Service Intranet, Service de courrier électronique, Service de stockage et d'entretien du Web public, Service SIP (Système Intégré de Prévention), Service de Bureau de l'Utilisateur, Gestion des Feuilles de Paie et Personnelle des Clients, et les services d'Hébergement des Systèmes SAP.

La présente Politique de Sécurité du SGSI stipule les directrices et principes suivis par COSTAISA afin de garantir le respect des objectifs de sécurité définis. Ces objectifs sont indiqués ci-après :

- Rendre manifeste l'engagement de la Direction relatif à la sécurité des informations, de manière cohérente avec la stratégie d'affaires.
- Définir, développer et implanter les contrôles techniques et organisationnels nécessaires à garantir la confidentialité, l'intégrité et la disponibilité des informations gérées par COSTAISA.
- Garantir le respect de la législation en vigueur en matière de protection des données de nature personnelle et société de l'information, ainsi que tous les prérequis légaux, réglementaires et contractuels applicables.
- Créer une « culture de sécurité » aussi bien en interne, relative à tout le personnel, qu'en externe, relative aux clients et fournisseurs de COSTAISA.
- Considérer que la sécurité des informations consiste en un processus d'amélioration constante, qui permet d'atteindre des niveaux de sécurité de plus en plus avancés.

Afin de garantir le respect des objectifs de sécurité établis, des règlements et procédures de sécurité ont été développés, lesquels détaillent les mesures techniques, organisationnelles et de gestion nécessaires à garantir le respect des directrices stipulées à la présente Politique.

Le Système de Gestion de Sécurité des Informations demeurera toujours actualisé et sera révisé de manière périodique afin de garantir son adéquation aux besoins spécifiques de COSTAISA. Ce processus impliquera les membres de l'Organisation dès le départ, en stimulant une attitude positive, critique et constructive, à la recherche permanente de l'amélioration et de la qualité du traitement des informations.

Ce processus de révision et d'évaluation a pour cadre un engagement d'amélioration continue du Système de Gestion de la Sécurité des Informations. L'obtention de la certification du SGSI, conformément aux normes ISO/IEC 27001 (Prérequis en matière de Systèmes de Gestion de Sécurité des informations) et ISO/IEC 27002 (Code relatif aux Bonnes Pratiques en matière de Gestion de la Sécurité des Informations), par un organisme indépendant, est le fruit de la sensibilité de la Direction Générale eu égard au traitement et à la gestion des informations, et a pour objet de garantir le respect de niveaux appropriés de confidentialité, intégrité et disponibilité, relatifs à ce traitement.

La Direction, qui s'est engagée à fournir les moyens nécessaires au respect des objectifs de sécurité établis, compte sur la collaboration de tous les employés et acteurs impliqués et assume la responsabilité de la motivation et de la formation de ces derniers, conformément à la présente Politique.

La présente Politique de Sécurité du SGSI est le cadre de référence en matière de sécurité des systèmes d'information de COSTAISA, en établissant les directrices de base pour le traitement sécurisé des informations. Ce cadre technologique, organisationnel et procédurier de sécurité s'appuie sur un ensemble de règlements, procédures, standards et outils de sécurité afin de garantir la protection des actifs d'information.

Julián Casado
Directeur Général