

Politique de Sécurité et Continuité des Activités

La Direction Générale de COSTAISA convient que la fourniture des services aux entreprises de l'Organisation nécessite de garantir à tout moment la confidentialité, l'intégrité et la disponibilité des informations faisant l'objet du traitement et des activités qui les soutiennent.

Afin de garantir la qualité et l'excellence des activités d'appui aux services fournis et au traitement de l'information, un Système de Gestion de la Sécurité de l'Information (ci-après dénommé ISMS) a été mis au point et mis en œuvre, ainsi qu'un Système de Gestion de la Continuité des Activités (ci-après SGCN), qui constitue le cadre de référence pour la réalisation de cet engagement.

Cette Politique de Sécurité et de Continuité des Activités établit les lignes directrices et les principes suivis par COSTAISA pour garantir l'accomplissement des objectifs définis. Ces objectifs sont ceux indiqués ci-dessous:

- Témoigner l'engagement de la Direction Générale en matière de sécurité de l'information et de continuité des activités, conformément à la stratégie de l'entreprise.
- Définir, développer et mettre en œuvre les contrôles techniques et organisationnels nécessaires pour garantir la confidentialité, l'intégrité et la disponibilité des informations gérées dans COSTAISA, ainsi que la continuité des activités.
- Garantir le respect de la législation en vigueur en matière de protection des données à caractère personnel et de la société de l'information, ainsi que de toutes les exigences légales, réglementaires et contractuelles applicables.
- Créer une "culture de sécurité" à la fois en interne, par rapport à tout le personnel, et en externe, liée aux clients et fournisseurs de COSTAISA.
- Considérer la sécurité de l'information et la continuité des activités comme un processus d'amélioration continue permettant d'atteindre des niveaux de sécurité de plus en plus avancés.

Afin de garantir la réalisation des objectifs fixés, des réglementations et procédures ont été élaborées, détaillant les mesures techniques, organisationnelles et de gestion nécessaires pour garantir le respect des directives établies dans la présente Politique.

L'ISMS et le SGCN seront mis à jour en permanence et feront l'objet de révisions périodiques afin de garantir leur adaptation aux besoins spécifiques de COSTAISA. Dans ce processus, les membres de l'Organisation seront impliqués dès le début, et une attitude positive, critique et constructive sera encouragée dans la recherche constante d'amélioration et de qualité dans la fourniture de services aux clients et le traitement de l'information.

Ce processus de révision et d'évaluation fait partie d'un engagement en faveur d'une amélioration continue du SGSI et du SGCN. La certification de l'ISMS par un organisme indépendant est le résultat de la sensibilité de la Direction Générale aux activités qui soutiennent leur survie, ainsi que le traitement et la gestion de

l'information, et vise à garantir la réalisation de niveaux de confidentialité adéquats, intégrité et disponibilité par rapport à ce traitement, ainsi que la continuité des activités.

Cette certification repose sur les normes suivantes:

- UNE-EN ISO / IEC 27001: 2017 (Exigences pour les Systèmes de Management de la Sécurité de l'Information).
- UNE-EN ISO / IEC 27002: 2017 (Code de Bonnes Pratiques pour la gestion de la Sécurité de l'Information).
- UNE-EN ISO / IEC 22301: 2015 (Exigences pour les Systèmes de Gestion de la Continuité des Activités).
- Régime de Sécurité Nationale (DR 3/2010).

La Direction, déterminée à fournir les moyens nécessaires pour atteindre les objectifs fixés, compte sur la collaboration de tous les employés et acteurs impliqués, et assume la responsabilité de leur motivation et de leur formation en ce qui concerne la connaissance et le respect de cette Politique.

Julián Casado Paniagua

Managing Director