

# Politique de sécurité de l'information



## Champ d'action et objectif

La politique de sécurité de l'information est applicable aux actifs d'information et à toute l'organisation, notamment à la structure de gestion et aux collaborateurs, ainsi qu'à toutes les parties concernées liées de quelque forme que ce soit aux systèmes d'information Ascendi, fournisseurs, consultants et partenaires y compris.

Elle a pour objectif de définir les lignes directrices et les orientations en termes d'activité de sécurité de l'information dans l'organisation, afin de garantir un niveau élevé de protection de l'information et des actifs d'information, ainsi que de promouvoir la mobilisation et l'implication de tous, pour assurer le respect des piliers principaux sur lesquels elle repose : confidentialité, disponibilité et intégrité.

## Lignes directrices

- Garantir le respect des exigences commerciales, légales et réglementaires, ainsi que des autres normes nationales et internationales pertinentes en matière de sécurité de l'information et protection de la vie privée;
- Assurer l'amélioration continue du système de gestion de la sécurité de l'information et de la vie privée en tant que partie intégrante des systèmes d'information lors de l'intégralité du cycle de vie des applications et des actifs;
- Définir des orientations et des outils pour la gestion et le contrôle des accès aux systèmes d'information de l'organisation, en garantissant des niveaux appropriés pour la ségrégation de l'accès aux informations critiques relatives à l'entreprise;
- Éviter l'accès non autorisé aux installations, les dommages au niveau des actifs physiques de l'organisation et l'interférence au niveau de son activité normale;
- Garantir une gestion appropriée des incidents et des vulnérabilités pouvant compromettre la sécurité de l'information, la protection des données personnelles ou la continuité des activités;
- Garantir une analyse de risque en matière de sécurité de l'information qui soit périodique, systématique et suive une logique d'amélioration continue, permettant d'identifier les menaces internes et externes potentielles et de prendre les mesures techniques et organisationnelles adaptées;
- Promouvoir la prise de conscience et proposer en permanence des actions de formation sur la sécurité de l'information, afin que tous les collaborateurs internes et externes comprennent l'importance de la sécurité de l'information dans l'exercice de leurs fonctions et responsabilités.