Cybersel
Cyber Risk Assessment and Prevention

Politique de sécurité de l'information

La politique de sécurité des ressources incluses dans le SMSI vise à protéger ces ressources contre les menaces (internes, externes, délibérées, accidentelles) susceptibles de les compromettre, en assurant principalement la confidentialité, l'intégrité et la disponibilité des informations.

En particulier, pour tous les systèmes relevant du SGSI, l'organisation s'engage à garantir que :

- L'information est accessible exclusivement aux personnes autorisées, internes et externes à l'entreprise, garantissant des niveaux de service et une complexité compatibles avec les exigences fonctionnelles des systèmes concernés ;
- Quel que soit le format des informations traitées, leur disponibilité, leur intégrité et leur confidentialité doivent être garanties dans Conformité aux exigences législatives applicables ;
- Une surveillance constante des évolutions des actifs et des technologies est mise en œuvre afin d'identifier rapidement les nouvelles vulnérabilités ;
- Des mises à jour constantes devraient être fournies par des sources faisant autorité et spécialisées dans les questions de sécurité, ainsi que par des groupes de discussion et de formation, afin d'identifier rapidement les nouveaux types de menaces ;
- Une attention particulière doit être portée aux changements des exigences réglementaires et contractuelles et aux priorités connexes en ce qui concerne les nouveaux développements d'applications ;
- La continuité opérationnelle doit être garantie par des interventions ciblées, tant organisationnelles que technologiques, et ces interventions doivent être définies, constamment mises à jour et vérifiées périodiquement ;
- Tout le personnel est formé à la sécurité, informé du caractère obligatoire des politiques de l'entreprise en la matière et sensibilisé aux conséquences de leur violation ;
- Des évaluations périodiques de l'efficacité du SMSI et de la formation du personnel doivent être réalisées au moyen de simulations dans le cadre d'application (évaluation de la vulnérabilité, tests d'intrusion, tests de connaissance des politiques et simulations de violations des politiques) ;
- Il convient d'introduire des indicateurs permettant d'évaluer les performances du système ;
- Les tâches et les environnements liés aux activités critiques (par exemple, le développement et les tests en production) doivent être séparés. et suivant une politique de moindre privilège);
- Les risques doivent être réduits autant que possible à la source ;
- Toute violation de sécurité, réelle ou suspectée, est signalée et fait l'objet d'une enquête ;
- Les incidents de sécurité doivent être rapidement identifiés et gérés, et les autorités compétentes doivent être mobilisées pour ceux qui l'impact a enfreint les exigences légales;
- Évitez d'utiliser des logiciels non autorisés ;
- Des revues périodiques du SMSI sont effectuées en ce qui concerne :
  - ou la vérification de la pertinence et de l'efficacité des contrôles appliqués aux menaces et vulnérabilités identifiées dans le plan traitement des risques ;
  - ou l'impact des contrôles mis en œuvre sur l'efficacité de la gestion ;
  - ou des changements induits par la technologie (vulnérabilités nouvelles ou modifiées, réduction des risques pour les nouvelles connaissances acquises grâce au progrès technologique);
  - ou les modifications apportées à la configuration des systèmes relevant du SGSI ;
  - ou une réévaluation périodique du risque, et notamment en amont et en aval de toute action préventive.

La méthodologie d'évaluation des risques basée sur les lignes directrices ISO/IEC 27005 est également définie et les objectifs ainsi que les paramètres de surveillance associés à la gestion des performances du système sont identifiés.
Les objectifs sont décrits dans le document ISMS_Objectif de sécurité de l'information - KPI.

La responsabilité de la mise en place et de la gestion du SMSI incombe au responsable de la sécurité de l'information.

Turin, le 20 mars 2025

RSSI

Dr Mauro Lisa

PDG

Walter Marmo