Politique de Sécurité de l'Information (SGSI)

ISO 27001:2022

NORDLOGWAY, S.L. a décidé de gérer son **Système de Gestion de la Sécurité de l'Information (SGSI)** conformément aux meilleures pratiques internationales, en s'alignant sur la norme **ISO/IEC 27001** et la **Directive (UE) 2022/2555 (NIS2)**.

OBJECTIF DE LA POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

La présente Politique poursuit un double objectif:

• **Cadre de référence:** établir les bases permettant de protéger les propriétés de sécurité des actifs soutenant les processus de NORDLOGWAY. Ce cadre repose sur les résultats de l'analyse des risques, sur les exigences stratégiques de l'entreprise alignées sur la sécurité et sur les obligations légales et contractuelles. Conformément à ce qui précède, la Politique fixe les principes essentiels qui se développent dans des normes, procédures, instructions techniques, registres et autres documents précisant l'utilisation appropriée de l'information, des systèmes et des actifs qui les soutiennent.

• **Mesures de sécurité:** définir les mesures organisationnelles, physiques et logiques appropriées pour préserver la sécurité de ces actifs, en partant du principe que la sécurité est un processus global et transversal (englobant les composantes techniques, humaines, matérielles et organisationnelles des systèmes d'information et de communication) et qu'elle doit être considérée comme un investissement pour prévenir les impacts négatifs sur l'activité, et non comme un simple coût.

CHAMP D'APPLICATION

La présente Politique s'applique aux systèmes d'information qui soutiennent l'ensemble des processus de NORDLOGWAY dans le cadre de ses activités. Toute réglementation, procédure ou document interne traitant d'aspects spécifiques de la sécurité de l'information devra respecter et se conformer à cette Politique.

La Politique s'applique à **toutes les personnes intervenant dans les activités** et processus commerciaux relevant du périmètre du SGSI : employés, partenaires, collaborateurs et tiers.

PRINCIPES FONDAMENTAUX ET OBJECTIFS

1. Conformité réglementaire: les systèmes d'information doivent se conformer à la législation, aux règlements et aux exigences sectorielles applicables en matière de sécurité de l'information, avec une attention particulière à la protection des données personnelles et à la sécurité des systèmes, des données, des communications et des services électroniques.

2. Gestion des risques: les risques doivent être réduits à des niveaux acceptables, en recherchant un équilibre entre les contrôles de sécurité et la nature de l'information. Les objectifs de sécurité doivent être établis, révisés périodiquement et cohérents avec les exigences de sécurité de l'information.

3. Sensibilisation et formation: des programmes de formation, de sensibilisation et de campagnes d'information en matière de sécurité seront mis en œuvre pour tous les utilisateurs ayant accès à l'information.

4. Confidentialité, intégrité, disponibilité, authenticité et traçabilité:

• **Confidentialité:** seules les personnes autorisées peuvent accéder à l'information.
• **Intégrité:** l'information doit être maintenue exacte et complète, garantissant la précision de son contenu et des processus associés.
• **Disponibilité:** l'information et les services doivent être disponibles lorsque cela est nécessaire, garantissant la continuité des activités à travers des plans de contingence.
• **Authenticité:** l'identité des entités (personnes ou processus) traitant l'information doit être garantie.
• **Traçabilité:** les actions effectuées sur l'information doivent pouvoir être attribuées de manière incontestable à l'entité qui les a réalisées.

5. Proportionnalité: la mise en œuvre des contrôles de sécurité visant à atténuer les risques doit maintenir un équilibre entre les mesures appliquées, la nature de l'information et le risque existant.

6. Responsabilité: tous les membres de NORDLOGWAY doivent agir de manière responsable en matière de sécurité de l'information et se conformer aux normes et contrôles établis.

7. Amélioration continue: la Direction assume la responsabilité de promouvoir l'amélioration continue du Système de Gestion de la Sécurité de l'Information, en veillant à ce que les contrôles mis en œuvre soient régulièrement révisés et renforcés pour anticiper l'évolution du risque et de l'environnement technologique.

Cette Politique constitue le cadre de référence pour l'établissement des objectifs de sécurité.

CONTINUITÉ DES ACTIVITÉS

NORDLOGWAY dispose d'un Plan de Continuité des Activités (PCA) afin de garantir la disponibilité des systèmes et services critiques. En particulier, les éléments suivants ont été définis:

• **Plan de Continuité des Activités (PCA).**
• **Analyse d'Impact sur l'Activité (BIA).**
• **Plan de Reprise après Sinistre (DRP).**

Le Plan de continuité est conçu pour maintenir le fonctionnement des activités clés de soutien de NORDLOGWAY, réduire les dommages et l'impact des incidents imprévus sur les services, et accélérer la reprise des activités.

TIERS

Tout tiers ayant accès aux informations de NORDLOGWAY dans le cadre d'une prestation de services doit avoir connaissance de la présente Politique et de sa réglementation associée, et s'engager à en respecter les obligations. Ces tiers peuvent développer leurs propres procédures opérationnelles afin de s'y conformer. Des procédures spécifiques de notification et de résolution des incidents seront établies. Le personnel de ces tiers devra être adéquatement sensibilisé à la sécurité, au moins au même niveau que celui requis par la présente Politique.

CONTACT

Pour toute information complémentaire concernant cette Politique ou pour soumettre des suggestions, veuillez écrire à: **info@nordlogway.com**

Víctor Gastón Puyo
Directeur Général de Nordlogway
10 juillet 2025