POLITIQUE DE SÉCURITÉ DE L'INFORMATION

EJASO PENAL RETAIL est une société spécialisée dans la prestation de services de conseil en matière juridique de toute nature, y compris dans les domaines économique, fiscal, financier et commercial, dans la mesure où la loi le permet, tant auprès des personnes physiques que des personnes morales.

La direction **d'EJASO PENAL RETAIL** a décidé de mettre en place un système de gestion de la sécurité de l'information basé sur la norme ISO 27001 dans le but de préserver la confidentialité, l'intégrité et la disponibilité des informations et de les protéger contre un large éventail de menaces. Ce système de gestion vise à assurer la continuité des activités, à minimiser les dommages, à maximiser le retour sur investissement et les opportunités commerciales, ainsi qu'à favoriser l'amélioration continue.

La direction **d'EJASO PENAL RETAIL** est consciente que l'information est un actif de grande valeur pour l'organisation et qu'elle nécessite donc une protection adéquate.

La direction **d'EJASO PENAL RETAIL** établit comme objectifs fondamentaux, point de départ et fondement des objectifs et principes de la sécurité de l'information les éléments suivants :

- La protection des données à caractère personnel et de la vie privée des personnes
- La sauvegarde des archives de l'organisation
- La protection des droits de propriété intellectuelle
- La documentation de la politique de sécurité de l'information
- L'attribution des responsabilités en matière de sécurité
- La formation et le perfectionnement en matière de sécurité de l'information
- L'enregistrement des incidents de sécurité
- La gestion de la continuité des activités
- La gestion des changements susceptibles de survenir au sein de l'entreprise en matière de sécurité

La direction **d'EJASO PENAL RETAIL,** par l'élaboration et la mise en œuvre du présent système de gestion de la sécurité de l'information, prend les engagements suivants :

- Développer des produits et des services conformes aux exigences législatives, en identifiant à cet effet les législations applicables aux secteurs d'activité développés par l'organisation et inclus dans le champ d'application du Système de gestion de la sécurité de l'information.
- Établir et respecter les exigences contractuelles avec les parties prenantes.
- Définir les exigences en matière de formation à la sécurité et dispenser la formation nécessaire en la matière aux parties prenantes par la mise en place de plans de formation.
- Prévenir et détecter les virus et autres logiciels malveillants, par l'élaboration de politiques spécifiques et la conclusion d'accords contractuels avec des organisations spécialisées.
- Gérer la continuité des activités en élaborant des plans de continuité conformes à des méthodologies de renommée internationale.
- Définir les conséquences des violations de la politique de sécurité, qui seront reflétées dans les contrats signés avec les parties prenantes, les fournisseurs et les sous-traitants.
- Agir à tout moment dans le respect de la plus stricte éthique professionnelle.

Cette politique fournit le cadre de référence pour l'amélioration continue du système de gestion de la sécurité de l'information et pour établir et réviser les objectifs dudit système. Elle est communiquée à l'ensemble de l'organisation par le biais du système de gestion documentaire mis en place au sein de l'organisation et de sa publication sur des panneaux d'information. Elle est révisée chaque année afin d'en vérifier l'adéquation et de manière extraordinaire en cas de situations particulières et/ou de changements substantiels dans le système de gestion de la sécurité de l'information, et est mise à la disposition du grand public.

Guillermo González Morín

Responsable de la sécurité de l'information