POLITIQUE GÉNÉRALE DU SYSTÈME INTERNE D'INFORMATIONS ET DÉFENSE DE LA INFORMATEUR

INDICE

1 - INTRODUCTION

La transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 en droit espagnol avec la loi 2/2023 du 20 février réglementant la protection des personnes qui signalent des violations
La réglementation et la lutte contre la corruption impliquent l'incorporation d'instruments spécifiques pour que ceux qui ont connaissance d'actions illégales ou irrégulières puissent fournir des données et des informations utiles, garantissant ainsi une protection complète et efficace desdits informateurs.

À cet égard, les réglementations susmentionnées régissent les exigences minimales que doivent respecter les différents canaux d'information internes et externes, ainsi que le régime spécial de protection des informateurs qui agissent de bonne foi et avec une conscience honnête, et qui sont désintéressés.

Conformément à ce qui précède, LE GROUPE a mis en place un Système Interne de
Le Système d'Information SIIF (SIIF) est un axe fondamental de supervision, de contrôle et de prévention en matière de conformité réglementaire. Il constitue un canal privilégié et un outil indispensable pour diffuser efficacement l'information, afin de renforcer la culture de l'information au sein de l'organisation.

Le SIIF a été conçu comme un outil de contrôle et de prévention, comprenant des canaux d'information gérés en interne et par une société externe spécialisée. Ces canaux bénéficient des plus hauts niveaux de professionnalisme, d'expérience, d'indépendance, de confidentialité et de conformité aux réglementations en matière de protection des données et autres cadres réglementaires applicables. De plus, le SIIF garantit les principes fondamentaux d'anonymat, de tenue de registres appropriée, de conservation et de non-altération, de prévention des conflits d'intérêts, de protection des lanceurs d'alerte et d'interdiction de représailles.

Conformément à la loi susmentionnée, il est essentiel que le SIIF dispose d'un
Une politique définissant les principes généraux du système et la protection des informateurs, dûment diffusée au sein du Groupe, constitue donc, avec la Procédure de gestion des informations reçues, un élément essentiel de la configuration et du fonctionnement du SIIF.

2 - PRINCIPES D'ACTION ET GARANTIES ESSENTIELLES

Le Système d'Information Interne (SIIF) est l'un des axes principaux des systèmes Conformité réglementaire et prévention de la criminalité. Conformément aux normes les plus strictes en matière de diligence raisonnable, le Groupe a mis en place auprès du SIIF une série de garanties pour garantir son efficacité, avec la collaboration et le soutien de l'expert externe BONET Consulting. Plus précisément, les principes fondamentaux et les garanties fondamentales régissant les processus et les actions du Groupe concernant le SIIF sont les suivants :

- **Indépendance, autonomie, impartialité et absence de conflits d'intérêts**Lors de la réception et du traitement des informations relatives aux violations, des mécanismes de réponse ont été définis pour gérer et contrôler les conflits d'intérêts potentiels et/ou le manque d'indépendance lorsque les personnes responsables de la gestion, du contrôle et/ou de la supervision présentent certaines caractéristiques compromettant et limitant l'exercice de leurs fonctions. De plus, toutes les communications reçues sont analysées conformément aux exigences d'indépendance requises, garantissant ainsi l'équité et la justice dans leur traitement.

- **Professionnalisme et expérience**:Les professionnels possédant une expertise en matière de conformité réglementaire, de prévention de la criminalité et de bonne gouvernance sont responsables de la gestion et du traitement appropriés des communications, préservant ainsi les droits des informateurs et des accusés.

- **Exhaustivité, intégrité et confidentialité des informations**Les participants aux différentes phases de l'enquête sont tenus à une obligation de confidentialité concernant toute information à laquelle ils pourraient avoir accès ou dont ils auraient connaissance dans l'exercice de leurs fonctions. De plus, l'accès non autorisé à ces informations est empêché et leur conservation sécurisée et à long terme est assurée par la création de copies de sauvegarde et de dossiers indépendants.

- **Protection des données et confidentialité des communications**Le traitement des données est effectué conformément aux mesures et politiques de protection des données personnelles les plus strictes, conformément à la réglementation applicable en matière de protection des données personnelles. De même, il existe un devoir de confidentialité concernant tout aspect lié aux informations communiquées.

- **Anonymat**:La possibilité de soumettre et de traiter ultérieurement des communications anonymes est prévue, ainsi que l'obligation générale de préserver l'identité de l'informateur qui s'est identifié lors de la communication, en le gardant anonyme et en ne révélant pas son identité à des tiers.

- **Utilisation abordable, simplicité et gratuité :**La simplicité de communication est garantie, permettant un accès universel au système sans frais associés, et l'application effective des principes de légalité et d'éthique qui régissent les activités du Groupe.

- **Enregistrement adéquat et indépendant**Un registre confidentiel des informations reçues et des enquêtes internes auxquelles elles ont donné lieu est tenu, garantissant leur traitement, leur gestion et leur non-altération, de manière indépendante et sans conflit d'intérêts, pendant la durée nécessaire et proportionnée à la législation en vigueur. En aucun cas, les données ne seront conservées plus de dix ans.

- **Bonnes pratiques de surveillance et d'enquête**Afin de vérifier la véracité des communications, de garantir la collecte adéquate des preuves et de garantir les droits des personnes concernées, le cycle de vie des communications sera encadré par une procédure interne efficace et transparente. Ces pratiques seront documentées dans la Procédure de gestion des informations reçues.

- Protection des lanceurs d'alerte et des personnes concernées : Les personnes qui signalent ou divulguent des violations ont droit à des mesures de protection et ne subiront aucune représaille ni conséquence négative pour leur coopération, y compris des menaces ou tentatives de représailles. De même, les personnes concernées par le signalement bénéficient des mêmes protections que les lanceurs d'alerte : leur identité est protégée et la confidentialité des faits et informations relatifs à la procédure est garantie.

- **Action diligente, responsabilité et bonne foi de l'informateur**L'utilisation du système repose sur les principes de responsabilité, de diligence et de bonne foi. Chaque informateur doit donc avoir des motifs raisonnables de croire que l'information est vraie au moment du signalement. Le signalement de faits infondés, faux ou déformés, ainsi que la soumission d'informations obtenues illégalement, avec malveillance ou de manière moralement malhonnête, constituent une violation du principe de bonne foi et peuvent entraîner des sanctions disciplinaires.

3 - RESPONSABLE DU SYSTÈME D'INFORMATION INTERNE

Pour l'efficacité du Système d'Information Interne (SIIF), il est essentiel de désigner une personne responsable de son bon fonctionnement, de son organisation et du traitement rigoureux des informations. Cette personne sera également chargée d'assurer la communication et la diffusion adéquates du SIIF, ainsi que d'élaborer et de mettre à jour le plan de formation correspondant.

L'organe d'administration ou de direction du Groupe est chargé de la nomination et de la notification à l'autorité compétente de l'organisme individuel ou collégial chargé de la gestion dudit système et de sa révocation ou de sa cessation (ci-après, le Gestionnaire du Système).

Le Responsable du Système exerce ses fonctions de manière indépendante et autonome par rapport aux autres organes organisationnels du Groupe, évitant ainsi tout conflit d'intérêt potentiel dans l'exercice ordinaire de ses fonctions.

Toutefois, le gestionnaire du système peut s’appuyer sur d’autres tiers pour un soutien spécialisé et/ou pour répondre aux exigences d’indépendance afin d’assurer la bonne exécution de ses fonctions.

Plus précisément, pour mener à bien ses fonctions, le gestionnaire du système coordonnera les sujets suivants :

A- Le responsable des ressources humaines, lorsque des mesures disciplinaires peuvent être appropriées à l'encontre des personnes concernées et/ou coordonne la mise en œuvre de mesures de protection.

B- Les responsables de la conformité réglementaire et/ou les services juridiques du Groupe, le cas échéant, doivent adopter des mesures de conformité légales ou réglementaires qui doivent être prises en considération par eux en relation avec les communications reçues dans le SIIF.

C- Les responsables du traitement qui peuvent être désignés.

D- Le délégué à la protection des données.

E- Autres personnes et/ou entités impliquées dans la gestion du SIIF.

4 - AUTORITÉ INDÉPENDANTE DE PROTECTION DES INFORMATEURS

Le Système d'Information Interne du Groupe (SIIF) est le moyen prioritaire et obligatoire pour signaler les comportements illicites ou les violations connus, car il garantit l'adoption appropriée de mesures de protection et favorise une culture de l'information au sein de l'organisation.

Toutefois, d'autres canaux d'information « externes » ont été créés pour offrir aux citoyens un moyen alternatif de soumettre des communications et/ou des plaintes dans les cas où les canaux internes ne respectent pas les garanties requises par la réglementation applicable, les mesures de protection pertinentes ne sont pas appliquées ou les individus sont exposés à des représailles en raison de leur statut d'informateurs.

Par conséquent, toute personne peut signaler directement à l'Autorité indépendante de protection des lanceurs d'alerte (AIWP) toute action ou omission constituant une violation de la loi, par le biais du canal d'information externe de cette autorité publique spécialisée. L'accès à ce canal d'information externe et les coordonnées de l'Autorité sont publiés sur son site web.

5 CONFIDENTIALITÉ ET PROTECTION DES DONNÉES PERSONNELLES

Le traitement des données personnelles issues du Système d'Information Interne (SIIF) sont régis par les dispositions du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la Loi organique 3/2018 du 5 décembre et de la Loi organique 7/2021 du 26 mai. Par conséquent, lors du recrutement, les personnes intéressées sont informées du traitement de leurs données et de leurs droits, conformément à la réglementation en vigueur.

Conformément au principe de minimisation des données, les données personnelles collectées sont celles qui sont nécessaires et pertinentes au traitement de la communication.
Si des données sont collectées accidentellement et ne sont pas nécessaires à la compréhension et à l'enquête sur les actions ou omissions, elles seront supprimées sans délai. De plus, elles seront conservées pendant la durée nécessaire à la décision d'ouvrir ou non une enquête.

De plus, la conception du SIIF garantit la confidentialité de l'identité de l'informateur et de tout tiers mentionné dans la communication, ainsi que des actions menées dans le cadre de sa gestion et de son traitement. À cet égard, l'accès aux données personnelles et autres informations contenues dans le système est limité aux personnes responsables de sa gestion, dans le cadre de leurs attributions. Par conséquent, des mesures techniques et organisationnelles appropriées sont mises en place pour protéger l'identité des personnes concernées et empêcher l'accès par des personnes non autorisées.

Pour toute question ou demande concernant le traitement des données personnelles effectué au sein des entités du Groupe en relation avec le SIIF, toute personne intéressée peut contacter le délégué à la protection des données désigné en utilisant les coordonnées précédemment fournies et mises à sa disposition.

6 MESURES DE PROTECTION

Les personnes qui signalent ou divulguent des violations en utilisant le système interne Les informations (SIIF) du Groupe bénéficient d'une protection, dans les mêmes conditions
que ceux qui signalent par des canaux externes, à condition qu'ils aient des motifs raisonnables de croire que les informations mentionnées sont vraies au moment de la communication ou de la divulgation, même s'ils ne fournissent pas de preuves concluantes.

À cet égard, les actes constituant des représailles, y compris les menaces et les tentatives, contre les personnes qui soumettent une communication sont expressément interdits. Les représailles sont définies comme suit :

a- Actes ou omissions interdits par la loi.

b- Actes ou omissions qui entraînent directement ou indirectement un traitement défavorable, désavantageant une personne par rapport à une autre.

À titre d'exemple et non limitatif, sont considérés comme des représailles :

- Suspension du contrat de travail, licenciement ou rupture de la relation, résiliation anticipée, annulation du contrat de travail et/ou commercial, mesures disciplinaires, blâme ou autre sanction, rétrogradation ou refus de promotion, modification substantielle des conditions et non-conversion d'un contrat temporaire en contrat permanent, ou mesures équivalentes.

- Dommage (y compris atteinte à la réputation), perte économique, coercition, intimidation, harcèlement ou ostracisme.

- Évaluations ou références négatives concernant le travail ou la performance professionnelle.

- Listes noires ou diffusion d'informations qui entravent ou empêchent l'accès à l'emploi/aux contrats de travaux ou de services.

- Refus ou annulation de licence ou de permis.

- Refus de formation.

- Discrimination, traitement défavorable ou injuste.

- Refus d'incitations, d'avantages, de primes, de commissions et de tout autre type de rémunération.

- Résiliation anticipée, suspension, modification ou annulation de contrats de biens ou de services.

Ces actes seront nuls et non avenus et donneront lieu, le cas échéant, à des mesures disciplinaires ou de responsabilité, pouvant aller jusqu'à l'indemnisation des dommages causés à la partie lésée.

Afin de garantir le droit à la protection de l'informateur et des personnes concernées par la communication, le Groupe a mis en place les mesures techniques et organisationnelles suivantes, qui sont appliquées dès la réception de la communication :

1- Configuration du SIIF : Le SIIF a été conçu avec des mesures techniques et organisationnelles appropriées pour garantir la protection de l'identité de l'entité déclarante, ainsi que des données et informations issues des communications soumises. À cet égard, le Groupe a mis en place plusieurs canaux de signalement internes permettant de soumettre des communications de manière anonyme. Ces canaux sont :

- Canal en ligne/numérique : Plateforme numérique pour la soumission de communications écrites.

- Canal face à face : Système permettant de recevoir des communications par le biais de réunions en face à face ou de vidéoconférences.

Quel que soit le canal utilisé, le SIIF garantit une application efficace
des principes fondamentaux et des garanties spécifiés dans la présente politique, afin de
se conformer aux exigences du cadre réglementaire et protéger les droits des
informateurs et personnes concernées.

2- Responsable SIIF : Afin de garantir la bonne application du SIIF, le Groupe a désigné un Responsable dont le rôle est de superviser, de suivre et de contrôler son fonctionnement. À cet effet, le Responsable, en collaboration avec l'expert externe, adoptera les mesures de protection nécessaires et assurera leur suivi et leur mise en œuvre. La participation de l'expert externe confère aux fonctions du Responsable les éléments d'autonomie et d'indépendance requis par la réglementation en vigueur.

   De même, le Responsable sera chargé de procéder à une analyse préliminaire des communications reçues afin de déterminer l'opportunité d'adopter des mesures de protection spécifiques pour l'informateur et/ou les tiers concernés. De plus, selon la nature et la portée de l'information, le Responsable bénéficiera du soutien et des conseils des responsables des différents services opérationnels du Groupe pour mener à bien l'enquête. Il pourra également faire appel à d'autres tiers spécialisés dans les questions nécessitant une expertise.

3- Conservation, gestion et sécurité des informations du SIIF : Le Groupe dispose d'un système de gestion documentaire configuré avec des mesures de sécurité et de contrôle appropriées pour démontrer l'efficacité du SIIF. Il convient de noter que ce système comprend des processus anonymes pour empêcher l'identification des informateurs. De plus, le Groupe a adopté des mesures techniques raisonnables pour sécuriser le stockage, la récupération et la destruction des informations, ainsi que la mise en œuvre de contrôles d'accès pour empêcher toute utilisation non autorisée.

Toutefois, les informations fausses, déformées, manifestement dénuées de crédibilité ou de fondement, ou dont il existe des motifs raisonnables de croire qu'elles ont été obtenues par la commission d'un crime, sont exclues de cette protection. En effet,

toute communication doit être faite de bonne foi et, par conséquent, l'informateur doit avoir des motifs raisonnables de croire que l'information est vraie au moment de la communication. En résumé, le principe de bonne foi exige qu'en aucun cas on ne puisse conclure à une fausseté, à une fausse déclaration ou à une intention de se venger ou de nuire à un tiers.

Il est important de rappeler que les mesures de protection ne s'appliquent pas uniquement aux informateurs. Les personnes concernées par les faits décrits dans la communication (personnes concernées) bénéficient également d'une protection particulière contre le risque que les informations, même apparemment véridiques, puissent avoir été manipulées, être fausses ou répondre à d'autres motivations. Pendant le traitement de l'affaire, ces personnes bénéficient du droit à la présomption d'innocence, à la protection judiciaire et à la défense, à l'accès au dossier, ainsi qu'à la confidentialité des faits et des détails de la procédure et à la protection de leur identité. En bref, elles bénéficient de la même protection et des mêmes droits que l'informateur.

7 - RÉGIME DISCIPLINAIRE

Le non-respect des réglementations applicables et les comportements contraires aux instructions, politiques, codes, procédures et protocoles du Groupe entraîneront l'application de mesures disciplinaires aux niveaux du travail et commercial, en coordination avec les dispositions de la convention collective applicable, du statut des travailleurs et des autres réglementations applicables.

Le Groupe notifiera et sanctionnera toute action ou omission contraire à la présente Politique commise par des employés, des collaborateurs ou tout membre lié au Groupe et, en particulier :

- Défaut de signaler toute suspicion ou connaissance de violations ou de manquements au cadre réglementaire et aux protocoles et normes internes du Groupe via le SIIF.

- Toute tentative ou action efficace visant à entraver la soumission des communications ou à empêcher, contrecarrer ou ralentir leur suivi.

- L’utilisation du SIIF de mauvaise foi, par exemple en fournissant des informations ou des documents dont on sait qu’ils sont faux.

- Toute représaille contre les informateurs ou autres personnes concernées découlant de la communication.

- La violation des garanties de confidentialité et d’anonymat, la révélation de l’identité des personnes concernées et la violation du devoir de confidentialité des informations.

- Manquement à l'obligation de coopérer à l'enquête sur les informations.

8 - COMMUNICATION, RÉVISION ET MISE À JOUR

La présente Politique, ainsi que toutes les informations nécessaires concernant l'utilisation du Système d'Information Interne (SIIF) mis en œuvre, sont disponibles dans une section distincte et facilement identifiable, afin que toutes les parties intéressées y aient accès de manière claire et aisée. Toutefois, toute personne peut demander des informations complémentaires au Groupe en contactant le Responsable du traitement.

Le Responsable du Système révisera périodiquement et, le cas échéant, proposera des mises à jour à l'organe d'administration ou de gouvernance du Groupe afin d'adapter la présente Politique aux circonstances et aux changements éventuels, ainsi qu'à la réglementation ou à la jurisprudence. L'objectif est d'aligner le SIIF sur les exigences réglementaires les plus strictes pour son bon fonctionnement et son efficacité.

De même, le Groupe est ouvert à toute suggestion et/ou proposition susceptible d’améliorer sa conduite éthique et de favoriser une culture de conformité réglementaire, soulignant la nécessité pour tous les employés et membres du Groupe ou des tiers de collaborer dans le respect de ses valeurs et principes.

9 - CANAUX D'INFORMATION INTERNES

Afin de se conformer aux dispositions de la loi 2/2023, le Groupe a mis en place un système conforme aux exigences techniques et procédurales établies par cette loi pour le bon traitement des communications. L'objectif est d'offrir aux informateurs un environnement de communication sécurisé, confidentiel, voire anonyme, avec le Groupe, et de traiter les informations de manière efficace, professionnelle et indépendante.

À cette fin, le Groupe s'est doté de ressources matérielles, techniques et humaines pour mettre en place différents canaux internes permettant la transmission de communications écrites ou orales. Ces canaux sont configurés, conçus et soutenus par un expert externe afin d'assurer les plus hauts niveaux de professionnalisme, d'expérience, d'indépendance, de confidentialité, de protection des données et des lanceurs d'alerte, ainsi que d'autres domaines applicables à ces types de canaux.

Il est à noter que toute information fournie via l'un de nos canaux internes sera traitée de manière confidentielle et ne sera accessible qu'au personnel autorisé pour sa bonne gestion et son traitement.

Les canaux à disposition de tout employé ou tiers associé au Groupe pour soumettre des communications sont détaillés ci-dessous :

https://www.corporate-line.com/cnormativo-salvat

Canal On-line/Digital CORPORATE LINE Canal de comunicaciones

Le Groupe dispose d'un outil numérique permettant de soumettre des communications écrites via un formulaire permettant l'ajout de fichiers en pièce jointe. Une fois le formulaire rempli, l'outil génère automatiquement un code permettant un suivi et une gestion appropriés par le responsable du traitement.

Une confirmation est également envoyée au déclarant concernant la saisie et l'enregistrement de la communication dans le système. Cette confirmation contient un résumé des informations fournies, ainsi que le code permettant au déclarant de suivre les informations.
Cet outil dispose de mesures de sécurité qui garantissent la protection des
Les informations, l'identité de l'informateur et des personnes concernées, ainsi que la confidentialité de l'ensemble du processus de gestion et de traitement des communications, sont garanties. À cet égard, le Groupe garantit un environnement de communication sécurisé et efficace pour la réception des communications.

L'outil permet également la soumission anonyme de communications.
Grâce au système de communication et de surveillance disponible, l'informateur et le gestionnaire du système peuvent communiquer via l'outil, que la communication ait été soumise de manière anonyme ou non.

Le lien pour accéder à cet outil et son périmètre d'utilisation sont disponibles sur le site internet du Groupe.

Canal Presencial / "Face to face"

- Téléphone : 911087727 / 930460116

  Les heures de service des informateurs sont les suivantes :

  - Du lundi au jeudi de 8h30 à 14h00 et de 15h00 à 18h00.
  - Vendredi de 8h30 à 14h30

- E-mail: salvatlogistica@sistema-interno-información.com

Le Groupe met également à la disposition de ses collaborateurs et des tiers avec lesquels il interagit le canal face à face, qui permet la transmission de communications verbales lors d'une réunion en personne ou d'une visioconférence. Dans ce cas, et compte tenu de la complexité pour le Groupe de garantir l'anonymat de l'informateur lorsque celui-ci est requis, le Groupe a confié cette fonction à l'expert externe BONET Consulting, chargé de recevoir et de gérer ce type de communications, ainsi que toute autre communication nécessitant l'identification des informateurs et nécessitant une gestion en face à face.
À cet égard, l'expert externe garantit la protection de l'identité de l'informateur tant lors du processus de demande de rendez-vous, lors de la soumission d'une communication en personne, qu'au lieu où le rendez-vous a lieu.

Afin de garantir la sécurité et l'intégrité des informations fournies par l'informateur, l'entretien sera enregistré conformément à la loi et avec le consentement préalable de l'informateur. Cet entretien sera documenté dans un format sécurisé, avec les mesures de sécurité et d'anonymat requises par le cadre réglementaire. À cette fin, BONET Consulting dispose et mettra en œuvre les mécanismes technologiques nécessaires pour transmettre des documents complémentaires aux informations fournies lors de l'entretien.

Afin de permettre l'utilisation de ce canal, le Groupe a mis en place un numéro de téléphone et une adresse courriel pour les demandes de communication sous ce format. BONET Consulting sera exclusivement chargé de la gestion et de la coordination de la réunion. Les coordonnées pour cette demande sont dûment publiées sur le site web du Groupe.