

Objet :

SIPCAM INAGRA, S.A., « SIPCAM » la « Société » ou l'« Organisation » dans le cadre de la mise en place d'un système de gestion des risques pénaux, a adopté un règlement relatif au dispositif d'alerte dont l'objectif était de permettre aux membres de l'Organisation¹ de signaler tout comportement contraire au Code d'éthique de la Société, ainsi que tout soupçon de comportement illicite ou susceptible de nuire à la réputation du Groupe SIPCAM.

Avec l'entrée en vigueur de la loi n° 2/2023 du 20 février relative à la protection des personnes signalant des infractions réglementaires et à la lutte contre la corruption (« loi n° 2/2023 »), afin de se conformer aux dispositions des paragraphes 2, h) et i), le règlement existant a été abrogé et le Conseil d'administration de SIPCAM a approuvé une Politique relative au système interne de signalement (la « Politique ») ainsi que la présente Procédure de gestion des informations reçues dans le cadre du système interne de signalement (la « Procédure »).

La présente procédure régit la réception, le traitement, l'examen et le règlement des signalements reçus par le système interne d'information (ci-après dénommé « le Système ») concernant des comportements des membres de l'Organisation qui seraient contraires au règlement interne de l'Organisation ou à la législation en vigueur, lorsque ces comportements constituent une infraction administrative grave, très grave, sont soupçonnées de constituer une infraction pénale, ou lorsque celles-ci pourraient constituer des infractions au droit de l'Union européenne portant atteinte à ses intérêts financiers ou ayant une incidence sur le marché intérieur.

Le système sera facilement accessible via le site web de l'entreprise (<https://sipcam.com/dz/fr/>). La présente procédure garantit la protection des lanceurs d'alerte, la possibilité de transmettre des informations de manière anonyme, l'indépendance et l'autonomie du responsable du système, l'absence de conflits d'intérêts dans la gestion et la conduite des enquêtes internes, les droits de la défense et la présomption d'innocence, ainsi que la rapidité du traitement des dossiers.

Champ d'application et portée :

1. Personnes concernées :

La présente procédure s'applique aux membres de l'Organisation, notamment, à titre indicatif mais non limitatif, aux membres du Conseil d'administration, aux dirigeants, aux personnes susceptibles d'entretenir une relation professionnelle commerciale avec l'Organisation, aux salariés, aux stagiaires et aux autres parties prenantes.

¹ Membres de l'organisation : les membres de l'organe de direction, les cadres, les employés, les travailleurs, les salariés temporaires ou sous contrat de collaboration, ainsi que les bénévoles d'une organisation, et toutes les autres personnes placées sous l'autorité hiérarchique de l'une des catégories susmentionnées.

2. Champ d'application matériel:

Le système doit être considéré comme un outil d'information permettant de signaler des soupçons d'irrégularités et de manquements énumérés ci-dessous :

- Soupçons d'actes, de comportements, de faits ou d'omissions contraires à la législation en vigueur, lorsqu'ils constituent une infraction administrative grave ou très grave.
- Soupçons d'actes, de comportements, de faits ou d'omissions susceptibles de constituer une infraction pénale.
- Soupçons d'actes, de comportements, de faits ou d'omissions susceptibles de constituer des infractions au droit de l'Union européenne en ce qui concerne ses intérêts financiers ou ayant une incidence sur le marché intérieur.
- Soupçons d'actes, de comportements, de faits ou d'omissions susceptibles de constituer une violation de la réglementation interne de l'Organisation.

3. Obligation de signalement :

Les membres de l'Organisation qui auraient des soupçons fondés concernant tout type d'acte, de fait, de comportement ou d'omission susceptible d'être contraire aux dispositions du paragraphe 2 des présentes doivent en informer le responsable du système interne de signalement par le biais du système mis à disposition sur le site web de SIPCAM.

CONTRÔLE DES MODIFICATIONS:			
N° Révision	Pages concernées	Modifications effectuées	Date d'approbation
01	Toutes	Création de la procédure	29/05/2023

Réalisé par :	Révisé par :	Approuvé par :
Andersen&Tax	Compliance Officer/Jose Barreiro	Conseil d'Administration
		Document approuvé lors de la réunion du Conseil d'administration du 29 mai 2023

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

ÍNDICE

1.	RESPONSABLE DEL SISTEMA DE INFORMACION	4
2.	DERECHOS DE LAS PERSONAS QUE INFORMEN	4
3.	DERECHOS DE LAS PERSONAS AFECTADAS POR LAS COMUNICACIONES	6
4.	PROCEDIMIENTO DE INVESTIGACION DE LAS COMUNICACIONES RECIBIDAS EN EL SISTEMA DE INFORMACION	7
1.1.	Fase de investigación	8
6.1.1	Comunicación y recepción de la comunicación	8
6.1.2.	Inicio del procedimiento de investigación	10
6.1.3.	Equipo investigador	10
6.1.4.	Acciones de la investigación.....	10
1.2.	Fase de Conclusiones	11
6.2.1.	Resolución	11
6.2.2.	Informe de Conclusiones	12
5.	COMUNICACIONES DE INFORMACIONES FALSAS O DE MAL FE.....	13
6.	IMPOSICION DE MEDIDAS DISCIPLINARIAS	13
	ANEXO I: CATÁLOGO DE REPRESALIAS. ARTICULO 36.3 LEY 2/2023.....	14

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	--	---

1. RESPONSABLE DU SYSTÈME D'INFORMATION

Le Conseil d'administration de SIPCAM, en vertu des dispositions de l'article 8.6 de la loi n° 2/2023, a désigné le responsable de la conformité (*Compliance Officer*) de l'organisation comme responsable du système interne d'information. S'agissant d'un organe collégial, afin de se conformer aux dispositions de l'article 8.2, M. José Ramón Barreiro a été désigné en tant que responsable du système interne d'information ; il sera enregistré en tant que représentant de SIPCAM auprès de l'Autorité indépendante de protection des lanceurs d'alerte (« A.A.I. »). Compte tenu de ce qui précède, le responsable du système interne d'alerte (le « Responsable ») de SIPCAM est composé des personnes physiques suivantes : D. José Ramón Barreiro Fernández. Responsable du système d'information interne de SIPCAM.

2. DROIT DES PERSONNES QUI SIGNALENT DES FAITS

Les droits dont bénéficie le Lanceur d'Alerte dès la réception d'une communication dans le Système de SIPCAM sont les suivants

1. **Droit à la protection.** L'Organisation assurera la protection de toute personne signalant des faits relevant du paragraphe 2 du présent document, intitulé « Champ d'application », afin d'éviter d'éventuelles représailles à son encontre. Dans le cas où le lanceur d'alerte rendrait public le contenu de l'information, en recourant à ce que l'on appelle la « divulgation publique », prévue à l'article 27 de la loi n° 2/2023, il ne pourra bénéficier des mesures de protection que lorsque :
 - a. Avoir d'abord signalé le fait via le Système SIPCAM.
 - b. S'il existe un risque manifeste pour l'intérêt public. On entend par là une situation d'urgence ou un risque de dommages irréversibles, y compris des atteintes à l'intégrité physique.
 - c. Si une communication a été effectuée par le biais d'un canal d'information externe et qu'il existe un risque de représailles ou que le traitement efficace de cette communication est peu probable compte tenu des circonstances particulières de l'affaire, par exemple en cas de dissimulation ou de destruction de preuves, de collusion avec une autorité ou avec l'auteur de l'infraction, ou si ce dernier est impliqué dans celle-ci.
2. **Protection contre d'éventuelles représailles.** En aucun cas, SIPCAM n'exercera de représailles à l'encontre du lanceur d'alerte, même si l'enquête venait à démontrer qu'il n'y a pas eu de violation de la loi, à condition qu'il n'ait pas agi de mauvaise foi. L'auteur des représailles sera sanctionné. (L'annexe I de la présente procédure répertorie les sanctions considérées comme des représailles).
3. **Droit à l'information.** Une fois la plainte examinée, le plaignant sera informé par écrit de sa

recevabilité ou non. À l'issue de l'enquête, si la plainte a été jugée recevable, le plaignant sera informé des mesures de suivi prévues ainsi que du résultat de l'enquête.

4. **Droit de choisir.** Le Lanceur d'Alerte pourra choisir le moyen qu'il juge le plus approprié pour transmettre les informations, et pourra recourir à des canaux externes.
5. **Concernant les informations demandées.** Il pourra être demandé au déclarant de fournir toutes les informations jugées nécessaires au bon traitement de la déclaration ; le responsable du système ne pourra conserver ces informations pendant une durée supérieure à dix (10) ans, conformément aux dispositions de l'article 26.2 de la loi n° 2/2023. Les informations fournies ne pourront être utilisées à des fins autres que l'enquête, cette disposition ne s'appliquant toutefois pas dans le cas où des signalements relatifs aux mêmes faits seraient reçus. Si les données sont transmises à un tiers afin qu'il mène une enquête sur un signalement, qu'il s'agisse d'une enquête interne ou externe, le lanceur d'alerte devra en être informé, son consentement n'étant toutefois pas nécessaire lorsque la transmission des données est autorisée par la législation en vigueur. Les données à caractère personnel traitées à la suite du dépôt d'un signalement via le système SIPCAM seront traitées conformément aux dispositions du Règlement général sur la protection des données à caractère personnel (Règlement (UE) 2016/679) et de la loi organique n° 3/2018 du 5 décembre relative à la protection des données et à la garantie des droits numériques, ainsi qu'à l'ensemble de la réglementation connexe en vigueur.
6. **Droit à l'anonymat.**
7. **Derecho à la confidentialité.** L'identité du lanceur d'alerte restera confidentielle et ne pourra être divulguée, sans son consentement exprès, à aucune personne autre que celles chargées du traitement des informations et de la conduite des enquêtes internes. Les exceptions sont celles prévues par le droit de l'Union européenne et la réglementation espagnole dans le cadre des enquêtes pouvant être menées par les autorités ou au cours de procédures judiciaires. SIPCAM garantit la confidentialité de la communication lorsqu'elle est transmise par d'autres moyens que le Système, ainsi que lorsqu'elle est transmise par l'intermédiaire de membres de l'Organisation non désignés comme responsables du Système, auquel cas ces derniers seront avertis que la violation de la confidentialité peut être qualifiée d'infraction très grave. De même, tous les membres de l'Organisation, grâce à une formation, sauront que dans ces cas, ils devront la transmettre immédiatement au responsable du système de l'Organisation.
8. **Droit de recevoir une réponse.** Le Lanceur d'Alerte recevra un accusé de réception des informations transmises dans un délai de **sept (7) jours calendaires** à compter de leur réception para le Responsable du Système Interne d'Information.

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

compromettre la confidentialité d'une communication. En ce qui concerne le **délai de réalisation de l'enquête**, celui-ci ne pourra excéder **trois (3) mois** à compter de la réception de la communication ou, dans le cas où aucun accusé de réception n'aurait été envoyé au lanceur d'alerte, **trois (3) mois** à compter de l'**expiration du délai de sept (7) jours** suivant la communication, sauf dans les cas présentant une **complexité particulière**, pour lesquels le délai pourra être prolongé de **trois (3) mois supplémentaires**.

9. **Droit à l'effacement des données.** Les données à caractère personnel relatives aux informations reçues et aux enquêtes internes ne seront conservées que pendant la durée nécessaire et proportionnée. Concrètement, conformément aux dispositions de l'article 32, paragraphes 3 et 4, ces durées seront les suivantes :

- a. Les données faisant l'objet du traitement ne peuvent être conservées dans le Système que pendant la durée strictement nécessaire pour décider s'il y a lieu d'ouvrir une enquête.
- b. S'il est établi que les informations fournies, ou une partie de celles-ci, ne sont pas véridiques, elles doivent être immédiatement supprimées, sauf si ce manque de véracité est susceptible de constituer une infraction pénale, auquel cas les informations seront conservées pendant la **durée** nécessaire au **déroulement de la procédure judiciaire**.
- c. À l'expiration d'un délai de **trois (3) mois** à compter de la réception de la notification, si aucune procédure d'enquête n'a été engagée, les données doivent être supprimées, sauf si l'objectif est de conserver des preuves du fonctionnement du système. Dans ce cas, elles peuvent être conservées sous forme anonymisée.
- d. En aucun cas, les données ne pourront être conservées pendant une durée supérieure à **dix (10) ans**.

3. DROITS DES PERSONNES CONCERNÉES PAR LES COMMUNICATIONS

Les droits dont bénéficie la personne concernée dès la réception d'une notification dans le Système SIPCAM sont les suivants :

1. **Droit à la protection pendant la durée de l'enquête.** SIPCAM garantira pleinement les droits de la personne concernée ; aucune mesure disciplinaire ou judiciaire ne sera appliquée tant que la véracité des faits signalés n'aura pas été vérifiée, que des preuves n'auront pas été recueillies et qu'il n'aura pas été conclu qu'il y a eu infraction administrative grave ou très grave, infraction pénale, une violation des règles internes de l'Organisation ou un comportement contraire aux intérêts financiers de l'Union européenne ou au marché intérieur.
2. **Droit à l'information.** La personne concernée a le droit d'être informée des actes, comportements, faits ou omissions qui lui sont imputés, ainsi que d'être entendue à tout moment. Cette communication sera effectuée dans les délais et selon les modalités jugées appropriées par le responsable du Système afin de garantir le bon déroulement de l'enquête. La communication des informations pourra être reportée afin d'éviter la destruction ou l'altération des preuves.
3. **Droit à la confidentialité.** La confidentialité des données à caractère personnel de la personne concernée doit être garantie afin d'éviter que leur divulgation ne porte atteinte à son honneur. Lorsque les actes, faits, omissions, comportements ou soupçons sont communiqués à la personne concernée, cette communication s'effectue sans révéler l'identité du lanceur d'alerte, sauf si le consentement exprès de ce dernier a été obtenu à cette fin.
4. **Droit à une enquête objective et transparente.** La personne concernée a droit à une enquête objective, transparente et efficace

4. PROCÉDURE D'ENQUÊTE SUR LES COMMUNICATIONS REÇUES DANS LE SYSTÈME D'INFORMATION

On distingue deux phases:

1. **Phase d'enquête :** elle comprend la réception et l'évaluation initiale de la plainte, ainsi que sa recevabilité ou son irrecevabilité. Elle englobe l'enquête sur les faits signalés, ainsi que la collecte des éléments de preuve.
2. **Phase de conclusions :** elle comprend l'analyse des éléments de preuve et des pièces justificatives fournies, ainsi que la rédaction du rapport de conclusions par le responsable du système. Ce rapport indiquera s'il y a lieu que le conseil d'administration applique des mesures disciplinaires.

4.1. Phase d'enquête

4.1.1. Dépôt et réception d'un signalement

Pour déposer un signalement dans le Système, le signalant doit y accéder via le site web de SIPCAM. S'il y a plusieurs signalants, chacun d'entre eux doit déposer un signalement. Les signalements doivent toujours être individuels. Dans le cas où des signalements portant sur les mêmes faits seraient reçus via le Système, ceux-ci pourront être regroupés afin de mener une seule et même procédure d'enquête.

Avant d'accéder au Système, le Signalant doit accepter la Politique du Système Interne d'information de SIPCAM, ainsi que la Politique en matière de protection des données. Une fois ces deux politiques acceptées, les champs suivants s'ouvrent afin d'être correctement remplis :

- Dans le cas où la **signalisation ne serait pas anonyme** :
 - Choix du type de signalement :
 - Harcèlement au travail ou harcèlement sexuel.
 - Non-respect de la loi.
 - Soupçon d'infraction pénale.
 - Non-respect du règlement interne.
 - Identité du Lanceur d'Alerte.
 - E-mail.
 - Description des faits.
 - Possibilité de joindre des documents : Word, pdf, images ou vidéos.
- Possibilité de signaler un conflit d'intérêts avec le Responsable du Système.
- Dans le cas où la **signalisation** serait **anonyme** :
 - Choix du type de signalement :
 - Harcèlement au travail ou harcèlement sexuel :
 - Non-respect de la loi.
 - Soupçon d'infraction pénale.
 - Non-respect de la réglementation interne.
 - Option d'anonymat.
 - Attribution d'un code pour un suivi adéquat.

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

- Possibilité de joindre des documents : Word, pdf, images ou vidéos.
- Enregistreur vocal avec effet de distorsion.
- Possibilité de signaler un conflit d'intérêts avec l'un des membres de l'organe collégial Chargé du Système.

Il est important que le Lanceur d'Alerte fournisse des détails sur les actes, comportements, faits ou omissions signalées, afin que le Responsable du Système puisse procéder à une analyse préliminaire adéquate du signalement.

À la demande du Lanceur d'alerte, la signalisation pourra également être effectuée lors d'un entretien en présentiel dans un délai maximal de **sept (7) jours**. Dans ce cas, le lanceur d'alerte sera informé de la nécessité de consigner le contenu de cet entretien. Tout comme pour les entretiens menés avec la personne concernée et d'autres témoins, lors de cet entretien, le lanceur d'alerte pourra choisir entre :

- L'enregistrement de la conversation dans un format sécurisé, durable et accessible.
- Transcription complète et fidèle de la conversation.
- À l'issue de la réunion, le procès-verbal sera remis à l'informateur afin qu'il puisse vérifier, rectifier et valider, par l'intermédiaire de son organisation, la transcription en question.

Après avoir examiné les pièces jointes à la déclaration, le Responsable du Système pourra :

- **Accepter de donner suite à la déclaration** : si les actes, comportements, faits ou omissions signalés sont présumés contraires à la réglementation interne de l'Organisation ou à la législation en vigueur, s'ils sont susceptibles de constituer une infraction administrative grave ou très grave, s'ils font l'objet d'un soupçon d'infraction pénale ou s'ils sont contraires aux intérêts financiers de l'Union européenne ou au marché intérieur.
- **Rejeter la plainte**:
 - Lorsque les actes, comportements ou faits sont **dépourvus de toute crédibilité**.
 - Lorsque les actes, comportements ou faits signalés **ne sont pas contraires** au règlement interne de l'Organisation ou à la législation en vigueur, pourraient constituer une infraction administrative grave ou très grave, un soupçon d'infraction pénale, une violation du règlement interne de SIPCAM ou ne seraient pas contraires aux intérêts financiers de l'Union européenne ou du marché intérieur.
 - Lorsque les actes, comportements ou faits signalés **sont manifestement sans fondement ou qu'il existe des indices laissant supposer que les informations ont été obtenues par la commission d'une infraction pénale**, auquel cas, outre le rejet de

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

la plainte, celle-ci sera transmise au ministère public.

- Lorsque les actes, comportements ou faits **ne contiennent pas d'informations nouvelles et significatives concernant des infractions par rapport à une communication antérieure** au sujet de laquelle une procédure d'enquête a déjà été menée et clôturée.

4.1.2. Ouverture de la procédure d'enquête

Une fois la déclaration acceptée, le responsable du système procède à la création d'un dossier relatif à la déclaration faisant l'objet d'une enquête. Ce dossier est géré via l'outil informatique prévu à cet effet, qui garantit qu'aucun membre de l'organisation ne puisse accéder aux données qu'il contient, celles-ci étant hébergées sur un serveur externe à SIPCAM.

L'outil utilisé par SIPCAM ne permet pas non plus de modifier les enregistrements qu'il contient et dispose d'un registre privé de toutes les communications reçues et des enquêtes internes.

4.1.3. Équipe d'enquête

L'équipe d'enquête est composée du Responsable du Système, qui est également le Responsable de la Conformité (Compliance Officer) de SIPCAM ; celui-ci peut faire appel à des tiers externes pour mener l'enquête et recueillir des éléments de preuve. Lorsqu'il le jugera nécessaire, le Responsable de la Conformité pourra solliciter la collaboration d'autres membres de SIPCAM pour mener l'enquête, toujours dans le respect des garanties de confidentialité requises et conformément aux principes de conduite applicables au Responsable du Système et au Responsable de la Conformité.

Le Responsable du Système pourra s'adresser à d'autres services de l'organisation pour demander et exiger des preuves et des éléments de preuve, et pourra également solliciter la collaboration de tiers externes pour le bon déroulement de l'enquête, en appliquant les garanties et les principes mentionnés au paragraphe précédent.

L'outil informatique permet d'identifier d'éventuels conflits d'intérêts chez le lanceur d'alerte avant même qu'il ne transmette une communication ; dans ce cas, l'outil lui-même empêchera le membre du Responsable du Système d'accéder à la procédure d'enquête dans laquelle il se trouve en situation de conflit. Si, une fois la communication reçue, un conflit d'intérêts est identifié, le membre du Responsable du Système présentant ledit conflit sera exclu de l'enquête.

4.1.4. Mesures prises dans le cadre de l'enquête

Le Responsable du Système prendra toutes les mesures qu'il jugera opportunes afin d'approfondir l'examen des actes, comportements et faits signalés, dans le but de recueillir des informations supplémentaires permettant de prendre une décision appropriée, de manière objective, sur la base des éléments de preuve recueillis

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

À titre indicatif, mais sans s'y limiter, les mesures d'enquête peuvent être les suivantes :

- Demander de nouveaux éléments de preuve et/ou des justificatifs à l'informateur afin d'améliorer le processus d'enquête.
- D'un commun accord avec l'informateur, il sera possible de convenir des mesures conservatoires nécessaires, notamment en matière de changement de poste et de télétravail.
 - Organiser des entretiens avec l'informateur, les témoins, d'autres professionnels et la personne concernée. Ces entretiens permettront d'obtenir les éléments de preuve suivants :
 - Enregistrement de l'entretien ou compte-rendu intégral de l'entretien mené.
 - Engagement de Confidentialité concernant les faits dont ils ont eu connaissance, qui devra être pris par l'Organisation, le Lanceur d'Alerte, les témoins, les autres professionnels et la personne concernée.
- Examen de toutes les informations relatives à la relation professionnelle des personnes concernées avec l'Organisation, dans le respects des dispositions de la législation en matière de protection des données et de la vie privée des personnes concernées.
- Collaboration avec des tiers externes.
- Analyse judiciaire réalisée para un expert externe indépendant.
- Autres mesures jugées nécessaires pour poursuivre le processus d'enquête dans le respect de la réglementation en vigueur en matière de protection des données.

L'enquête consistera, à tout moment, en une analyse objective de la documentation disponible, en la recherche d'indices, en la collecte de preuves et en l'analyse de celles-ci.

La procédure d'enquête durera au **maximum trois (3) mois** à compter du jour où le Responsable du Système aura reçu la notification ou, à défaut d'accusé de réception envoyé au Lanceur d'Alerte, **trois (3) mois** à compter de l'expiration du délai de **sept (7) jours** suivant la notification, **sauf dans les cas présentant une complexité particulière, pour lesquels ce délai pourra être prolongé de trois (3) mois** supplémentaires.

4.2. Phase de conclusions

4.2.1. Décision

Une fois les éléments de preuve recueillis et analysés par le Responsable du Système, la phase d'enquête sera clôturée et la phase de conclusions débutera, au cours de laquelle des décisions seront prises concernant la communication faisant l'objet de l'enquête, et les mesures qu'il est recommandé d'adopter seront proposées au Conseil d'Administration.

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

Le Conseil d'Administration pourra prendre les mesures suivantes :

- **Signalement non fondé** : dans le cas où l'enquête sur les actes, comportements et faits signalés révèle l'absence de manquement. Le responsable du système informera le lanceur d'alerte et la personne concernée de cette décision, en précisant les motifs qui la justifient.
- **Communication fondée** : S'il est prouvé que les actes, comportements ou faits signalés sont avérés, il convient de détailler les éléments qui étayent cette conclusion. Le régime de sanctions s'appliquera conformément à la convention collective applicable, à la législation du travail, ainsi qu'aux obligations civiles ou commerciales contractées envers le membre de l'Organisation

4.2.2. **Rapport de Conclusions**

Le Responsable du Système rédigera un rapport de conclusions rendant compte des résultats de l'ensemble de la phase d'enquête. Ce rapport de conclusions comprendra :

- Aspects techniques : numéro de dossier, enquêteurs, date de réception de la signalisation, objet, niveau de confidentialité (qui y a accès), code d'identification et date de clôture de l'enquête.
- Contexte du dossier : actes, comportements ou faits à l'origine de la signalisation, ainsi que les personnes ou services faisant l'objet de l'enquête.
- Objet de l'enquête et son objectif.
- Actions menées, faits pertinents examinés et constatés, éléments de preuve et indices analysés.
- Conclusions établies, sur la base de l'objectif et de la portée de l'enquête.
- Propositions de mesures disciplinaires que devra adopter le Conseil d'administration, conformément à la convention collective applicable, à la législation du travail et à l'ensemble des autres obligations civiles et commerciales contractées par le membre de l'organisation concerné, sans préjudice des responsabilités pénales pouvant découler de la commission d'infractions.

Le Responsable du Système consignera ces conclusions de manière claire et concise. En outre, si des contraintes ont été rencontrées au cours de l'enquête, celles-ci devront être mentionnées dans le rapport.

Les rapports ainsi établis seront communiqués au Conseil d'Administration dans le cadre du rapport annuel d'activité.

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

5. COMMUNICATIONS DE FAUSSES INFORMATIONS OU DE MAUVAISE FOI

Le système d'information de SIPCAM doit être utilisé de manière responsable et appropriée. Le signalement d'actes, de comportements ou de faits mensongers, dans une intention malveillante et moralement malhonnête, constitue une atteinte à la bonne foi qui doit présider aux relations de travail au sein de l'Organisation et peut donner lieu à des mesures disciplinaires conformément à la convention collective en vigueur.

Si, après analyse, il s'avérait que les faits dénoncés sont manifestement faux et que la plainte a été déposée avec malveillance et de mauvaise foi :

- La plainte sera classée sans suite, en précisant les motifs ayant conduit à ce classement, ce qui mettra fin à l'enquête.
- Cette situation sera transmise au Service des Ressources Humaines (RH) de la Société afin que, en coordination avec le Responsable du Système, des mesures disciplinaires soient proposées conformément à la Convention Collective en vigueur.
- La proposition de sanction sera communiquée par écrit au Conseil d'Administration, qui décidera de la mesure disciplinaire à appliquer à l'auteur d'un signalement de mauvaise foi.

6. APPLICATION DE MESURES DISCIPLINAIRES

Si, à l'issue de l'enquête, il s'avérait que les actes, faits ou comportements signalés sont avérés et liés à des comportements irréguliers, illicites, constitutifs d'infractions administratives graves ou très graves, contraires à la législation en vigueur, au règlement interne de l'Organisation, aux intérêts financiers de l'Union européenne ou au marché intérieur, la personne concernée pourra faire l'objet d'une sanction conformément aux dispositions de la Convention Collective applicable, à la législation du travail, ainsi qu'aux autres obligations civiles et commerciales contractées par le membre de l'Organisation.

Si les résultats de l'enquête révèlent des indices laissant supposer qu'une infraction pénale a été commise, les faits devront être portés à la connaissance du ministère public. S'il s'agit d'un autre type d'infraction, SIPCAM pourra porter les faits à la connaissance des autorités judiciaires si elle le juge nécessaire.

	PROCÉDURE DE GESTION DES INFORMATIONS REÇUES DANS LE SYSTÈME D'INFORMATION INTERNE	PRCOM-GSE 003 Rev 01 Systèmes de gestion
---	---	---

ANNEXE I: LISTE DES MESURES DE REPRÉSAILLES. ARTICLE 36.3 DE LA LOI N° 2/2023

- a) Suspension du contrat de travail, licenciement ou cessation de la relation de travail ou statutaire, y compris le non-renouvellement ou la résiliation anticipée d'un contrat de travail à durée déterminée une fois la période d'essai terminée, ou la résiliation anticipée ou l'annulation de contrats de biens ou de services, l'imposition de toute mesure disciplinaire, la rétrogradation ou le refus de promotion, ainsi que toute autre modification substantielle des conditions de travail et la non-conversion d'un contrat de travail à durée déterminée en contrat à durée indéterminée, dans le cas où le salarié aurait eu des attentes légitimes quant à l'obtention d'un emploi à durée indéterminée ; à moins que ces mesures ne soient prises dans le cadre de l'exercice régulier du pouvoir de direction, conformément à la législation du travail ou à la réglementation régissant le statut des fonctionnaires, en raison de circonstances, de faits ou d'infractions avérés, et sans rapport avec la présentation de la notification..
- b) Préjudices, y compris ceux portant atteinte à la réputation, ou pertes économiques, contraintes, intimidations, harcèlement ou ostracisme.
- c) Évaluation ou références négatives concernant les performances professionnelles.
- d) Inscription sur des listes noires ou diffusion d'informations dans un secteur donné, rendant difficile ou impossible l'accès à l'emploi ou l'attribution de marchés de travaux ou de services.
- e) Refus ou annulation d'une licence ou d'un permis.
- f) Refus d'accès à la formation.
- g) Discrimination, ou traitement défavorable ou injuste.