# ALLGEMEINE RICHTLINIEN DES INTERNEN SYSTEMS VON INFORMATIONEN UND VERTEIDIGUNG DER INFORMANT

# INDEX

# 1 - EINLEITUNG

Die Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 in spanisches Recht mit dem Gesetz 2/2023 vom 20. Februar zur Regelung des Schutzes von Personen, die Verstöße melden
Vorschriften und der Kampf gegen Korruption erfordern die Einführung spezifischer Instrumente, damit diejenigen, die Kenntnis von illegalen oder unregelmäßigen Handlungen haben, nützliche Daten und Informationen liefern können, wodurch ein umfassender und wirksamer Schutz der Informanten gewährleistet wird.

Die genannten Regelungen regeln dabei die Mindestanforderungen an die verschiedenen internen und externen Informationskanäle sowie den besonderen Schutz von Informanten, die nach bestem Wissen und Gewissen und uneigennützig handeln.

In Übereinstimmung mit dem Vorstehenden hat die Gruppe ein internes System implementiert,
Das Informationssystem (SIIF) ist eine grundlegende Achse für Überwachung, Kontrolle und Prävention im Bereich der Einhaltung gesetzlicher Vorschriften. Dieses System ist ein bevorzugter Kanal und ein obligatorisches Instrument für die sorgfältige Kanalisierung von Informationen, um die Informationskultur innerhalb der Organisation zu stärken.

Das SIIF wurde als Kontroll- und Präventionsinstrument konzipiert und umfasst Informationskanäle, die sowohl intern als auch von einem spezialisierten externen Unternehmen verwaltet werden. Diese Kanäle zeichnen sich durch höchste Professionalität, Erfahrung, Unabhängigkeit, Vertraulichkeit und die Einhaltung der Datenschutzbestimmungen und anderer geltender regulatorischer Rahmenbedingungen aus. Darüber hinaus garantiert das SIIF die Grundprinzipien der Anonymität, der ordnungsgemäßen Aufzeichnung, Aufbewahrung und Nichtveränderung, der Vermeidung von Interessenkonflikten, des Schutzes von Hinweisgebern und des Verbots von Vergeltungsmaßnahmen.

Gemäß dem oben genannten Gesetz ist es eine wesentliche Voraussetzung, dass der SIIF über eine
Eine Richtlinie, die die allgemeinen Grundsätze des Systems und den Schutz von Informanten darlegt und innerhalb der Gruppe ordnungsgemäß bekannt gemacht wird. Zusammen mit dem Verfahren zur Verwaltung der erhaltenen Informationen ist diese Richtlinie daher ein wesentlicher Bestandteil der Konfiguration und des Betriebs des SIIF.

# 2 - HANDLUNGSGRUNDSÄTZE UND WESENTLICHE GARANTIEN

Das Interne Informationssystem (SIIF) ist eine der Hauptachsen des Systems Einhaltung gesetzlicher Vorschriften und Kriminalprävention. Unter Einhaltung höchster Sorgfaltsstandards in diesem Bereich hat die Gruppe dem SIIF in Zusammenarbeit mit dem externen Experten BONET Consulting eine Reihe von Sicherheitsvorkehrungen zur Gewährleistung seiner Wirksamkeit gegeben. Im Einzelnen lauten die Grundprinzipien und grundlegenden Sicherheitsvorkehrungen, die die Prozesse und Maßnahmen der Gruppe in Bezug auf den SIIF regeln, wie folgt:

- **Unabhängigkeit, Autonomie, Unparteilichkeit und Abwesenheit von Interessenkonflikten**: Für den Empfang und die Bearbeitung von Hinweisen auf Verstöße wurden Reaktionsmechanismen definiert, um potenzielle Interessenkonflikte und/oder mangelnde Unabhängigkeit zu bewältigen und zu kontrollieren, wenn die für Management, Kontrolle und/oder Aufsicht Verantwortlichen bestimmte Merkmale aufweisen, die die Erfüllung ihrer Aufgaben beeinträchtigen und einschränken. Darüber hinaus werden alle eingehenden Mitteilungen gemäß den erforderlichen Unabhängigkeitsanforderungen analysiert, um eine faire und gerechte Bearbeitung zu gewährleisten.

- **Professionalität und Erfahrung**: Fachleute mit Fachkenntnissen in der Einhaltung gesetzlicher Vorschriften, der Kriminalprävention und der verantwortungsvollen Unternehmensführung sind für die ordnungsgemäße Handhabung und Verwaltung der Kommunikation verantwortlich und wahren dabei die Rechte sowohl der Informanten als auch der Beschuldigten.

- **Vollständigkeit, Integrität und Vertraulichkeit der Informationen**Die Teilnehmer an den verschiedenen Phasen der Untersuchung sind zur Vertraulichkeit aller Informationen verpflichtet, auf die sie im Rahmen ihrer Aufgaben Zugriff haben oder von denen sie Kenntnis erhalten. Darüber hinaus wird der unbefugte Zugriff auf die Informationen verhindert, und durch die Erstellung von Sicherungskopien und separaten Dateien ist eine langfristige und sichere Speicherung der Informationen gewährleistet.

- **Datenschutz und Vertraulichkeit der Kommunikation**: Die Datenverarbeitung erfolgt unter Einhaltung höchster Datenschutzmaßnahmen und -richtlinien gemäß den geltenden Datenschutzbestimmungen. Ebenso besteht eine Vertraulichkeitspflicht hinsichtlich aller Aspekte der übermittelten Informationen.

- **Anonymität**: Es besteht die Möglichkeit, anonyme Mitteilungen einzureichen und später zu verarbeiten, sowie die allgemeine Pflicht, die Identität des Hinweisgebers, der sich bei der Mitteilung identifiziert hat, zu wahren, ihn anonym zu halten und seine Identität nicht an Dritte weiterzugeben.

- **Günstiger Einsatz, einfach und kostenlos:**Eine einfache Kommunikation ist gewährleistet, da ein universeller Zugriff auf das System ohne zusätzliche Kosten möglich ist und die rechtlichen und ethischen

Grundsätze, die die Aktivitäten der Gruppe bestimmen, wirksam angewendet werden.

- **Angemessene und unabhängige Registrierung**Über die erhaltenen Informationen und die daraus resultierenden internen Untersuchungen wird ein privates Logbuch geführt, um deren unabhängige und nicht-interessierte Verarbeitung, Verwaltung und Nichtveränderung für einen gemäß der geltenden Gesetzgebung erforderlichen und angemessenen Zeitraum zu gewährleisten. Die Daten werden unter keinen Umständen länger als zehn Jahre gespeichert.

- **Bewährte Verfahren für Überwachung und Untersuchung**Um die Richtigkeit der Kommunikation zu überprüfen, die ordnungsgemäße Beweiserhebung sicherzustellen und die Rechte der Betroffenen zu wahren, wird der Kommunikationszyklus durch ein wirksames und transparentes internes Verfahren geregelt. Diese Vorgehensweisen werden im Verfahren zur Verwaltung erhaltener Informationen dokumentiert.

- Schutz von Hinweisgebern und Betroffenen: Personen, die Verstöße melden oder offenlegen, haben Anspruch auf Schutzmaßnahmen und müssen für ihre Mitarbeit weder mit Vergeltungsmaßnahmen noch mit negativen Konsequenzen rechnen, einschließlich Androhung oder versuchter Vergeltungsmaßnahmen. Ebenso genießen die von der Meldung Betroffenen den gleichen Schutz wie Hinweisgeber. Ihre Identität wird geschützt und die Vertraulichkeit der Fakten und Informationen rund um das Verfahren ist gewährleistet.

- **Sorgfältiges Handeln, Verantwortung und guter Glaube des Informanten**Die Nutzung des Systems basiert auf den Grundsätzen von Verantwortung, Sorgfalt und Treu und Glauben. Jeder Hinweisgeber muss daher zum Zeitpunkt der Meldung hinreichend Anlass zu der Annahme haben, dass die Informationen wahr sind. Die Meldung unbegründeter, falscher oder verzerrter Tatsachen sowie die Übermittlung illegal, böswillig oder moralisch unredlich erlangter Informationen stellt einen Verstoß gegen den Grundsatz von Treu und Glauben dar und kann disziplinarische Maßnahmen nach sich ziehen.

# 3 - VERANTWORTLICH FÜR DAS INTERNE INFORMATIONSSYSTEM

Für die Effektivität des internen Informationssystems (SIIF) ist es unerlässlich, eine Person zu benennen, die für dessen ordnungsgemäße Funktion, Organisation und sorgfältige Informationsverarbeitung verantwortlich ist. Diese Person ist außerdem für die ordnungsgemäße Kommunikation und Verbreitung des SIIF sowie für die Entwicklung und Aktualisierung des entsprechenden Schulungsplans verantwortlich.

Das Verwaltungs- oder Leitungsorgan der Gruppe ist für die Ernennung und Benachrichtigung der zuständigen Behörde der für die Verwaltung des besagten Systems verantwortlichen Einzelperson oder Kollegialorgans (nachfolgend „Systemmanager“) sowie für deren Entlassung oder Kündigung verantwortlich.

Der Systemmanager führt seine Aufgaben unabhängig und autonom von den anderen Organisationsgremien der Gruppe aus und vermeidet potenzielle Interessenkonflikte bei der normalen Erfüllung seiner Aufgaben.

Der Systemmanager kann sich jedoch zur Gewährleistung der ordnungsgemäßen Erfüllung seiner Aufgaben auf die Hilfe anderer Dritter verlassen, um fachliche Unterstützung zu erhalten und/oder die Unabhängigkeitsanforderungen zu erfüllen.

Um seine/ihre Aufgaben zu erfüllen, koordiniert der/die Systemmanager/in insbesondere die folgenden Themen:

A- Der Personalleiter entscheidet, wann Disziplinarmaßnahmen gegen die betroffenen Personen angebracht sein können und/oder koordiniert die Umsetzung von Schutzmaßnahmen.

B- Die für die Einhaltung gesetzlicher Vorschriften Verantwortlichen und/oder die Rechtsabteilung der Gruppe sollten gegebenenfalls Maßnahmen zur Einhaltung gesetzlicher oder behördlicher Vorschriften ergreifen, die von ihnen im Hinblick auf die im SIIF eingehenden Mitteilungen berücksichtigt werden müssen.

C- Die gegebenenfalls benannten Verantwortlichen für die Datenverarbeitung.

D- Der Datenschutzbeauftragte/Beauftragte.

E- Andere Personen und/oder Einrichtungen, die an der Verwaltung des SIIF beteiligt sind.

# 4 - UNABHÄNGIGE BEHÖRDE ZUM INFORMANTENSCHUTZ

Das interne Informationssystem der Gruppe (SIIF) ist das vorrangige und obligatorische Mittel zur Meldung bekannter rechtswidriger Verhaltensweisen oder Verstöße, da es die ordnungsgemäße Umsetzung von Schutzmaßnahmen gewährleistet und eine Informationskultur innerhalb der Organisation fördert.

Es wurden jedoch auch andere „externe“ Informationskanäle eingerichtet, um den Bürgern eine alternative Möglichkeit zur Übermittlung von Mitteilungen und/oder Beschwerden zu bieten, wenn die internen Kanäle die in den geltenden Vorschriften geforderten Garantien nicht erfüllen, die entsprechenden Schutzmaßnahmen nicht angewendet werden oder Einzelpersonen aufgrund ihres Status als Informanten Repressalien ausgesetzt sind.

Folglich kann jede Person Handlungen oder Unterlassungen, die einen Verstoß gegen das Gesetz darstellen, direkt der unabhängigen Whistleblower-Schutzbehörde (AIWP) über den externen Informationskanal dieser spezialisierten Behörde melden. Der Zugang zu diesem externen Informationskanal und die Kontaktdaten der Behörde sind auf ihrer Website veröffentlicht.

# 5 VERTRAULICHKEIT UND SCHUTZ PERSONENBEZOGENER DATEN

Die Verarbeitung personenbezogener Daten aus dem internen Informationssystem (SIIF) unterliegen den Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, des Organgesetzes 3/2018 vom 5. Dezember und des Organgesetzes 7/2021 vom 26. Mai. Daher werden die Interessenten zum Zeitpunkt der Einstellung gemäß den geltenden Vorschriften über die Verarbeitung ihrer Daten und ihre Rechte informiert.

Unter Beachtung des Grundsatzes der Datenminimierung werden nur die personenbezogenen Daten erhoben, die für die Abwicklung der Kommunikation erforderlich und relevant sind.
Sollten Daten versehentlich erhoben werden und für die Aufklärung und Untersuchung der Handlungen oder Unterlassungen nicht erforderlich sein, werden sie unverzüglich gelöscht. Darüber hinaus werden die Daten so lange gespeichert, wie es für die Entscheidung über die Einleitung einer Untersuchung erforderlich ist.

Darüber hinaus gewährleistet das SIIF-Konzept die Vertraulichkeit der Identität des Informanten und aller in der Mitteilung genannten Dritten sowie der im Rahmen ihrer Verwaltung und Verarbeitung durchgeführten Maßnahmen. Der Zugriff auf personenbezogene Daten und andere im System enthaltene Informationen ist dabei auf die für die Verwaltung Verantwortlichen im Rahmen ihrer Befugnisse und Funktionen beschränkt. Daher sind geeignete technische und organisatorische Maßnahmen vorhanden, um die Identität der Betroffenen zu schützen und den Zugriff Unbefugter zu verhindern.

Bei Fragen oder Unklarheiten zur Verarbeitung personenbezogener Daten innerhalb der Konzerngesellschaften im Zusammenhang mit dem SIIF kann sich jede interessierte Partei an den zuständigen Datenschutzbeauftragten/-beauftragten unter den ihm zuvor mitgeteilten und zur Verfügung stehenden Kontaktdaten wenden.

# 6 SCHUTZMASSNAHMEN

Personen, die Verstöße über das interne System melden oder offenlegen
Informationen (SIIF) der Gruppe haben Anspruch auf Schutz unter den gleichen Bedingungen
dass diejenigen, die über externe Kanäle Meldung erstatten, zum Zeitpunkt der Mitteilung oder Offenlegung hinreichende Gründe für die Annahme haben, dass die betreffenden Informationen der Wahrheit entsprechen, auch wenn sie keine schlüssigen Beweise vorlegen.

In diesem Zusammenhang sind Vergeltungsmaßnahmen, einschließlich Drohungen und Versuche, gegen Personen, die eine Mitteilung einreichen, ausdrücklich verboten. Vergeltungsmaßnahmen werden wie folgt definiert:

a- Gesetzlich verbotene Handlungen oder Unterlassungen.

b- Handlungen oder Unterlassungen, die direkt oder indirekt zu einer ungünstigen Behandlung führen und eine Person gegenüber einer anderen benachteiligen.

Als Beispiele und nicht als Einschränkung werden folgende Handlungen als Repressalien angesehen:

- Suspendierung des Arbeitsvertrags, Entlassung oder Beendigung des Arbeitsverhältnisses, vorzeitige Kündigung, Aufhebung des Arbeits- und/oder Handelsvertrags, Disziplinarmaßnahmen, Verweis oder sonstige Sanktionen, Degradierung oder Verweigerung einer Beförderung, wesentliche Änderung der Bedingungen, Nichtumwandlung eines befristeten Arbeitsvertrags in einen unbefristeten Vertrag oder gleichwertige Maßnahmen.

- Schäden (einschließlich Rufschädigung), wirtschaftliche Verluste, Nötigung, Einschüchterung, Belästigung oder Ausgrenzung.

- Negative Beurteilungen oder Referenzen bezüglich der Arbeits- oder Berufsleistung.

- Schwarze Listen oder die Verbreitung von Informationen, die den Zugang zu Beschäftigung/Arbeits- oder Dienstleistungsverträgen erschweren oder verhindern.

- Ablehnung oder Aufhebung einer Lizenz oder Genehmigung.

- Verweigerung der Ausbildung.

- Diskriminierung, benachteiligte oder unfaire Behandlung.

- Verweigerung von Anreizen, Vorteilen, Boni, Provisionen und jeglicher anderer Art von Vergütung.

- Vorzeitige Kündigung, Aussetzung, Änderung oder Stornierung von Verträgen über Waren oder Dienstleistungen.

Diese Handlungen sind nichtig und führen gegebenenfalls zu Disziplinar- oder Haftungsmaßnahmen, die auch Schadensersatz für den Geschädigten umfassen können.

Um das Recht auf Schutz des Informanten und der von der Mitteilung betroffenen Personen zu gewährleisten, hat die Gruppe die folgenden technischen und organisatorischen Maßnahmen ergriffen, die ab dem Zeitpunkt des Eingangs der Mitteilung Anwendung finden:

1- Konfiguration des SIIF: Der SIIF wurde mit geeigneten technischen und organisatorischen Maßnahmen ausgestattet, um den Schutz der Identität des meldenden Unternehmens sowie aller aus den übermittelten Mitteilungen gewonnenen Daten und Informationen zu gewährleisten. In diesem Zusammenhang hat der Konzern mehrere interne Meldekanäle eingerichtet, die eine anonyme Übermittlung von Mitteilungen ermöglichen. Diese Kanäle sind:

- Online-/Digitalkanal: Digitale Plattform zur Übermittlung schriftlicher Mitteilungen.

- Face-to-Face-Kanal: Das System zum Empfangen von Mitteilungen durch persönliche Treffen oder Videokonferenzen.

Unabhängig vom genutzten Kanal garantiert das SIIF eine effektive Anwendung der in dieser Richtlinie festgelegten Grundprinzipien und Garantien, um die Anforderungen des regulatorischen Rahmens erfüllen und die Rechte der Informanten und Betroffene.

2- SIIF-Manager: Um die ordnungsgemäße Anwendung des SIIF zu gewährleisten, hat die Gruppe einen Manager benannt, dessen Aufgabe es ist, dessen Betrieb zu beaufsichtigen, zu überwachen und zu kontrollieren. In diesem Zusammenhang ergreift der Manager gemeinsam mit dem externen Experten die erforderlichen Schutzmaßnahmen und sorgt für deren ordnungsgemäße Überwachung und Umsetzung. Die Beteiligung des externen Experten verleiht den Funktionen des Managers die nach den geltenden Vorschriften erforderliche Autonomie und Unabhängigkeit.

   Der Verantwortliche ist zudem für die Durchführung einer Voranalyse der eingegangenen Mitteilungen verantwortlich, um die Angemessenheit spezifischer Schutzmaßnahmen für den Hinweisgeber und/oder betroffene Dritte zu prüfen. Je nach Art und Umfang der Informationen wird der Verantwortliche zudem von den Leitern der verschiedenen operativen Bereiche des Konzerns unterstützt und beraten, um die Untersuchung erfolgreich abzuschließen. Er kann auch weitere Dritte hinzuziehen, die auf Sachverhalte spezialisiert sind, die eine Expertenmeinung erfordern.

3- Aufbewahrung, Verwaltung und Sicherheit von SIIF-Informationen: Die Gruppe verfügt über ein Dokumentenmanagementsystem mit entsprechenden Sicherheits- und Kontrollmaßnahmen, um die Wirksamkeit des SIIF nachzuweisen. Es ist zu beachten, dass dieses System anonyme Prozesse beinhaltet, um die Identifizierung von Informanten zu verhindern. Darüber hinaus hat die Gruppe angemessene technische Maßnahmen zur sicheren Speicherung, Abfrage und Entsorgung von Informationen sowie zur

Implementierung von Zugriffskontrollen ergriffen, um unbefugte Nutzung zu verhindern.

Von diesem Schutz ausgenommen sind jedoch Informationen, die falsch, verzerrt, offensichtlich unglaubwürdig oder unbegründet sind oder bei denen begründete Anhaltspunkte dafür vorliegen, dass sie durch die Begehung einer Straftat erlangt wurden. Denn jede Mitteilung muss in gutem Glauben erfolgen, und der Informant muss daher zum Zeitpunkt der Mitteilung begründete Annahmen über die Wahrheit der Information haben. Kurz gesagt: Der Grundsatz von Treu und Glauben verlangt, dass in keinem Fall auf Unwahrheit, falsche Angaben oder die Absicht, Rache zu nehmen oder Dritten zu schaden, geschlossen werden kann.

Es ist wichtig zu bedenken, dass sich Schutzmaßnahmen nicht nur an Informanten richten. Auch diejenigen, auf die sich die in der Mitteilung beschriebenen Tatsachen beziehen (betroffene Personen), genießen besonderen Schutz vor dem Risiko, dass die Informationen, selbst scheinbar wahrheitsgemäß, manipuliert, falsch oder anderweitig motiviert sein könnten. Während der Bearbeitung des Falles haben diese Personen Anspruch auf Unschuldsvermutung, Rechtsschutz und Verteidigung, Akteneinsicht sowie auf Vertraulichkeit der Tatsachen und Einzelheiten des Verfahrens und Schutz ihrer Identität. Kurz gesagt: Sie genießen denselben Schutz und dieselben Rechte wie der Informant.

# 7 - DISZIPLINARREGELUNG

Die Nichteinhaltung geltender Vorschriften und ein Verhalten, das den Anweisungen, Richtlinien, Kodizes, Verfahren und Protokollen der Gruppe zuwiderläuft, führt zur Anwendung disziplinarischer Maßnahmen auf Arbeits- und Handelsebene, in Abstimmung mit den Bestimmungen des geltenden Tarifvertrags, des Arbeitnehmerstatuts und anderer geltender Vorschriften.

Die Gruppe wird alle Handlungen oder Unterlassungen von Mitarbeitern, Mitarbeitern oder mit der Gruppe verbundenen Mitgliedern melden und sanktionieren, die dieser Richtlinie zuwiderlaufen, und insbesondere:

- Unterlassene Meldung jeglicher Verdachtsmomente oder Kenntnis von Verstößen oder Verletzungen des regulatorischen Rahmens und der internen Protokolle und Standards der Gruppe über das SIIF.

- Jeder Versuch oder jede wirksame Maßnahme, die Übermittlung von Mitteilungen zu behindern oder deren Weiterverfolgung zu verhindern, zu vereiteln oder zu verlangsamen.

- Die Verwendung des SIIF in böser Absicht, beispielsweise durch die Bereitstellung von Informationen oder Unterlagen, die bekanntermaßen falsch sind.

- Jegliche Vergeltungsmaßnahmen gegen Informanten oder andere betroffene Personen, die sich aus der Kommunikation ergeben.

- Die Verletzung von Vertraulichkeits- und Anonymitätsgarantien, die Offenlegung der Identität der betroffenen Personen und die Verletzung der Geheimhaltungspflicht von Informationen.

- Nichterfüllung der Verpflichtung zur Mitwirkung bei der Ermittlung von Informationen.

# 8 - KOMMUNIKATION, ÜBERPRÜFUNG UND AKTUALISIERUNG

Diese Richtlinie sowie alle notwendigen Informationen zur Nutzung des implementierten internen Informationssystems (SIIF) sind in einem separaten und leicht zugänglichen Abschnitt verfügbar, sodass sie allen Interessierten übersichtlich und leicht zugänglich sind. Jeder kann jedoch über die Kontaktdaten des Verantwortlichen zusätzliche Informationen von der Gruppe anfordern.

Der Systemmanager überprüft diese Richtlinie regelmäßig und schlägt gegebenenfalls dem Verwaltungs- oder Leitungsgremium der Gruppe Aktualisierungen vor, um sie an etwaige Umstände und Änderungen sowie an etwaige Vorschriften und Rechtsprechung anzupassen. Dies alles dient dazu, den SIIF an die höchsten regulatorischen Compliance-Anforderungen anzupassen, um seine ordnungsgemäße Funktion und Wirksamkeit zu gewährleisten.

Ebenso ist die Gruppe offen für alle Anregungen und/oder Vorschläge, die ihr ethisches Verhalten verbessern und eine Kultur der Einhaltung gesetzlicher Vorschriften fördern können. Dabei wird die Notwendigkeit betont, dass alle Mitarbeiter und Mitglieder der Gruppe oder Drittparteien im Einklang mit ihren Werten und Grundsätzen zusammenarbeiten.

# 9 - INTERNE INFORMATIONSKANÄLE

Um den Bestimmungen des Gesetzes 2/2023 zu entsprechen, hat der Konzern ein System implementiert, das die im Gesetz festgelegten technischen und verfahrenstechnischen Anforderungen für die ordnungsgemäße Abwicklung von Mitteilungen erfüllt. Ziel ist es, Informanten eine sichere, vertrauliche oder sogar anonyme Kommunikationsumgebung mit dem Konzern zu bieten und Informationen effizient, professionell und unabhängig zu verarbeiten.

Zu diesem Zweck hat sich der Konzern mit materiellen, technischen und personellen Ressourcen ausgestattet, um verschiedene interne Kanäle für die Übermittlung schriftlicher und mündlicher Mitteilungen zu ermöglichen. Diese Kanäle werden von einem externen Experten konfiguriert, konzipiert und betreut, um ein Höchstmaß an Professionalität, Erfahrung, Unabhängigkeit, Vertraulichkeit, Daten- und Hinweisgeberschutz sowie weitere für diese Kanäle relevante Aspekte zu gewährleisten.

Bitte beachten Sie, dass alle über einen unserer internen Kanäle bereitgestellten Informationen vertraulich behandelt werden und nur autorisiertem Personal zur ordnungsgemäßen Verwaltung und Verarbeitung zugänglich sind.

Die Kanäle, die jedem Mitarbeiter oder mit der Gruppe verbundenen Dritten zur Übermittlung von Mitteilungen zur Verfügung stehen, sind nachstehend aufgeführt:

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

**Canal On-line/Digital** CORPORATE LINE Canal de comunicaciones

Die Gruppe verfügt über ein digitales Tool, mit dem schriftliche Mitteilungen über ein Formular mit Dateianhängen übermittelt werden können. Nach dem Ausfüllen des Formulars generiert das Tool automatisch einen Code, der eine ordnungsgemäße Nachverfolgung und Verwaltung durch die für die Bearbeitung zuständige Person ermöglicht.

Dem Hinweisgeber wird zudem eine Bestätigung über die Erfassung und Registrierung der Mitteilung im System zugesandt. Diese Bestätigung enthält eine Zusammenfassung der gemachten Angaben sowie den Code, sodass der Hinweisgeber die Informationen auch nachvollziehen kann.
Dieses Tool verfügt über Sicherheitsmaßnahmen, die den Schutz der Informationen, die Identität des Hinweisgebers und der Betroffenen sowie die Vertraulichkeit und Vertraulichkeit des gesamten Kommunikationsmanagement- und -verarbeitungsprozesses. In diesem Zusammenhang garantiert die Gruppe eine sichere und effiziente Kommunikationsumgebung für den Empfang von Mitteilungen.

Das Tool ermöglicht auch die anonyme Übermittlung von Mitteilungen.

Dank des verfügbaren Kommunikations- und Überwachungssystems können der Informant und der Systemmanager über das Tool kommunizieren, unabhängig davon, ob die Mitteilung anonym übermittelt wurde.

Der Link zum Zugriff auf dieses Tool sowie dessen Nutzungsumfang sind auf der Website der Gruppe verfügbar.

## Canal Presencial / "Face to face"


- Telefon: 911087727 / 930460116

  Die Auskunftsdienstzeiten sind wie folgt:

  - Montag bis Donnerstag von 8:30 bis 14:00 Uhr und von 15:00 bis 18:00 Uhr
  - Freitag von 8:30 bis 14:30 Uhr

- E-Mail:salvatlogistica@sistema-interno-informacion.com

Ein weiterer Kanal, den die Gruppe ihren Mitarbeitern und Drittparteien, mit denen sie interagiert, zur Verfügung stellt, ist der persönliche Kontakt. Dieser ermöglicht die Übermittlung mündlicher Mitteilungen in einem persönlichen Treffen oder per Videokonferenz. Angesichts der Komplexität, die die Gruppe mit der Wahrung der Anonymität des Hinweisgebers in den Fällen, in denen dies gewünscht wird, verbindet, hat die Gruppe diese Funktion dem externen Experten BONET Consulting übertragen. Dieser ist für den Empfang und die Bearbeitung solcher Mitteilungen sowie aller anderen Fälle zuständig, in denen die Hinweisgeber identifiziert werden und ein persönliches Gespräch erforderlich ist.
Dabei gewährleistet der externe Experte den Schutz der Identität des Hinweisgebers sowohl im Rahmen der Terminanfrage als auch bei der persönlichen Abgabe einer Mitteilung und am Ort der Termindurchführung.

Um die Sicherheit und Integrität der vom Informanten bereitgestellten Informationen zu gewährleisten, wird das Gespräch gemäß den gesetzlichen Bestimmungen und mit vorheriger Zustimmung des Informanten aufgezeichnet. Das Gespräch wird in einem sicheren Format unter Einhaltung der gesetzlich vorgeschriebenen Sicherheits- und Anonymitätsmaßnahmen dokumentiert. Zu diesem Zweck verfügt BONET Consulting über die notwendigen technologischen Mechanismen, um ergänzende Unterlagen zu den im Gespräch bereitgestellten Informationen zu versenden.

Um diesen Kanal nutzen zu können, hat die Gruppe eine Telefonnummer und eine E-Mail-Adresse für Anfragen zur Übermittlung von Mitteilungen in diesem Format eingerichtet. BONET Consulting ist ausschließlich für die Abwicklung und Koordination des Treffens verantwortlich. Die entsprechenden Kontaktinformationen sind auf der Website der Gruppe veröffentlicht.