

SISTEMA DE INFORMAÇÃO INTERNO

MERZ AESTHETICS IBERIA, S.L. (doravante, a Entidade) implementou um **Sistema Interno de Informação (SIIF)**, que integra os diferentes canais internos de informação da organização e está configurado como um eixo fundamental para a promoção da cultura de ação ética, responsável e sustentável, com o dever de supervisão, controlo e prevenção em termos de conformidade regulamentar.

O sistema é o canal preferido e uma ferramenta obrigatória para canalizar diligentemente comunicações sobre infrações e incumprimento das regulamentações, com total proteção dos denunciantes, sem risco de represálias e com as medidas de proteção necessárias. Da mesma forma, este sistema constitui o principal canal para a submissão de comunicações relacionadas com situações de assédio no local de trabalho, assédio sexual, discriminação ou outras condutas contrárias às regulamentações internas ou à legislação vigente nesta área.

Para aprender em detalhe os princípios de ação e as garantias fundamentais que regem o Sistema Interno de Informação da Entidade em virtude dos requisitos exigidos pelos novos regulamentos, pode consultar e aceder à [Política Geral do Sistema de Informação Interna e Defesa contra Denunciantes](#)

Canais de Informação

A Entidade habilitou diferentes canais internos de informação que permitem a submissão de comunicações em formato escrito ou verbal. Para tal, a Entidade conta com a configuração, conceção e apoio de um especialista externo para proporcionar os mais elevados níveis de profissionalismo, experiência, independência, confidencialidade, proteção de dados e denunciante, bem como outras áreas aplicáveis a este tipo de canal.

Canal online/Digital

A Entidade disponibiliza uma ferramenta online através da qual qualquer colaborador ou pessoa relacionada com a Entidade pode submeter uma comunicação escrita através do seguinte [link](#).

Esta ferramenta possui medidas de segurança que garantem a proteção da informação, da identidade do informador e dos seus afetados, bem como a confidencialidade e confidencialidade de todo o processo de gestão e processamento da comunicação.

Canal presencial

Outra das formas que a Entidade disponibiliza aos seus colaboradores e aos terceiros que lhe estão relacionados é o canal presencial, que permite a apresentação de comunicações verbais através de uma reunião presencial ou por videoconferência.

Os dados de contacto para utilizar o canal presencial são os seguintes: SIIF.AX@merz.com.

Canal Telefónico (Espanha)

Se preferir falar com alguém de forma confidencial, contacte-nos para o **900 031 156** e um dos nossos representantes terá todo o gosto em ajudá-lo.

(NOTA: Esta não é uma linha de emergência. Se estiver a reportar uma emergência, por favor contacte o serviço de emergência apropriado ou as autoridades policiais da sua região ou país específico.)

Por favor, siga as instruções descritas acima para aceder corretamente e utilizar os canais oficiais habilitados pela Entidade para a submissão de comunicações e aplicação de todos os nossos mecanismos de segurança e proteção necessários.

Se tiver alguma dúvida sobre o funcionamento do Sistema de Informação Interno da Entidade, pode contactar o Gestor do Sistema através do seguinte email: SIIF.AX@merz.com.

Proteção de dados

O tratamento de dados pessoais derivados do canal de denúncia será regulado pelas disposições do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, na Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção dos Dados Pessoais e garantia dos direitos digitais, e na Lei Orgânica 7/2021, de 26 de maio, sobre a proteção dos dados pessoais tratados para fins de prevenção, deteção, investigação e acusação de crimes e execução de sanções criminais.

A MERZ AESTHETICS IBERIA, S.L.U. disponibiliza-lhe aqui um Sistema Interno de Informação, SIIF, para a comunicação de possíveis condutas que constituam infrações, para efeitos da Lei 2/2023, de 20 de fevereiro, que regula a proteção de pessoas que denunciam infrações regulamentares e o combate à corrupção. Este canal é constituído como um meio de comunicação transparente e absolutamente confidencial que visa canalizar quaisquer queixas que a Entidade possa receber.

A comunicação através do Sistema de Informação Interna (SIIF) pode levar ao início de investigações internas ou externas e pode ter consequências negativas para os afetados. Por esta razão, deve fornecer-nos apenas informações que sejam verdadeiras, tanto quanto o seu conhecimento, e que sejam relevantes para detetar uma violação da conformidade regulamentar e/ou do Código de Ética ou Conduta da Entidade.

Em conformidade com as regulamentações atuais sobre a Proteção dos Dados Pessoais, a Entidade informa-o de que os dados pessoais que possa fornecer ao apresentar a queixa, bem como quaisquer outras informações pessoais que possam ser recolhidas nos processos de investigação que possam ser iniciados, serão processados pela Entidade para fins de gestão da sua comunicação. para investigar os factos denunciados, adotar as medidas corretivas pertinentes, se necessário, e mantê-lo informado sobre o resultado do procedimento.

Caso o denunciante tenha optado por apresentar a queixa de forma anónima, não será realizado qualquer tratamento dos seus dados pessoais.

Toda a informação fornecida será tratada de forma confidencial pelo pessoal interno da Entidade e não será comunicada a terceiros, salvo se tal for necessário para a investigação dos factos denunciados, caso em que os dados serão comunicados à empresa-mãe do Grupo Merz, cuja participação é essencial na gestão do Sistema de Informação Interno - SIIF corporativo e, quando apropriado, à empresa do grupo afetada pela queixa cuja participação é necessária no processo de investigação.

La base jurídica que legitima este tratamiento es el cumplimiento de las obligaciones legales que resultan de aplicación a la Entidad y el interés legítimo de la Entidad.

Toda a informação fornecida será processada durante o período necessário para a sua investigação, de acordo com as disposições dos regulamentos em vigor. Em todo o caso, se decorrerem três meses desde a introdução dos dados sem que tenham sido iniciadas quaisquer ações de investigação, estes serão eliminados, salvo se o objetivo da retenção for deixar provas do funcionamento do sistema. No caso de qualquer responsabilidade legal pelos factos apresentada ao conhecimento da Entidade, os dados serão mantidos pelo tempo necessário para cumprir essas responsabilidades e para que a Entidade, quando apropriado, possa tomar as medidas legais necessárias.

Se forneceu dados pessoais que permitam a sua identificação, pode exercer, sempre que aplicável, os seus direitos de acesso, retificação, eliminação, oposição, limitação e portabilidade relativamente aos dados pessoais que forneceu, através do email: informacion.cliente@merz.com. Se considerar que o seu direito à proteção de dados foi violado, pode apresentar uma queixa à Agência Espanhola de Proteção de Dados (www.aepd.es) ou ao Responsável pela Proteção de Dados da Entidade (informacion.cliente@merz.com).

POLÍTICA GERAL DO SISTEMA INTERNO DE INFORMAÇÃO E DEFESA DOS DENUNCIANTES



Índice

1. INTRODUÇÃO	1
2. PRINCÍPIOS DE AÇÃO E GARANTIAS ESSENCIAIS	2
3. ENTIDADE RESPONSÁVEL PELO SISTEMA INTERNO DE INFORMAÇÃO	4
4. AUTORIDADE INDEPENDENTE DE PROTEÇÃO DE DENUNCIANTES	5
5. CONFIDENCIALIDADE E PROTEÇÃO DE DADOS PESSOAIS	6
6. MEDIDAS DE PROTEÇÃO	7
7. REGIME DISCIPLINAR	11
8. COMUNICAÇÃO, REVISÃO E ATUALIZAÇÃO	12
9. CANAIS INTERNOS DE INFORMAÇÃO	13
Canal Digital.....	13
Canal Presencial	14
Canal Telefónico.....	14

1. INTRODUÇÃO

A transposição da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho de 23 de outubro de 2019 para o direito espanhol, com **a Lei 2/2023 de 20 de fevereiro de 2023, que regula a proteção das pessoas que denunciam violações regulamentares e o combate à corrupção**, envolve a incorporação de instrumentos específicos para que, Quem conhece ações ilegais ou irregulares pode fornecer dados e informações úteis, garantindo uma proteção total e eficaz desses informadores.

Neste sentido, o regulamento referido regula os aspetos mínimos que devem ser satisfeitos pelos diferentes canais internos e externos de informação, juntamente com o regime especial de proteção para denunciadores que atuem de boa-fé e consciência honesta, de forma desinteressada.

De acordo com o exposto acima, **a MERZ AESTHETICS IBERIA S.L.U.** implementou um **Sistema Interno de Informação (SIIF)**, que está configurado como um eixo fundamental para supervisão, controlo e prevenção no campo da conformidade regulatória. Tal sistema é um canal preferencial e uma ferramenta de uso obrigatório para canalizar a informação de forma diligente, de modo a fortalecer a cultura de informação dentro da própria organização.

O SIIF foi concebido como um instrumento de controlo e prevenção, que inclui canais de informação geridos tanto internamente como por uma empresa externa especializada. Estes canais beneficiam dos mais elevados níveis de profissionalismo, experiência, independência, confidencialidade, conformidade com regulamentos de proteção de dados e outros quadros regulatórios aplicáveis. Da mesma forma, o SIIF garante os princípios básicos do anonimato, registo adequado, conservação e não alteração, prevenção de conflitos de interesse, proteção do denunciante e proibição de retaliação.

De acordo com a referida Lei, é um requisito essencial que o SIIF tenha uma **Política que enuncie os princípios gerais do sistema e a defesa do informador**, devidamente divulgada dentro da Entidade. Portanto, juntamente com o Procedimento para gerir a informação recebida, esta Política é um elemento essencial da configuração e operação do SIIF.

2. PRINCÍPIOS DE AÇÃO E GARANTIAS ESSENCIAIS

O **Sistema de Informação Interna (SIIF)** é um dos principais eixos dos sistemas de conformidade regulamentar e prevenção criminal. De acordo com os mais elevados requisitos de diligência nesta área, a Entidade forneceu ao SIIF uma série de garantias para garantir a sua eficácia, com a colaboração e apoio do consultor externo **especializado BONET**. Especificamente, os princípios básicos e garantias fundamentais que regem o processo e as ações da Entidade em relação ao SIIF são os seguintes:

- > **Independência, autonomia, imparcialidade e ausência de conflitos de interesse:** Na receção e processamento de informação sobre infrações, foram definidos mecanismos de reação para gerir e controlar possíveis conflitos de interesses e/ou falta de independência, quando os responsáveis pela gestão, controlo e/ou supervisão apresentam uma série de características que comprometem e condicionam o desempenho das suas funções. Da mesma forma, todas as comunicações recebidas estão sujeitas a análise com os requisitos necessários de independência, que garantem equidade e justiça no seu tratamento.
- > **Profissionalismo e experiência:** Profissionais especialistas em conformidade regulamentar, prevenção criminal e boa governação são responsáveis pelo processamento e gestão adequada das comunicações, preservando os direitos dos informadores e daqueles reportados.
- > **Completude, integridade e confidencialidade da informação:** Os participantes nas diferentes fases da investigação têm o dever de confidencialidade relativamente a qualquer informação a que possam ter acesso ou conhecimento devido ao exercício das suas funções. Além disso, o acesso a ela por pessoal não autorizado é impedido e é permitido que seja armazenada de forma durável e segura, através da geração de backups de informação e ficheiros independentes.
- > **Proteção de dados e segredo das comunicações:** O tratamento de dados está de acordo e está em conformidade com as mais elevadas medidas e políticas para a proteção de dados pessoais, em conformidade com as regulamentações aplicáveis sobre a Proteção de Dados Pessoais. Da mesma

forma, existe um dever de segredo relativamente a qualquer aspeto relacionado com a informação comunicada.

- > **Anonimato e Anonimização:** Prevê-se a possibilidade de submeter e posteriormente processar comunicações anónimas, bem como o dever geral de preservar a identidade do informador identificado ao realizar a comunicação, mantendo-o anónimo e não revelando a sua identidade a terceiros.
- > **Utilização acessível, simplicidade e gratuita:** A simplicidade da comunicação é garantida, o que permite o acesso universal ao sistema sem custo associado, e a aplicação eficaz da legalidade e dos princípios éticos que regem a atividade da Entidade.
- > **Registo adequado e independente:** É preparado um livro de registos privado das informações recebidas e das investigações internas a que estas deram lugar, como garantia do seu processamento, gestão e não alteração, de forma independente e sem conflitos de interesse, por um período necessário e proporcional de acordo com a legislação vigente. Em nenhum caso os dados serão mantidos por um período superior a dez anos.
- > **Boas práticas de monitorização e investigação:** Para verificar a veracidade das comunicações, a recolha correta de provas e garantir os direitos dos afetados, o ciclo de vida da comunicação será regulado num procedimento interno eficaz e transparente. Estas práticas serão documentadas no Procedimento para a gestão da informação recebida.
- > **Proteção dos denunciadores e dos titulares dos dados:** As pessoas que reportarem ou divulgarem violações têm direito a medidas de proteção e não estarão sujeitas a quaisquer retaliações ou consequências adversas pela sua cooperação, incluindo ameaças de retaliação e tentativa de retaliação. De igual modo, as pessoas afetadas pela comunicação terão direito à mesma proteção estabelecida para os informadores, preservando a sua identidade e garantindo a confidencialidade dos factos e dados do procedimento.
- > **Ação diligente, responsabilidade e boa-fé do informador:** A utilização do sistema baseia-se nos princípios de responsabilidade, diligência e boa-fé, de modo que todo informador deve ter motivos razoáveis para acreditar que a informação é verdadeira no momento da sua comunicação. A comunicação de factos infundados, falsos ou distorcidos, bem como a submissão de informações obtidas ilegalmente, com uma atitude maliciosa e moralmente desonesta,

constitui violação do princípio da boa-fé e pode levar à aplicação de medidas disciplinares.

3. ENTIDADE RESPONSÁVEL PELO SISTEMA INTERNO DE INFORMAÇÃO

Para a eficácia do **Sistema de Informação Interno (SIIF)**, é essencial nomear uma pessoa responsável pelo seu funcionamento adequado, organização e processamento diligente da informação. Da mesma forma, este último será responsável por garantir a comunicação e disseminação adequadas do SIIF, bem como por executar e atualizar o plano de formação relevante.

O órgão administrativo ou órgão regulador da Entidade é competente para a designação e comunicação à autoridade competente da pessoa física ou do órgão colegiado responsável pela gestão do referido sistema e pela sua demissão ou destituição (doravante, o Órgão **Responsável pelo Sistema**).

O Órgão Responsável pelo Sistema desempenha as suas funções **de forma independente e autónoma** em relação aos restantes órgãos organizacionais da Entidade, evitando possíveis situações de conflito de interesses com o desempenho ordinário da sua posição. No entanto, o Órgão Responsável pelo Sistema pode recorrer a terceiros para receber apoio especializado e/ou cumprir os requisitos de independência, garantindo o correto desempenho das suas funções.

Em particular, para o exercício das suas funções, o Órgão Responsável pelo Sistema coordenará com os seguintes assuntos:

- A** O responsável pelos recursos humanos, quando podem ser tomadas medidas disciplinares contra as pessoas envolvidas e/ou a aplicação de medidas de proteção, pode ser coordenada.
- B** Os responsáveis pela conformidade regulamentar e/ou pelos serviços jurídicos da Entidade, se aplicável, pela adoção de medidas legais ou regulatórias de conformidade que devem ser tidas em consideração relativamente às comunicações recebidas no SIIF.
- C** Os processadores de dados que podem ser designados.

- D** O Responsável pela Proteção de Dados.
- E** Outras pessoas e/ou entidades envolvidas na gestão do SIIF.

4. AUTORIDADE INDEPENDENTE DE PROTEÇÃO DE DENUNCIANTES

O **Sistema Interno de Informação da Entidade (SIIF)** é o meio prioritário e obrigatório para a comunicação de condutas ou infrações ilegais de que tem conhecimento, pois assegura a devida adoção de medidas de proteção e promove a cultura da informação dentro da organização.

No entanto, foram determinados outros canais de informação "externos", de modo a oferecer aos cidadãos uma alternativa onde apresentar a comunicação e/ou queixa, caso os canais internos não cumpram as garantias exigidas pelas regulamentações aplicáveis, as medidas de proteção relevantes não sejam aplicadas ou as pessoas fiquem expostas a represálias pelo seu estatuto de informadores.

Consequentemente, qualquer pessoa física pode reportar diretamente à **Autoridade Independente para a Proteção dos Denunciantes, A.A.I.** da comissão de quaisquer ações ou omissões que constituam violação do sistema jurídico, através do canal externo de informação dessa autoridade pública especializada. O acesso a este canal externo de informação e os dados de contacto da Autoridade são publicados no seu website.

5. CONFIDENCIALIDADE E PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais derivados do **Sistema Interno de Informação (SIIF)** é regulado pelas disposições do Regulamento (UE) 2016/679 do Parlamento Europeu, de 27 de abril de 2016, da Lei Orgânica 3/2018, de 5 de dezembro, e da Lei Orgânica 7/2021, de 26 de maio. Assim, no momento da recolha, as partes interessadas são informadas do tratamento dos seus dados e dos seus direitos, de acordo com os regulamentos vigentes.

Em conformidade com o princípio da **minimização de dados**, os dados pessoais recolhidos são os necessários e relevantes para o processamento da comunicação. No caso de os dados serem recolhidos por acidente, o que não é necessário para o conhecimento e investigação das ações ou omissões, serão eliminados sem demora indevida. Da mesma forma, os dados serão mantidos pelo tempo necessário para decidir o precedente de iniciar uma investigação.

Por outro lado, o desenho do SIIF garante a **confidencialidade** da identidade do informante e de qualquer terceiro mencionado na comunicação, bem como as ações realizadas na gestão e processamento da comunicação. Neste sentido, o acesso a dados pessoais e outras informações contidas no sistema é limitado aos responsáveis pela gestão, dentro do âmbito das suas competências e funções. Por isso, existem medidas técnicas e organizacionais adequadas para preservar a identidade dos afetados e impedir o acesso de pessoas não autorizadas.

Em caso de qualquer dúvida ou questão relativa ao tratamento de dados pessoais realizado dentro da Entidade em relação ao SIIF, qualquer parte interessada pode contactar o **Responsável de Proteção de Dados** designado, por email para o endereço: informacion.cliente@merz.com

A Entidade tem uma Política de Privacidade onde são fornecidas informações sobre o tratamento de dados pessoais recolhidos através do SIIF, que pode ser [consultada aqui](#).

6. MEDIDAS DE PROTEÇÃO

As pessoas que reportam ou divulgam violações através do **Sistema de Informação Interno da Entidade (SIIF)** têm direito à proteção, **nas mesmas condições que aquelas que reportam através de canais externos, desde que tenham fundamentos razoáveis para acreditar que a informação referida é verdadeira no momento da comunicação ou divulgação, mesmo que não forneçam provas conclusivas.**

Neste sentido, são expressamente proibidos atos que constituam **retaliação**, incluindo ameaças e tentativas, contra pessoas que submetam uma comunicação. Retaliação significa:

- a** Atos ou omissões proibidos por lei.
- b** Atos ou omissões que envolvam direta ou indiretamente tratamento desfavorável, colocando a pessoa em desvantagem em relação a outra.

Como exemplo e não limitação, os seguintes são considerados retaliação:

- > Suspensão do contrato de trabalho, despedimento ou cessação da relação, rescisão antecipada, cancelamento do contrato de trabalho e/ou comercial, medidas disciplinares, repreensão ou outra sanção, degradação ou recusa de promoções, modificação substancial das condições e não conversão do contrato temporário em contrato indefinido ou medidas equivalentes.
- > Danos (incluindo danos reputacionais), perdas financeiras, coerção, intimidação, assédio ou ostracismo.
- > Avaliação negativa ou referências sobre trabalho ou desempenho profissional.
- > Listas negras ou disseminação de informação que dificulta ou impede o acesso ao emprego/contratos para trabalhos ou serviços.
- > Negação ou cancelamento da licença ou autorização.
- > Recusa de formação.
- > Discriminação, tratamento desfavorável ou injusto.

- > Recusa de incentivos, benefícios, bônus, comissões e qualquer outro tipo de compensação.
- > Rescisão antecipada, suspensão, alteração ou cancelamento de contratos de bens ou serviços.

Estes atos serão nulos e sem efeito e, quando apropriado, darão origem a medidas disciplinares ou corretivas de responsabilidade, que poderão incluir a compensação correspondente pelos danos causados pela parte lesada.

Para garantir o direito à proteção do denunciante e das pessoas afetadas pela comunicação, a Entidade estabeleceu as seguintes medidas técnicas e organizacionais aplicadas desde o momento inicial em que a comunicação é recebida:

1 Configuração do SIIF: O SIIF foi concebido com as medidas técnicas e organizacionais adequadas para garantir a proteção da identidade do informador, bem como dos dados e informações derivados das comunicações apresentadas. Neste sentido, a Entidade criou uma série de canais internos de informação, que permitem que as comunicações sejam submetidas de forma anónima. Estes canais são:

- **Canal digital:** Plataforma digital para a apresentação de comunicações escritas.
- **Canal telefónico:** 031 156
- **Canal presencial:** O sistema para receber comunicações através de uma reunião presencial, solicitando-as por escrito dirigindo-se a SIIF.AX@merz.com.

Independentemente do canal utilizado, o SIIF garante a aplicação eficaz dos princípios e garantias básicos especificados nesta Política, de modo a cumprir os requisitos do quadro regulamentar e proteger os direitos dos denunciantes e das pessoas afetadas.

2 Órgão Responsável do SIIF: Para garantir a correta aplicação do SIIF, a Entidade designou um Órgão Responsável cuja função é supervisionar, monitorizar e controlar o seu funcionamento. Neste sentido, o Órgão Responsável, juntamente com o perito externo, adotará as medidas de proteção necessárias e garantirá o seu devido acompanhamento e aplicação. A

participação do perito externo confere às funções do Órgão Responsável os elementos de autonomia e independência exigidos pelas regulamentações vigentes.

Da mesma forma, o Órgão Responsável será responsável por realizar uma análise preliminar das comunicações recebidas, de modo a determinar a adequação da adoção de medidas específicas de proteção relativamente ao denunciante e/ou terceiros afetados. Além disso, dependendo da natureza e do âmbito da informação, o Órgão Responsável terá o apoio e aconselhamento dos responsáveis das diferentes áreas operacionais da Entidade, para a conclusão bem-sucedida da investigação. Também poderá recorrer a terceiros especializados em matérias que requerem um parecer especialista.

- 3 Custódia, gestão e segurança da informação do SIIF:** A Entidade possui um sistema de gestão documental configurado com as medidas de segurança e controlo adequadas, de modo a demonstrar a eficácia do próprio SIIF. Deve notar-se que este sistema inclui processos de anonimização, para não permitir a identificação de informadores. Além disso, a Entidade adotou medidas técnicas razoáveis para a preservação, recuperação e eliminação segura de informações, bem como para a implementação de controlos de acesso para prevenir o uso não autorizado.

No entanto, informações apresentadas que sejam falsas, distorcidas, manifestamente careçam de qualquer plausibilidade e fundamento, ou que existam indicações razoáveis de que foram obtidas através da prática de um crime, estão excluídas da proteção mencionada. Isto porque todas as comunicações devem ser feitas de **boa-fé** e, portanto, o informador deve ter motivos razoáveis para acreditar que a informação é verdadeira no momento da comunicação. Em resumo, o princípio da boa-fé exige que, em nenhum caso, se possa inferir que existe falsidade, falta de verdade, intenção de vingança ou de prejudicar um terceiro.

É importante lembrar que as medidas de proteção não são dirigidas apenas a favor dos informadores. As pessoas a quem se referem os factos reportados na comunicação (**pessoas afetadas**) também têm uma proteção única contra o risco de que a informação, mesmo com sinais aparentes de veracidade, tenha sido manipulada, seja falsa ou responda a outras motivações. Durante o processamento do processo, estas pessoas têm direito à presunção de inocência, à proteção e defesa judiciais, ao acesso ao processo, bem como à confidencialidade dos factos e dados do procedimento e à

confidencialidade da sua identidade. Em conclusão, têm a mesma proteção e direitos de que o informador desfruta.

7. REGIME DISCIPLINAR

O incumprimento das regulamentações aplicáveis e a conduta contrária às instruções, políticas, códigos, procedimentos e protocolos da Entidade constitui fundamento para a aplicação do **regime disciplinar ao nível laboral e comercial**, em coordenação com as disposições do Acordo Coletivo aplicável, do Estatuto dos Trabalhadores e das restantes regulamentações aplicáveis.

A Entidade notificará e sancionará quaisquer ações ou omissões contrárias a esta Política incorridas por funcionários, colaboradores ou qualquer membro relacionado com a Entidade e, em particular:

- > Falha em reportar qualquer suspeita ou conhecimento de violações e violações do quadro regulatório e dos protocolos e regras internos da Entidade através do SIIF.
- > Qualquer tentativa ou ação eficaz para dificultar a submissão de comunicações ou para impedir, frustrar ou atrasar o seu seguimento.
- > O uso do SIIF de má-fé, por exemplo, com a disponibilização de informação ou documentação sabendo da sua falsidade.
- > A adoção de qualquer retaliação derivada da comunicação contra os informadores ou outras pessoas afetadas.
- > Violação das garantias de confidencialidade e anonimato, revelação da identidade das pessoas afetadas e violação do dever de segredo da informação.
- > Incumprimento da obrigação de cooperar com a investigação da informação.

8. COMUNICAÇÃO, REVISÃO E ATUALIZAÇÃO

Esta Política, bem como toda a informação necessária sobre a utilização do **Sistema de Informação Interno (SIIF)** implementado, está disponível numa secção separada e rapidamente identificável, para que todas as partes interessadas a tenham à disposição de forma clara e facilmente acessível. No entanto, qualquer pessoa pode solicitar informações adicionais à Entidade através do seguinte email: SIIF.AX@merz.com

O Órgão **Responsável pelo Sistema** irá periodicamente rever e, quando apropriado, propor ao órgão administrativo ou órgão governativo da Entidade a atualização desta Política, de modo a adaptá-la a todas as circunstâncias e alterações que possam surgir, bem como aos regulamentos ou jurisprudência que possam ser emitidos. Tudo isto com o objetivo de adaptar o SIIF aos requisitos máximos de conformidade regulamentar para o seu correto funcionamento e eficácia.

Da mesma forma, a Entidade está aberta a qualquer **sugestão e/ou proposta** que possa melhorar o seu desempenho ético e promover uma cultura de conformidade regulamentar, sublinhando a necessidade de todos os colaboradores e membros relacionados com a Entidade ou terceiros colaborarem para cumprir os seus valores e princípios.

9. CANAIS INTERNOS DE INFORMAÇÃO

Para cumprir as disposições da Lei 2/2023, a Entidade implementou um sistema configurado com os requisitos técnicos e processuais exigidos por essa Lei para a devida atenção às comunicações. Tudo isto com o objetivo de oferecer aos informadores um ambiente de comunicação seguro, confidencial ou até anónimo com a Entidade, processando a informação de forma eficiente, profissional e independente.

Para tal, a Entidade disponibilizou-se com recursos materiais, técnicos e humanos para permitir diferentes canais internos que permitam a submissão de comunicações em formato escrito ou verbal. Estes canais têm a configuração, design e apoio de um especialista externo para proporcionar os mais elevados níveis de profissionalismo, experiência, independência, confidencialidade, proteção de dados e denunciante, bem como outras áreas aplicáveis a este tipo de canal.

Deve notar-se que a informação fornecida através de qualquer um dos canais internos será tratada de forma confidencial, e apenas pessoal autorizado terá acesso a ela para a sua gestão e processamento adequados.

Seguem-se os canais disponíveis para qualquer colaborador ou terceiro ligado à Entidade para a submissão de comunicações:

Canal Digital

A Entidade dispõe de uma ferramenta digital que permite submeter comunicações escritas através de um formulário, que permite anexar ficheiros. Uma vez preenchido o formulário, a ferramenta gera automaticamente um código que permite que a pessoa responsável pelo processamento seja devidamente monitorizada e gerida. Da mesma forma, é enviada uma confirmação ao informador sobre a introdução e registo da comunicação no sistema, que contém um resumo da informação fornecida, bem como o código, para que possa também realizar este seguimento.

Esta ferramenta possui medidas de segurança que garantem a proteção da informação, da identidade do informador e dos seus afetados, bem como a confidencialidade e confidencialidade de todo o processo de gestão e processamento da comunicação. A ferramenta também permite a submissão de comunicações de forma anónima. O link

para aceder a esta ferramenta e ao seu âmbito de utilização está disponível no site da Entidade.

Canal Presencial

Outra das formas que a Entidade disponibiliza aos seus colaboradores e aos terceiros que lhe estão relacionados é o canal presencial, cujo objetivo é permitir a apresentação de comunicações verbais através de uma reunião presencial.

Para garantir a segurança e preservar a integridade das informações fornecidas pelo informador, a reunião será documentada por transcrição escrita, de acordo com as disposições da Lei e com o consentimento prévio do informador. Esta reunião será documentada num formato seguro, com as medidas de segurança e anonimização exigidas pelo quadro regulamentar.

Para utilizar este canal, a Entidade ativou um email de contacto para solicitar a submissão de comunicações neste formato: SIIF.AX@merz.com.

Canal Telefónico

A Entidade dispõe de um Canal Telefónico dedicado para a apresentação de comunicações verbais, de modo a oferecer uma forma acessível e direta de reportar qualquer incidente ou comportamento inadequado. Este canal é gerido por uma empresa externa especializada que assegura confidencialidade e imparcialidade na gestão da informação fornecida. Graças a esta gestão externa, é garantido que as comunicações são tratadas de forma objetiva e segura, protegendo a identidade do denunciante e garantindo que todos os casos sejam avaliados de forma justa e sem influências internas.

DIREITOS DE AUTOR

O conteúdo desta política geral sobre o sistema interno de informação está sujeito a direitos de autor. Consequentemente, para prosseguir com a sua distribuição ou comunicação a outras entidades, é necessário o consentimento expresso do titular dos direitos de autor.