



CPS 7.202- Credibom Procedures and Standard

Direitos e Obrigações dos Colaboradores - Reporte de Incidentes e Linhas de Ética



Título	Direitos e Obrigações dos Colaboradores – Reporte de Incidentes e Linhas de Ética Identificação da CPS	Versão	3.0
Owner	Gabinete de Compliance e Apoio Jurídico	Data do Documento	18-11-2021
Aprovado por	ICC	Data Efeito	19-11-2021

GPS CACF	N/A
-----------------	-----

Motivo de Atualização	Atualização da informação relativa à nova ferramenta do Grupo e ao Aviso 3/2020
Documentos Complementares	CPS 7.201 – Credibom Código de Conduta v04 GPS 511_ Função de Compliance GPS 510 - Risk and Permanent Control Policy NP 2020-19 - Whistleblowing GPS 513 Organização e Gestão da Fraude GPS 514 Warning system by nature of risk GPS 518 Operational risk management
Documentos Revogados	CPS_7.202- Reporte de incidentes e linhas de ética v02
Sumário	Assegura a implementação de um sistema de deteção, reporte e correção de incidentes e irregularidades na aplicação de leis, regulamentos, código de conduta e padrões profissionais, com regras e responsabilidades definidas, garantindo-se um adequado sistema de controlo interno.

Unidades Orgânicas intervenientes			
<input checked="" type="checkbox"/> Todas	<input type="checkbox"/> CE	<input type="checkbox"/> GRCP	<input type="checkbox"/> DO
<input type="checkbox"/> GESC	<input type="checkbox"/> GCAJ	<input type="checkbox"/> DTI	<input type="checkbox"/> CISO
<input type="checkbox"/> DFIN	<input type="checkbox"/> DRH	<input type="checkbox"/> DM	
<input type="checkbox"/> DCOM	<input type="checkbox"/> DRC	<input type="checkbox"/> GAI	

Histórico de Versões		
Versões	Data do Documento	Data Efeito
1	10-04-2017	04-05-2017
2	11-10-2018	19-10-2018-
3	18-11-2021	19-11-2021



Índice

Índice	3
1. Âmbito.....	5
2. Objetivos	6
3. Definição de conceitos	6
3.1 Incidente de compliance	6
3.2 Irregularidades	7
3.3 Whistleblowing	7
3.4 Banco de Portugal.....	8
4. Responsabilidades	9
4.1 Colaboradores em geral	9
4.2 Responsáveis departamentais	9
4.3 Gabinete de Compliance e Apoio Jurídico	10
4.4 Auditoria Interna	11
5. Comunicação de irregularidades – Linha de Reporte	11
5.1 Regras Gerais	11
5.2 Requisitos	12
5.3 Plataformas de reporte.....	13
5.4 Tratamento de incidentes.....	14
6. Confidencialidade e proteção do denunciante.....	16
6.1 Confidencialidade	16
6.2 Proteção do whistleblower.....	16
6.3 Informação sobre a(s) pessoa(s) envolvida(s) no alerta.....	17
6.4 Proteção e preservação de dados	17
6.5 Denúncias anónimas	18
7. Relatórios e Controlo	18
7.1 Reporte	18
8. Matriz RACI	19
9. Regra especial relativa a dados pessoais e tratamento de dados pessoais	19
10. - Anexo 1 – Política de Comunicação de Irregularidades no Banco Credibom S.A.	20
10.1 Objeto	20
10.2 Definição.....	20



10.3 Entidades aplicáveis	20
10.4 Comunicação de Irregularidades e Contactos	20
10.5 Outros modos de receção de comunicações	21
10.6 Acesso à Informação e Documentação	21
10.7 Competências	21
10.8 Reporte a entidades oficiais.....	21



1. Âmbito

O respeito pelas regras de compliance baseia-se no princípio da existência de medidas preventivas para assegurar que o Banco Credibom como entidade integrante do Grupo Credit Agricole, no âmbito do controlo interno, não se encontra em situação de presença/prevalência de risco de uma sanção legal, administrativa ou disciplinar, perda financeira significativa ou dano à sua reputação como um resultado da incapacidade de respeitar as disposições específicas para atividades bancárias e financeiras. Estas disposições podem ser legais ou regulamentares, ser expressas em padrões profissionais ou códigos de conduta, ou podem ser apenas instruções do órgão executivo.

Paralelamente, vem o Banco de Portugal ("BdP"), por meio do Aviso N.º 3/2020, estabelecer deveres de comunicação por parte dos Administradores e dos membros dos órgãos de supervisão, junto do BdP, quando se verificarem situações de desconformidade com o normal funcionamento do Banco, quer sejam por estes detetadas ou a estes transmitidas pelos colaboradores.

O programa de compliance do Grupo Credit Agricole SA está baseado em três pilares fundamentais: uma organização assente na esfera da função de Compliance, um conjunto de procedimentos que regulam o exercício desta função e a existência de sessões de sensibilização/formação que assegurem a assimilação dos princípios e regulamentos existentes.

Organização: a organização explora duas linhas de negócio - Compliance e Assessoria Jurídica - que constituem a função de Compliance na sua generalidade;

Um conjunto de procedimentos a serem adaptados a todas as entidades do Grupo CA, SA com os seguintes objetivos:

- Especificar as regras de funcionamento para as duas linhas de negócio (Compliance e Assessoria Jurídica), assim como a cooperação entre as respetivas Áreas;
- Reiterar os princípios e medidas operacionais que devem ser respeitados, quer para as atividades focadas no cliente ("Know Your Customer", lançamento de novos produtos e atividades, etc.);
- Organizar formas de comunicação que permitam envolver a área de Compliance e criação de meios de rastreabilidade confiáveis.

Existência de sessões de sensibilização/formação que permitam:

- Desenvolver uma boa compreensão do mecanismo de compliance, incluindo as questões, conceitos, diretrizes e procedimentos;
- Adotar comportamentos face às situações que ocorrem no seio da entidade;
- Desenvolver novas práticas.

A implementação destas disposições cria condições favoráveis para o reforço dos controlos *a priori* e, assim,



contribuir para o seu mecanismo de controlo permanente. No entanto, quando estas medidas preventivas não evitam a ocorrência de uma lacuna ou irregularidade de compliance, é importante que a questão:

- Seja detetada e analisada o mais rápido possível;
- Suscite a atenção dos responsáveis das Unidades Orgânicas e em especial do Gabinete de Compliance e Apoio Jurídico;
- Seja monitorizada e corrigida, e as suas causas eliminadas.

O objetivo deste procedimento é então definir os princípios, responsabilidades e processos que irão reger estas três etapas do processo.

Desta forma, com este documento pretende-se:

- Assegurar a distinção e aplicabilidade dos conceitos “incidente” vs. “irregularidade”;
- Garantir a existência de mecanismos para reporte, análise e correção de incidentes e irregularidades, como parte fundamental do processo de auto-regulação e auto-correção no seio do reforço da política de compliance do Credibom;

2. Objetivos

Este documento pretende definir e formalizar as regras de gestão de um sistema de deteção, reporte e correção de incidentes e irregularidades na aplicação de leis, regulamentos, código de conduta e padrões profissionais, assim como garantir a existência de um mecanismo de controlo na gestão do mesmo salvaguardando a confidencialidade das situações que se enquadrem no âmbito deste documento.

O direito de denúncia visa reforçar a prevenção de riscos, mediante a concessão a qualquer empregado do Grupo, qualquer entidade ou pessoa externa ao Grupo e ao Credibom, nomeadamente qualquer fornecedor ou subcontratado com quem o Grupo tenha estabelecido uma relação comercial, o denunciante (ou “whistleblower”) de meios para comunicar, desinteressadamente e de boa-fé, qualquer suposto facto (“o alerta”) de que tenha tomado conhecimento pessoalmente, no âmbito descrito no ponto 5.2 deste procedimento.

O uso do direito de denúncia é opcional para os colaboradores, e a não utilização do mesmo não pode ser objeto de quaisquer consequências para os mesmos.

3. Definição de conceitos

3.1 Incidente de compliance



A centralização de incidentes através de um processo de reporte permite uma avaliação à exposição ao risco de compliance por parte do Banco Credibom SA e em consequência do Grupo CA, SA.

Um incidente de compliance é definido como uma anomalia que possa surgir durante a implementação efetiva das obrigações de acordo com as disposições específicas para as atividades bancárias e financeiras, sejam as mesmas, o produto de leis ou regulamentos, normas profissionais ou de códigos de conduta, ou emissão de instruções do órgão executivo. Esta definição aplica-se às situações envolvendo entidades externas ou apenas intervenientes internos.

De acordo com a sua categorização, o incidente pode ser ativo ou passivo:

- Ativo - quando um colaborador, de forma consciente, realiza, autoriza ou não divulga uma operação considerada como não conforme e/ou proibida.
- Passivo - quando um colaborador realiza ou autoriza uma transação desconhecendo que a mesma não se encontra em conformidade ou é proibida, de acordo com as políticas definidas (internas e externas à organização).

A gravidade da ocorrência depende:

- Das consequências financeiras ou os seus resultados em termos de sanções disciplinares, profissionais, administrativas ou regulamentares;
- Das consequências penais para o Banco, seus administradores, diretores e colaboradores;
- Do risco que representam para a imagem ou a reputação do Banco.

3.2 Irregularidades

São consideradas irregularidades, factos que violem ou comprometam gravemente:

- i. O cumprimento das leis ou regulamentos, normas profissionais ou de códigos de conduta, ou emissão de instruções do órgão executivo;
- ii. A preservação do património dos clientes e acionista;
- iii. A imagem e reputação institucional;
- iv. As situações suscetíveis de configurarem abuso de confiança ou autoridade ou má gestão.

As irregularidades não devem ser confundidas com Reclamações, as quais são objeto de regulamentação e tratamento específico, via Departamento de Experiência e Satisfação do Cliente.

Todas as irregularidades afiguram-se como incidentes, mas nem todos os incidentes serão irregularidades.

3.3 Whistleblowing



Trata-se de um canal que permite o reporte de incidentes de compliance. Este canal é suportado com recurso a dois sistemas, a saber:

- Informal
 - Suportado na gestão de contactos informais entre colaboradores do Credibom ou elementos externos ao Credibom e seus colaboradores. Por norma, não existe registo formal da comunicação do incidente.
Desta forma, qualquer participação pode ser apresentada por escrito, verbalmente ou em reunião com a maior brevidade possível, após tomada de conhecimento da irregularidade.

- Formal:
 - Suportado em ferramenta de reporte – linha de reporte.

Nestes casos existe um mecanismo de reporte dedicado para o efeito, comum ao Grupo CA CF, assegurado com recurso a um fornecedor externo, o qual é acessível de qualquer local e que garante a segurança e confidencialidade da comunicação que venha a ser realizada.
Todos os reportes realizados por esta via são apenas acessíveis pelo GCAJ, garantindo-se a confidencialidade da informação.

 - Suportado em outro mecanismo de reporte.

Nestes casos o reporte mantém-se formal, i.e. escrito (ex. e-mail, etc.), porém não são garantidos os requisitos de segurança existentes na linha de reporte, mantendo-se, no entanto, o compromisso de confidencialidade.

De referir que, independentemente da forma de comunicação, sempre que uma situação chegue ao conhecimento do GCAJ, a mesma é sempre analisada.

3.4 Banco de Portugal

Está igualmente disponível no site de Banco de Portugal, um dispositivo de reporte de incidentes através do qual é possível fazer a participação de infrações dos seguintes deveres previstos no:

- No Regime Geral das Instituições de Crédito e Sociedades Financeiras;
- No Regulamento (UE) n.º 575/2013, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento

A participação pode ser efetuada através do preenchimento do formulário web disponível em:
<https://www.bportugal.pt/webform/participar-uma-infracao>:

Mais informação disponível em: <https://www.bportugal.pt/page/participar-uma-infracao>



4. Responsabilidades

Todos os colaboradores do Banco comprometem-se, quer através do Código de Conduta quer pelas disposições ao nível do Código de Trabalho e demais legislação aplicável, a respeitar as disposições legislativas ou regulamentares que regem as atividades bancárias e financeiras, assim como todas as normas éticas e profissionais aplicáveis ao Credibom e as instruções da Comissão Executiva.

4.1 Colaboradores em geral

Compete a todos os colaboradores, numa situação em que o colaborador suspeitar ou observar a existência de um incidente de compliance, informar, presencialmente ou por escrito, o seu superior hierárquico. Sempre que essa situação não seja possível ou não recomendável deverá ser contactado o Gabinete de Compliance e Apoio Jurídico ou ser utilizado o mecanismo de reporte descrito no ponto 3.3.

Aquando do reporte deverão ser assegurados os seguintes requisitos:

- Limitar as declarações sobre os factos em questão;
- Os factos utilizados para descrever o incidente não podem violar a privacidade dos colaboradores, administradores ou diretores, e mais genericamente, a privacidade de terceiros, como por exemplo de clientes;
- A ocorrência deve ser apresentada factualmente usando a consideração e profissionalismo expectável por parte do colaborador.

4.2 Responsáveis departamentais

Compete a todos os responsáveis departamentais, independentemente da sua posição na hierarquia na organização do Credibom, assegurar o registo e análise e comunicação de todas as situações que sejam reportadas relativamente a incidentes de compliance, assegurando-se o respeito pelos seguintes princípios:

- Sempre que necessário deverá ser assegurada a análise conjuntamente com o Gabinete de Compliance e Apoio Jurídico;
- Eventual documentação associada ao incidente, quer disponibilizada pelo colaborador ou que venha a ser recolhida posteriormente aquando da análise do incidente, deverá ser encaminhada juntamente com a comunicação;
- A classificação da informação associada ao incidente reportado é da responsabilidade da função Compliance, eventualmente em coordenação com outras UOs (ex. Recursos Humanos). Este nível é definido com base na gravidade dos detalhes, o risco de sanções legais, administrativas ou disciplinares, o risco de reputação para o Banco e conseqüentemente para o Grupo Credit Agricole. Nos casos em que o incidente reportado estiver associado à má aplicabilidade de aplicação das leis e regulamentos locais ou do Grupo devem ser comunicadas à Comissão Executiva e/ou aos órgãos



sociais do Banco Credibom, assim como ao acionista, de acordo com os procedimentos em vigor.

Aquando da comunicação do incidente ao GCAJ deverá ser assegurado o reporte da seguinte informação:

- Descrição;
- Impactos;
- As suas causas e consequências, a fim de permitir decidir pela:
 - o Necessidade de investigação adicional ou intervenção da Direção de Recursos Humanos ou outra UO aplicável;
 - o Realização de medidas imediatas para evitar a ocorrência de novas situações ou manutenções dos impactos decorrentes da verificação do incidente;

Após a análise dos incidentes, e de acordo com as conclusões obtidas, é da responsabilidade dos responsáveis departamentais:

- Analisar a natureza, as causas e as consequências da transgressão em conjunto com o GCAJ e, se necessário tomar medidas imediatas para limitar os efeitos da transgressão sobre a entidade, os seus colaboradores e os seus clientes;
- Implementar ações de correção para prevenir a repetição da ocorrência dos incidentes;
- Informar o GCAJ da implementação das medidas corretivas que tenham sido definidas.

As medidas de correção devem visar:

- Adequar o nível de informação ou a formação do pessoal cuja falta ou insuficiência pode ter conduzido ao incidente em questão;
- Rever os procedimentos e processos associados às causas que originaram o incidente.

4.3 Gabinete de Compliance e Apoio Jurídico

Compete ao Gabinete de Compliance e Apoio Jurídico assegurar:

- A definição de regras e procedimentos para a gestão de incidentes de compliance, e mais concretamente para irregularidades;
- A disponibilização de ferramentas para assegurar o reporte atempado de incidentes de compliance, garantindo a confidencialidade do declarante, assim como dos incidentes reportados, em conformidade com as regras e regulamentação em vigor;
- Na sequência do ponto anterior assegurar a existência de informação e formação, quer aos colaboradores como a elementos externos ao Banco, dos mecanismos existentes para reporte de



incidentes de compliance;

- A gestão da ferramenta de suporte à linha de reporte – Whistleblowing, garantindo os requisitos de segurança e confidencialidade definidos;
- Com exceção dos eventos associados ao próprio Gabinete de Compliance e Apoio Jurídico, a análise de todos os incidentes de compliance que sejam reportados ao GCAJ, assegurando igualmente um registo centralizado dos mesmos, independentemente da forma de comunicação;
- Proceder às diligências consideradas necessárias, quer direta ou indiretamente, para garantir um cabal esclarecimento dos incidentes comunicados;
- Assegurar a realização de reportes à Comissão Executiva assim como aos órgãos sociais do Banco Credibom dos incidentes reportados, quer numa perspetiva de monitorização do dispositivo de controlo interno, assim como em respeito pelos procedimentos de alerta em vigor, incluindo os aplicáveis ao reporte ao acionista;
- Garantir a integração no mapa de riscos e controlos permanentes do Banco de medidas corretoras, de modo a evitar a ocorrência de novos incidentes. Tal poderá ser assegurado pela revisão dos processos impactados, implementação de controlos, etc.;
- Monitorizar numa base regular as deficiências identificadas e respetiva implementação do plano de ação definido, assim como assegurar o reporte regular do seu cumprimento à Comissão Executiva.

4.4 Auditoria Interna

Compete à auditoria interna, no âmbito das suas funções apoiar na realização de investigações adicionais que sejam entendidas como necessárias de modo a confirmar ou identificar situações de desconformidades decorrentes de incidentes reportados e assim garantir a existência de medidas corretivas.

Mais concretamente, compete à auditoria interna assegurar a gestão de todos os incidentes de compliance que sejam reportados como envolvendo os elementos do Gabinete de Compliance e Apoio Jurídico responsáveis pela gestão deste tipo de eventos, assegurando-se assim a independência total na gestão do processo.

Adicionalmente, aplicam-se os procedimentos definidos para o Gabinete de Compliance e Apoio Jurídico, com as devidas adaptações.

5. Comunicação de irregularidades – Linha de Reporte

5.1 Regras Gerais

A política de comunicação de irregularidades do Banco assenta nas seguintes linhas gerais:



- **Categorias de entidades sujeitos à comunicação:** todos os colaboradores de entidades do Grupo, qualquer entidade ou pessoa externa ao Grupo e ao Credibom, nomeadamente qualquer fornecedor ou subcontratado com quem o Grupo tenha estabelecido uma relação, poderão exercer o direito de denúncia.
- **Precisão da comunicação:** as comunicações deverão ser concretas e indicada a causa exata da irregularidade. Não serão consideradas alegações vagas sobre pessoas e/ou factos;
- **Confidencialidade;** é garantida absoluta confidencialidade acerca da identificação das pessoas que efetuarem a comunicação dos incidentes;
- **Não retaliação ou discriminação:** não serão tomadas quaisquer medidas contra os colaboradores ou terceiros que notifiquem comportamentos irregulares. Caso o colaborador denunciante refira que sofreu algum tipo de retaliação por ter comunicado ou participado numa investigação, deve comunicar de imediato essa suspeita ao GCAJ;
- **Utilização abusiva:** a utilização abusiva e de má-fé do mecanismo de comunicação de irregularidades poderá expor o denunciante a sanções disciplinares e a procedimento judicial, de acordo com a legislação aplicável e na medida que tal seja aplicável;
- **Medidas de Segurança:** nos termos das normas de proteção de dados e de segurança da informação, o Credibom compromete-se a implementar das medidas de segurança adequadas à proteção de informação e dos dados contidos;
- **Conservação e arquivo de conservação dos dados objeto do tratamento:** quando seja manifesta a falta de credibilidade das comunicações, os dados pessoais objeto de denúncia serão de imediato destruídos. Quando não haja lugar a procedimento disciplinar ou judicial, os dados que tenham sido objeto de comprovação serão destruídos decorrido o prazo de 6 meses a contar do encerramento de averiguações. No caso em que a denúncia tenha como consequência a instauração de procedimento disciplinar ou judicial, os dados serão conservados até ao termo desse procedimento. Neste caso, serão conservados no quadro de um sistema de informação de acesso restrito e por prazo que não exceda o procedimento judicial.
- **Segregação de funções:** eventos associados aos elementos do Gabinete de Compliance e Apoio Jurídico serão encaminhados diretamente para análise pela função de Auditoria Interna, nomeadamente a sua direção.

No anexo I é apresentada a política do Banco relativamente a esta matéria, a qual deverá ser alvo de divulgação no seio do Banco, nomeadamente através das plataformas intranet e outros meios que sejam considerados necessários.

5.2 Requisitos



Qualquer denunciante pode exercer o seu direito de alerta através dos meios aqui previstos, por exemplo:

- quando se trate de um colaborador do Banco, se considerar:
 - que o seu responsável da área não tomou medidas adequadas na sequência de uma irregularidade que lhe possa ter reportado;
 - que o seu responsável de área, outro empregado de Grupo ou um terceiro externo ao Grupo está a fazer pressão sobre si suscetível de o/a levar a cometer uma infração;
 - que reportar a irregularidade ao seu responsável de área é insuficiente ou inadequado, dadas as circunstâncias.
- Tratando-se de uma entidade externa, sempre que justificadamente considerar que o Banco ou um dos seus colaboradores cometeu uma irregularidade.

Os seguintes factos podem ser comunicados através do sistema de denúncia:

- Qualquer crime ou delito;
- Qualquer violação grave e óbvia de um compromisso internacional;
- Qualquer violação óbvia e séria de um ato unilateral de uma organização internacional, com base num compromisso internacional devidamente assinado;
- Qualquer violação séria e óbvia de uma lei ou regulamento;
- Qualquer ameaça ou risco sério ao interesse público;
- Qualquer comportamento ou situação que viole o código de conduta anticorrupção do grupo;
- Qualquer violação grave dos direitos humanos e das liberdades fundamentais, a saúde e segurança das pessoas ou do ambiente, decorrentes das atividades do grupo e das atividades dos subcontratados ou dos fornecedores com quem seja mantida uma relação comercial, cujas atividades estejam relacionadas com essa atividade.

Contudo, o denunciante não pode relatar factos, informações ou documentos abrangidos pelo segredo de Estado, sigilo médico ou bancário, bem como sigilo advogado-cliente, independentemente da sua forma.

Qualquer alerta relativo a assuntos que não os enumerados acima, pode ser comunicado através da linha de gestão hierárquica ou ao Responsável de Compliance da entidade.

As entidades do Grupo continuarão responsáveis pelo cumprimento deste procedimento, tendo em conta os regulamentos locais que se lhes possam aplicar.

5.3 Plataformas de reporte

Plataforma Web

Esta plataforma é assegurada com recurso a uma entidade externa, devidamente especializada para o efeito,



encontrando-se previsto contratualmente que a mesma garanta os requisitos de sigilo da identidade do denunciante e confidencialidade da informação.

Para todas as situações de reporte será assegurada a criação de uma caixa de correio segura que permite a visualização/acompanhamento do evento reportado pelo denunciante, nomeadamente ações desenvolvidas, pedido adicional de informações e estado atual do mesmo.

O reporte com recurso à plataforma web é realizado através do acesso a um endereço específico, nomeadamente:

<https://www.bkms-system.com/bkwebanon/report/clientInfo?cin=3CAgr18&c=pt&language=por> .

Este endereço encontra-se disponível 24 horas, 7 dias da semana e é acessível a partir de qualquer rede de internet (rede pública, rede pessoal, rede Credibom).

Encontra-se disponível formulário em língua portuguesa, podendo ser escolhidos outros idiomas.

Após o preenchimento de todos os campos o incidente será encaminhado para gestão pelo Credibom, de acordo com os requisitos definidos neste documento. A eventual não disponibilização de toda a informação poderá comprometer o registo e desenvolvimento do incidente.

De referir que não é assegurado o registo da origem da comunicação.

5.4 Tratamento de incidentes

Após a realização da comunicação dos incidentes, seja por via das plataformas de reporte, seja por via de outros meios (e-mail ou contacto pessoal) é da responsabilidade do GCAJ proceder à análise e tratamento dos mesmos.

Todas as comunicações são acedidas exclusivamente por colaboradores do Gabinete de Compliance e Apoio Jurídico. que possuem acesso à ferramenta de gestão de eventos disponibilizada pelo Grupo.

De referir que, se um dos destinatários do reporte acima discriminados for referenciado nas comunicações estas serão remetidas somente para o Gabinete de Auditoria Interna, nomeadamente para o seu responsável.

Os factos relatados pelo denunciante devem ser verificados, assegurando-se sempre que a fonte da informação permanece confidencial.

As fases associadas ao tratamento são:

- Confirmação:

O GCAJ deve promover as ações necessárias à confirmação inicial sobre a existência de fundamentos suficientes para a realização de uma investigação. Desta forma, poderá ser levado a cabo um contacto prévio com o autor da comunicação, se possível, de forma a serem melhor apuradas as informações consideradas relevantes para a confirmação inicial. O GCAJ poderá comunicar as irregularidades



participadas ao nível hierárquico superior dos visados na denúncia, caso esta transmissão não coloque em causa as finalidades do procedimento de participação e, se for caso disso, à respetiva autoridade de supervisão competente;

De referir, que este contacto será sempre realizado respeitando o mesmo formato e será realizado de forma a assegurar a confidencialidade da identidade do comunicante.

Esta confirmação inicial deve basear-se nas informações preliminares obtidas e deve ser objeto de um relatório onde se ponderem os seguintes fatores:

- a) A natureza da comunicação, determinando se recai no âmbito das “matérias cobertas”;
- b) O caráter irregular do comportamento objeto da comunicação;
- c) A exequibilidade da investigação, com destaque para os potenciais obstáculos da mesma;
- d) As pessoas que possam estar envolvidas ou tenham conhecimento de factos relevantes, que devam ser confrontadas com os dados das investigações ou que devam ser inquiridas.

A realização de investigações depende da direção do GCAJ.

- **Investigação**

Esta fase compreende a realização de diligências para comprovar, ou não, as situações relatadas assim como permitir concluir pela efetiva existência de um incidente.

Deverá ser garantida a recolha de toda a documentação que seja considerada como relevante para suportar os resultados da investigação, quer se confirme o incidente ou não.

Ao investigar um relatório, o GCAJ pode, se considerar necessário, ser apoiado por uma equipa de investigador(es) e especialista(s) identificado(s), sujeito à mais estrita confidencialidade, a funcionar em modo “gabinete de crise, fornecendo especialização funcional transversal, a fim de apreciar a admissibilidade e gerir o alerta feito pelo whistleblower e permitir decisões coletivas a respeito das ações de acompanhamento a serem tomadas.

O GCAJ trata o alerta num prazo razoável (definido em 2 meses no Grupo) e comunica regularmente com o whistleblower para o manter informado do seguimento do seu alerta: confirmação de receção, decisão sobre a admissibilidade, tratamento e encerramento do alerta.

- **Decisão**

Como consequência da investigação e da apreciação e avaliação final dos respetivos resultados, o GCAJ proporá o arquivamento, a adoção ou a promoção de medidas adequadas para mitigar a situação identificada e/ou evitar a ocorrência de situações similares no futuro.

Todas as situações de investigação deverão ser aprovadas pela direção do GCAJ.



6. Confidencialidade e proteção do denunciante

6.1 Confidencialidade

O exercício de um direito de alerta ocorre em circunstâncias que o whistleblower considerará excepcionais. Elas exigem um ambiente de estrita confidencialidade que lhe permita relatar os factos e ao mesmo tempo proteger a sua identidade. Portanto, o Referente trata os alertas na mais estrita confidencialidade e só partilha a informação comunicada com terceiros cujo envolvimento seja absolutamente essencial para tratar o alerta. Tal inclui uma equipa de investigador(es) ou perito(s) identificado(s), também sujeitos a estrita confidencialidade. Em qualquer caso, a identidade do whistleblower e da(s) pessoa(s) envolvida(s) no alerta, bem como toda a informação recolhida pelos recetores do alerta são tratadas de modo confidencial.

Em geral, a verificação dos factos relatados por um whistleblower no exercício do seu direito de alerta de irregularidades é realizada de forma a que a fonte da informação permaneça confidencial, e que sejam tomadas todas as medidas para evitar colocar o whistleblower numa posição incómoda. A estrita confidencialidade da identidade do whistleblower, dos factos alegados e das pessoas abrangidas pelo alerta terá que ficar garantida.

Este direito de alerta descrito no presente procedimento foi concebido para garantir a segurança e confidencialidade de todas as informações fornecidas pelos whistleblowers.

Informação que permita identificar o whistleblower não pode ser divulgada, exceto à autoridade judicial e só com o seu consentimento.

Informação que permita identificar a(s) pessoa(s) envolvida(a) num alerta não pode ser divulgada, exceto à autoridade judicial e comprovados os motivos do alerta.

6.2 Proteção do whistleblower

A proteção do whistleblower é garantida, desde que:

- relate, desinteressadamente e de boa-fé, um facto de que tenha conhecimento pessoal;
- a divulgação seja “necessária e proporcional para salvaguardar os interesses em causa” e seja feita em conformidade com os procedimentos de denúncia definidos acima mencionados, ou outra legislação aplicável.

Se estes critérios forem cumpridos, o whistleblower não é criminalmente responsável por ter revelado factos, mesmo que sujeitos a sigilo bancário. Além disso, o whistleblower não pode ser objeto de demissão, sanção ou qualquer tipo de discriminação, direta ou indireta, especialmente a respeito do seu salário ou desenvolvimento de carreira.



Contudo, se o whistleblower tiver violado deliberadamente leis e regulamentos ou ocultado factos que deveriam ter sido comunicados nos termos da lei e/ou se não tiver feito a sua denúncia desinteressadamente e de boa-fé, sujeita-se a processo cível e/ou criminal e medidas disciplinares.

Além disso, qualquer pressão sobre um whistleblower para obstruir o reporte de um alerta constitui uma infração punível com sanções disciplinares e criminais.

6.3 Informação sobre a(s) pessoa(s) envolvida(s) no alerta

Qualquer pessoa objeto de alerta é presumida inocente até que as alegações sejam investigadas e os factos verificados.

O GCAJ notifica a pessoa objeto do alerta das alegações contra si, para que tenha a oportunidade de fazer ouvir a sua posição. Pode, no entanto, decidir tomar medidas cautelares, sobretudo para evitar a destruição de provas, antes de notificar a pessoa objeto do alerta.

Todas as medidas necessárias para garantir a confidencialidade da identidade da pessoa objeto do alerta são aplicadas.

6.4 Proteção e preservação de dados

Qualquer pessoa identificada no alerta tem o direito, a qualquer momento, nos termos da regulamentação aplicável, de ter acesso aos seus dados pessoais, a opor-se por motivos legítimos ao seu tratamento, a vê-los corrigidos, a solicitar a sua eliminação, a limitar o seu tratamento ou a dar instruções sobre o procedimento aplicável aos seus dados pessoais em caso de morte da pessoa identificada.

Em Portugal, qualquer pessoa identificada pode apresentar queixa à CNPD, cujos dados de contacto se encontram no endereço Internet: www.cnpd.pt.

Todas as informações e/ou documentos obtidos no âmbito de um alerta e durante todas as operações realizadas relativas à admissibilidade e processamento do alerta devem ser arquivados em estrita conformidade com a regulamentação relativa à proteção de dados pessoais.

Assim que o GCAJ receber um alerta, os dados relativos a esse alerta que não caibam no âmbito do direito de alerta serão destruídos ou arquivados depois de serem anonimizados, sem demora.

Quando o alerta não for seguido de um procedimento disciplinar ou judicial, os dados relativos a esse alerta serão destruídos ou anonimizados e arquivados pelo Grupo num prazo de 12 meses após o encerramento da investigação.

Quando processos disciplinares ou jurídicos forem instaurados contra a(s) pessoa(s) envolvida(s) no alerta, ou contra o autor de um alerta abusivo, os dados do alerta são mantidos pelo Grupo até ao encerramento do processo.



Em qualquer caso, os dados arquivados serão mantidos num sistema de informação dedicado e separado com acesso restrito, por um período que não exceda a duração dos processos judiciais.

6.5 Denúncias anónimas

O denunciante poderá optar por fazer o alerta sem se identificar, ou seja, através de uma denúncia anónima. Uma denúncia neste formato, sem prejuízo de quanto à mesma se exercerem todos os passos e meios de investigação, poderá dificultar o seu tratamento por não se poderem obter declarações adicionais, se necessárias, da parte do denunciante, o que poderá levar ao arquivamento da investigação.

7. Relatórios e Controlo

O GCAJ informará regularmente o seu órgão de administração assim como a sua compliance Business Line do Grupo e fornecerá uma análise quantitativa e qualitativa dos alertas recebidos.

7.1 Reporte

Deverá ser assegurado o reporte à Comissão Executiva do Credibom e ao Conselho de Administração ou outro similar, todos os incidentes reportados enquadráveis no âmbito deste documento, garantindo-se a apresentação

dos resultados decorrentes das investigações realizadas e estado das medidas corretivas (follow-up). Neste reporte a identificação dos denunciante será sempre mantida confidencial.

Desde já se define os seguintes requisitos de reporte:

- a) Número identificativo da comunicação
- b) Data de receção
- c) Modo de transmissão
- d) Classificação da Comunicação (nível de prioridade)
- e) Descrição da natureza da comunicação
- f) Medidas tomadas em virtude da comunicação
- g) Estado atual do processo (pendente ou encerrado)
- h) Responsável pela análise (Unidade Orgânica e colaborador)



8. Matriz RACI

Actividades/Processos	GCAJ	CA	CACF	GRCP	AI
Receção das Denúncias	R		I		
Averiguação das Denúncias	R		I		
Decisão das Denúncias	R	I	I	I	I

Legenda:

R esponsável pela execução;

A utoridade, quem deve responder, o aprovador;

C onsultado, quem deve ser consultado e participar da decisão ou atividade;

I nformado, quem deve receber a informação de que uma atividade foi executada.

9. Regra especial relativa a dados pessoais e tratamento de dados pessoais

Em resultado das obrigações e regras previstas no Regulamento Geral de Proteção de Dados (Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016), o “RGPD” ou “GDPR”, qualquer tratamento de dados pessoais terá que respeitar as referidas regras. Da mesma forma, todos os documentos do corpo normativo devem respeitar os princípios subjacente a esta regulamentação. Assim, qualquer regra ou operação relativa a tratamento de dados pessoais que possa estar incluída no texto da presente CPS ou na GPS que lhe esteja associada, se aplicável, que seja contraditória aos requisitos do GDPR é desde já considerada como nula, devendo para o efeito ser consultada a GPS 533, prevalecendo sempre as orientações dessa GPS 533 para todos os tratamentos de dados pessoais.

Para esclarecimento, é entendido ao abrigo do GDPR como:

1) Dados Pessoais, qualquer informação relativa a uma pessoa singular identificada ou identificável, sendo considerada identificável uma pessoa que possa ser identificada, direta ou indiretamente, como por exemplo através do nome, de um número de identificação, dos dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

2) Tratamento de Dados, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a eliminação ou a destruição.



10. - Anexo 1 – Política de Comunicação de Irregularidades no Banco Credibom S.A.

10.1 Objeto

É atribuída ao Gabinete de Compliance e Apoio Jurídico a competência para a receção das comunicações de irregularidades ocorridas no seio do Banco, bem como a implementação da política de gestão de irregularidades.

10.2 Definição

São consideradas irregularidades, factos que violem ou comprometam gravemente:

- O cumprimento das leis ou regulamentos, normas profissionais ou de códigos de conduta, ou emissão de instruções do órgão executivo;
- A preservação do património dos clientes e acionista;
- A imagem e reputação institucional;
- As situações suscetíveis de configurarem abuso de autoridade ou má gestão.

10.3 Entidades aplicáveis

Este Regulamento aplica-se a todos os colaboradores de entidades do Grupo, qualquer entidade ou pessoa externa ao Grupo e ao Credibom, nomeadamente qualquer fornecedor ou subcontratado com quem o Grupo tenha estabelecido uma relação.

10.4 Comunicação de Irregularidades e Contactos

O Banco mantém um sistema de comunicação de irregularidades, publicitado no seu sítio da intranet e site da internet sob a supervisão do Gabinete de Compliance e Apoio Jurídico. O referido sistema inclui as seguintes formas de comunicação:

- Formulário web acessível em
- <https://www.bkms-system.com/bkwebanon/report/clientInfo?cin=3CAgr18&c=pt&language=por>
- Endereço de e-mail: **fraude@credibom.pt**
- Formulário web do Banco de Portugal acessível em: <https://www.bportugal.pt/webform/participar-uma-infracao>
- Morada Postal:

Banco Credibom S.A.



A/C Gabinete de Compliance e Apoio Jurídico – Área de Compliance (Confidencial)
Lagoas Park
Edifício 14, Piso 2
2740-262 Porto Salvo

- Contacto Pessoal, por intermédio de um dos elementos previstos no Anexo a este documento.

A comunicação deve descrever o motivo do reporte e indicar a causa da pretensa irregularidade, não sendo consideradas alegações vagas sobre factos ou sobre pessoas.

10.5 Outros modos de receção de comunicações

Não serão aceites comunicações de irregularidades rececionadas por outras formas de origem diferente das contempladas no número anterior.

10.6 Acesso à Informação e Documentação

O acesso à informação e documentos associados ao sistema de comunicação de irregularidades está previsto internamente e limitado ao pessoal autorizado, o qual é revisto de forma regular de acordo com a organização em vigor no Banco.

10.7 Competências

O responsável pela Área de Compliance deverá fazer acompanhamento das comunicações de irregularidades. A cada comunicação deve ser atribuído um número de registo, devendo a mesma ser incluída na base de dados de registo de comunicação de irregularidades.

10.8 Reporte a entidades oficiais

Após análise da irregularidade poderá ser determinado o conhecimento da mesma às autoridades policiais ou judiciais, sem prejuízo de que seja dada a competente sequência interna a tais comunicações.