Critical Software

PROGRAMA DE CUMPRIMENTO NORMATIVO

DATA: 2023-04-04
ESTADO: APPROVED
PÁGINAS: 49
CLASSIFICAÇÃO DA INFORMAÇÃO: CONFIDENCIAL
VERSÃO: 1

© 2023 Copyright Critical Software S.A. All Rights Reserved.

APROVAÇÃO

VERSÃO	NOME	FUNÇÃO	DATA
V1		CA	2023-04-04

AUTORES E CONTRIBUIÇÕES

NOME	DESCRIÇÃO	DATA
Sónia Frias Marques		2023-02-28

COPYRIGHT

O conteúdo deste documento está protegido por direitos autorais da Critical Software S.A., liberalizado na condição de não ser copiado no seu todo, em parte ou de outra forma (seja por fotografia ou qualquer outro método) e, portanto, não deve ser divulgado a qualquer outra pessoa que não o destinatário (exceto para outros escritórios autorizados da organização que tenham a necessidade de conhecer tais conteúdos, com a finalidade para a qual a divulgação é feita) sem o consentimento prévio por escrito do Responsável pelo Cumprimento Normativo da CSW.

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

ÍNDICE

1. INTRODUÇÃO 4
1.1. Introdução e Objetivos 4
1.2. Normas de Atualização e Disponibilização 4
1.2.1. Processo de Revisão e Atualização 4
1.2.2. Disponibilização da Informação 5
1.3. Responsabilidades 5
1.3.1. Responsabilidades do Conselho de Administração 5
1.3.2. Responsabilidades do Responsável pelo Cumprimento Normativo 6
1.3.3. Responsabilidades dos Colaboradores 6
1.4. Enquadramento Legal 6
2. PLANO DE GESTÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS 7
2.1. Estratégia de prevenção DA CORRUPÇÃO E INFRAÇÕES CONEXAS 7
2.2. Estrutura interna 7
2.3. Avaliação do Risco 8
2.3.1. Avaliação Global do Risco 8
2.3.2. Avaliação de Risco 8
2.3.3. Avaliação Prévia de Risco 8
2.4. CLASSIFICAÇÃO DOS RISCOS 9
2.5. Avaliação de eficácia do Sistema de Prevenção de CORRUPÇÃO E INFRAÇÕES CONEXAS 10
3. CÓDIGO DE CONDUTA E CANAIS DE DENÚNCIA 10
3.1. CÓDIGO DE CONDUTA 10
3.2. CANAL DE DENÚNCIA 11
4. POLÍTICA DE FORMAÇÃO DE PREVENÇÃO DA CORRUPÇÃO E INFRAÇÕES CONEXAS 12
ANEXO 1- MATRIZ DE RISCO 13
ANEXO 2 – FICHA DE IDENTIFICAÇÃO DE PESSOA COLECTIVA 13
ANEXO 3 – CÓDIGO DE CONDUTA CRITICAL 13
ANEXO 4 – REGULAMENTO CANAL DENÚNCIA 13

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

1. INTRODUÇÃO

1.1. INTRODUÇÃO E OBJETIVOS

As medidas de natureza preventiva e repressiva de combate à corrupção e infrações conexas regem-se pelo Decreto-Lei n.º 109-E/2021, de 9 de dezembro, adiante designado por RGPC, o qual é aplicável às pessoas coletivas com sede em Portugal que empregue 50 ou mais trabalhadores, nos termos do artigo 2.º, n.º 1 do referido regime. Estando a Critical Software, S.A. abrangida pelo âmbito de aplicação, encontra-se por isso sujeita aos deveres previstos por este quadro legal.

O presente Plano de Cumprimento Normativo (PCN) visa dar cumprimento ao quadro legal existente em matéria de prevenção e combate à corrupção e infrações conexas, propondo-se atingir os seguintes objetivos:

- Formalizar e assegurar o integral cumprimento dos procedimentos relacionados com a prevenção, deteção e repressão da corrupção e infrações conexas;
- Enquadrar a execução das atividades desenvolvidas no âmbito da Prevenção da Corrupção e Infrações Conexas;
- Definir a matriz de risco com identificação, análise e classificação dos riscos enquadráveis no âmbito da corrupção e infrações conexas;
- Realizar formação interna, com vista ao conhecimento e compreensão das políticas e procedimentos de prevenção da corrupção e infrações conexas implementados.

1.2. NORMAS DE ATUALIZAÇÃO E DISPONIBILIZAÇÃO

1.2.1. Processo de Revisão e Atualização

O presente Manual será revisto e atualizado em função da evolução legislativa e do mercado em que a Critical opera, dos riscos existentes ou identificados, dos seus objetivos e da sua estrutura organizacional, em concordância com as diretrizes gerais do Responsável pelo Cumprimento do Normativo (RCN), posteriormente aprovadas, em sede de reunião, pelo Conselho de Administração.

Nesse sentido, os Colaboradores da Critical devem efetuar um acompanhamento permanente das normas aplicáveis, bem como uma revisão dos circuitos de informação e procedimentos instituídos, por forma a melhorar a sua eficiência e eficácia. Os Colaboradores podem, ainda, comunicar ao RCN propostas de alterações que considerem necessárias, para que, eventualmente, se proceda à correspondente atualização no Manual.

A periodicidade da avaliação da atualidade e adequação das políticas e dos procedimentos e controlos é efetuada duas vezes ao ano (em Abril e Outubro) devendo ser elaborado um relatório em cada uma das fases de avaliação.

A avaliação dos procedimentos e controlos existente em matéria de RGPC têm em conta os seguintes fatores:

- Adequação das políticas e dos procedimentos e controlos face às atividades desenvolvidas no período decorrido desde a última avaliação;
- Eventuais alterações do modelo de negócio;
- Eventuais alterações nos riscos derivados das circunstâncias envolventes externas da atividade;
- Eventuais recomendações emitidas por organismos nacionais ou internacionais com tutela na área da prevenção e combate à corrupção e infrações conexas;
- Resultados de avaliações intercalares.

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

A atualização do PCN deverá ser realizada de acordo com os seguintes princípios:

- Qualquer atualização, dos procedimentos e de outros aspetos contidos no PCN, deve ser efetuada sob a orientação do RCN. A emissão da aprovação final de todas as alterações e revisões do PCN, é da responsabilidade do Conselho de Administração da Critical;
- Após emissão de aprovação de uma alteração ao PCN, deve ser emitida uma comunicação interna, a ser distribuída a todos os Colaboradores da Critical, fazendo referência aos procedimentos alterados;
- O RCN deverá promover a atualização do PCN em suporte informático;
- A cópia em formato eletrónico deste PCN, e suas respetivas atualizações, estará arquivada e disponível em rede interna de acesso comum aos Colaboradores e Conselho de Administração da Critical, promovendo a comunicação formal e transparente da atividade em causa;
- Sempre que se efetue uma atualização ao presente PCN, todos os campos apresentados em pé de página devem ser preenchidos;
- Deverá ser mantido um registo de todas as alterações realizadas, mantendo em arquivo informático as versões obsoletas devidamente identificadas como tal;
- A lista de revisões e edições, apresentada na página 2 do presente Manual, deverá ser atualizada sempre que ocorram alterações.

1.2.2. Disponibilização da Informação

O Programa de Cumprimento Normativo estará disponível em suporte informático, através da rede informática interna da Critical, encontrando-se disponível para consulta a todos os Colaboradores e Conselho de Administração.

O RCN terá acesso ao suporte informático em formato editável, para efeitos de realização de alterações ao PCN.

1.3. RESPONSABILIDADES

1.3.1. Responsabilidades do Conselho de Administração

Em matéria de Prevenção da Corrupção e Infrações Conexas, compete ao Conselho de Administração, assegurar a aplicação das políticas, procedimentos e controlos. Especificamente, o Conselho de Administração possui a incumbência de:

- Aprovar e atualizar as políticas e os procedimentos e controlos em matéria de prevenção da corrupção e infrações conexas;
- Dispor de conhecimento adequado dos riscos de corrupção e infrações conexas a que a Critical se encontra exposta, bem como dos processos utilizados para identificar, avaliar, acompanhar e controlar esses riscos;
- Garantir que a estrutura organizacional da Critical e os meios disponibilizados permitem a adequada execução das políticas e dos procedimentos e controlos em matéria de prevenção da corrupção e infrações conexas, prevenindo conflitos de interesses e, sempre que necessário, promovendo a separação de funções;
- Promover uma cultura de prevenção da corrupção e infrações conexas que abranja todos os colaboradores da Critical cujas funções sejam relevantes para efeitos da prevenção da corrupção e infrações conexas, sustentada em elevados padrões de ética e de integridade;
- Designar o responsável pelo controlo do cumprimento do quadro normativo em matéria de prevenção da corrupção e infrações conexas;
- Acompanhar a atividade dos demais membros da direção de topo, na medida em que estes tutelem áreas de negócio que estejam ou possam vir a estar expostas a riscos de corrupção e infrações conexas;

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

- Acompanhar e avaliar periodicamente a eficácia das políticas e dos procedimentos e controlos em matéria de prevenção da corrupção e infrações conexas, assegurando a execução das medidas adequadas à correção das deficiências detetadas nos mesmos.

1.3.2. Responsabilidades do Responsável pelo Cumprimento Normativo

O responsável nomeado pelo Conselho de Administração para garantir o cumprimento integral do cumprimento do quadro normativo em matéria de prevenção da corrupção e infrações conexas, possui as seguintes competências:

- Participar na definição das políticas e procedimentos e controlos destinados à prevenção da corrupção e infrações conexas;
- Acompanhar, permanentemente, a adequação, suficiência e atualidade das políticas e procedimentos e controlos destinados à prevenção da corrupção e infrações conexas, sempre que necessário, as devidas atualizações tendo em consideração eventuais alterações do modelo de negócio, alterações de riscos, recomendações emitidas por organismos nacionais ou internacionais e os resultados de avaliação de eficácia;
- Coordenar a revisão e atualização do Programa de Cumprimento Normativo;
- Monitorizar o cumprimento do quadro normativo aplicável em matéria prevenção da corrupção e infrações conexas;
- Participar na definição, acompanhamento e avaliação da política de formação interna da Critical, identificando as necessidades de formação no âmbito da prevenção da corrupção e infrações conexas;
- Desempenhar o papel de interlocutor das Autoridades Judiciárias, Policiais e de Supervisão e Fiscalização;
- Proceder à comunicação às autoridades competentes em matéria da avaliação dos procedimentos de controlo interno referentes à prevenção da corrupção e infrações conexas, sem depender de autorização ou decisão de qualquer órgão de administração ou intervenção de terceiros;
- Elaborar e apresentar ao Conselho de Administração o reporte intercalar e anual sobre corrupção e infrações conexas;
- Conservar o arquivo de documentação no âmbito da prevenção da corrupção e infrações conexas.

1.3.3. Responsabilidades dos Colaboradores

É da responsabilidade de todos os colaboradores o acompanhamento permanente do presente PCN, com vista à sua execução. Quando aplicável, os Colaboradores podem apresentar propostas de alteração do mesmo.

O incumprimento das regras e procedimentos internos mencionados no presente PCN, sempre que corresponda a uma infração disciplinar, poderá dar origem a um processo disciplinar.

1.4. ENQUADRAMENTO LEGAL

O presente Manual encontra-se alinhado com os seguintes instrumentos legais e regulamentares:

- Decreto-Lei n.º 109-E/2021de 9 de dezembro;
- Lei n.º 59/2007, de 4 de setembro, Código Penal;

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

2. PLANO DE GESTÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

2.1. ESTRATÉGIA DE PREVENÇÃO DA CORRUPÇÃO E INFRAÇÕES CONEXAS

Por forma a reduzir o risco de que a sua atividade possa ser o veículo para a prática de crimes de corrupção e infrações conexas, a Critical encontra-se inteiramente comprometida na aplicação de procedimentos rigorosos, no contexto da prevenção da corrupção e infrações conexas, sendo, estes, parte integrante do seu Sistema de Controlo Interno.

Para esse efeito, a Critical definiu e implementou uma estratégia de prevenção em matéria de corrupção e infrações conexas que pretende dotar a sua organização de procedimentos, formação e meios adequados, procurando reduzir o risco de exposição a possíveis intenções de corrupção e infrações conexas no âmbito da sua atividade e transações comerciais estabelecidas com os seus diversos *stakeholders*, nomeadamente:

- Dispor de Plano de Gestão de Riscos em matéria de corrupção e infrações conexas, devidamente aprovado;
- Prover a formação adequada e contínua aos seus Colaboradores, por forma a incutir uma cultura de gestão de risco no que se refere a matérias de corrupção e infrações conexas.

Os procedimentos definidos e implementados pela Critical são continuamente monitorizados sendo o PPR revisto a cada três anos ou sempre que se opere uma alteração nas atribuições ou na estrutura orgânica ou societária da entidade que justifique a revisão dos elementos constantes do PPR ou em função das recomendações e orientações das organizações internacionais, da evolução legislativa e regulamentar e do acompanhamento efetuado no âmbito das funções diretamente relacionadas com as matérias de corrupção e infrações conexas.

No âmbito da política de prevenção de corrupção e infrações conexas da Critical, todas as operações são alvo de procedimentos de identificação e diligência. No entanto, para operações classificadas como risco elevado e médio, são definidas e documentadas um conjunto de medidas de diligência reforçada. As referidas medidas encontram-se refletidas nos procedimentos de prevenção de corrupção e infrações conexas, das quais se destacam as seguintes:

- Identificação dos riscos relacionados com a corrupção e infrações conexas aplicáveis ao negócio bem como a probabilidade da sua ocorrência;
- Realização de diligências para mitigação de riscos;
- Monitorização do acompanhamento da relação de negócio pelo responsável pelo cumprimento normativo;

2.2. ESTRUTURA INTERNA

De forma a garantir a eficácia da sua atuação no âmbito das matérias de prevenção de corrupção e infrações conexas, a Critical estabelece uma estrutura interna orientada pelos seguintes princípios:

- Dispor de recursos providos de formação adequada para o desempenho das suas funções;
- Dispor de procedimentos documentados e assentes numa lógica de segregação de funções no que diz respeito à análise, tratamento e validação das operações;
- Manter um registo informático centralizado e devidamente controlado no que aos acessos diz respeito, com todas as ações desenvolvidas no âmbito da prevenção de corrupção e infrações conexas, sob a competência do RCN;
- Manter um arquivo específico, segregado e devidamente controlado no que aos acessos diz respeito, sob a competência do RCN.

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

2.3. AVALIAÇÃO DO RISCO

2.3.1. Avaliação Global do Risco

Anualmente, a Critical procede à realização da avaliação global de riscos, tendo em conta as circunstâncias em que opera nesse momento, permitindo, consequentemente, a execução do ajuste da identificação e avaliação dos riscos. A avaliação global de riscos desenvolvida tem por base os seguintes fatores de risco:

- A natureza, complexidade e dimensão das suas atividades;
- As tipologias dos clientes, fornecedores e parceiros, atuais e potenciais;
- As áreas de negócio desenvolvidas e produtos/serviços disponibilizados;
- Os canais de distribuição e meios de comunicação utilizados;
- Os países e territórios onde os seus clientes, fornecedores e parceiros (atuais e potenciais) atuam, residem ou desenvolvem as suas atividades através de terceiros;
- As informações e riscos identificados pelas Autoridades Setoriais bem como das Autoridades Nacionais e Europeias de Supervisão e Fiscalização sobre os riscos de corrupção e infrações conexas.

2.3.2. Avaliação de Risco

A Critical efetua a avaliação do risco de cada uma das áreas de atuação da organização tendo adotado uma metodologia de classificação dos riscos com base num conjunto de indicadores relacionados com as atividade/operações, finalidade, regularidade e duração das relações de negócio e/ou colaboração.

A referida avaliação do perfil de risco de corrupção e infrações conexas realizada pela Critical encontra-se em documento próprio – Anexo 1 – Matriz de Risco. O referido documento detalha o conjunto de riscos em cada uma das áreas de negócio e áreas de suporte da Critical.

Foram avaliadas todas as áreas da Critical, tanto as áreas de negócio como as áreas de suporte que, pela sua natureza intrínseca, podemos identificar algumas situações que podem consubstanciar riscos de gestão, de fraude e de corrupção.

Cumpre realçar que o critério adotado na identificação das áreas assentou unicamente na circunstância das mesmas comportarem, em abstrato, a potencialidade da verificação de situações de risco e não na deteção, passada ou presente, de casos suscetíveis de serem qualificados como casos de desvios indesejáveis às regras aplicáveis.

Cada área específica foi objeto de uma apreciação conjunta, na qual foram identificadas

situações de risco, bem como as medidas de mitigação da probabilidade da sua ocorrência.

No âmbito da identificação de riscos de corrupção e infrações conexas pode ser suscitada a necessidade de integrar ou reclassificar estes indicadores. Caso tal se verifique o RCN deverá proceder à atualização do Anexo 1 – Matriz de Risco, submetendo-o à aprovação do Conselho de Administração.

Todos os perfis de Risco Médio e Elevado são alvo de Exame pelo Responsável pelo Cumprimento do quadro Normativo em matéria de prevenção da corrupção e infrações conexas.

2.3.3. Avaliação Prévia de Risco

A Critical procede, nos termos do artigo 18.º do RGPC, a uma avaliação prévia do perfil de risco relativamente a terceiros que ajam em seu nome, fornecedores e clientes.

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

Neste processo de avaliação a Critical adota uma metodologia de classificação dos clientes, fornecedores e terceiros que ajam em seu nome com base na identificação dos Beneficiários Efetivos com vista à identificação de possíveis conflitos de interesses.

A referida avaliação do perfil de risco de corrupção e infrações conexas realizada pela Critical, é formalizada em documento próprio – Anexo 2 – Ficha de Identificação de Pessoa Colectiva.

Todos os perfis de Risco Médio e Elevado são alvo de Exame pelo Responsável pelo Cumprimento do quadro Normativo em matéria de prevenção da corrupção e infrações conexas

2.4. CLASSIFICAÇÃO DOS RISCOS

Os riscos foram classificados segundo uma escala: elevado, moderado e fraco, em função do grau de probabilidade de ocorrência e da gravidade/impacto das suas consequências.

Probabilidade de ocorrência:

Baixa: Possibilidade de ocorrência, mas com hipótese de obviar o evento com o controlo existente para o tratar

Média: Possibilidade de ocorrência, mas com hipóteses de obviar o evento através de decisões e ações adicionais

Alta: Forte possibilidade de ocorrência e escassez de hipóteses de obviar o evento mesmo com decisões e ações adicionais essenciais

Impacto previsível:

Baixo: Afetação da otimização do desempenho ou das atividades operacionais, requerendo revisão de procedimentos ou de calendarizações.

Médio: Impacto moderado na imagem institucional ou sobre o desempenho

Alto: Prejuízo na imagem e reputação institucional, ou impacto significativo sobre a estratégia, o desempenho e atividades operacionais.

Do cruzamento das variáveis probabilidade e impacto resulta a seguinte matriz de risco, que é aplicada a cada um dos riscos potenciais identificados para a organização.

MATRIZ DE RISCO		IMPACTO		
		Baixo	Médio	Alto
PROBABILIDADE	BAIXO	FRACO	FRACO	MODERADO
	MÉDIO	FRACO	MODERADO	ELEVADO
	ALTO	MODERADO	ELEVADO	ELEVADO

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

2.5. AVALIAÇÃO DE EFICÁCIA DO SISTEMA DE PREVENÇÃO DE CORRUPÇÃO E INFRAÇÕES CONEXAS

A avaliação de eficácia do sistema de Prevenção de Corrupção e Infrações Conexas é assegurada duas vezes por ano, com base no acompanhamento regular das operações no âmbito das responsabilidades do RCN, e nos relatórios do intercalar e anual a elaborar pelo RCN, de acordo com as disposições normativas no mês de Abril e Outubro de cada ano.

A adequação e suficiência dos meios e procedimentos de controlo destinados à mitigação dos riscos identificados e avaliados também são monitorizados pela Critical e devidamente avaliados quanto à sua eficácia.

Deste modo, a Critical verifica com a periodicidade a que está legalmente obrigada, se os mecanismos de prevenção contra a corrupção e infrações conexas estão a ser aplicados eficazmente.

Os resultados das avaliações são reduzidos a escrito, sendo publicados na intranet e na página oficial na Internet da Critical, conforme artigo 6.º n.º 6 do RGPC.

3. CÓDIGO DE CONDUTA E CANAIS DE DENÚNCIA

Para além dos procedimentos previstos no capítulo 2. Plano de Prevenção de Riscos de Corrupção e Infrações Conexas, a Critical tem em vigor o Código de Conduta da Critical e o Regulamento de Comunicação de Infrações, ambos disponíveis em www.criticalsoftware.com e que são parte integrante do Plano de Cumprimento Normativo.

3.1. CÓDIGO DE CONDUTA

A Critical tem em vigor um Código de Conduta, o qual se encontra em documento próprio – Anexo 3.

A Critical repudia qualquer prática de corrupção, suborno ou infração conexa, de forma ativa ou passiva, e outras formas de influência indevida ou condutas ilícitas, impondo o cumprimento rigoroso desses princípios em todas as suas relações internas e externas, seja com entidades privadas ou entidades públicas.

Todos(as) os(as) colaboradores(as) devem cumprir as normas aplicáveis, nacionais e internacionais, de combate à corrupção e infrações Conexas, sendo expressamente proibidos todos e quaisquer comportamentos que possam consubstanciar a prática do crime de corrupção ou de qualquer infração conexa previstos na lei.

Em particular, é expressamente proibido a todos(as) os(as) colaboradores(as):

a. aceitar quaisquer vantagens ou ofertas como contrapartida do tratamento preferencial de qualquer terceiro, para influenciar uma ação ou decisão;

b. oferecer ou aceitar, em qualquer circunstância e independentemente do valor, dinheiro, cheques e outros bens sujeitos a restrições legais;

c. influenciar as decisões dos parceiros de negócio por qualquer forma ilegal ou que pareça contrariar as normas aplicáveis;

d. obter algum benefício ou vantagem para a empresa, para o(a) colaborador(a) ou para terceiros, através de práticas pouco éticas ou contrárias aos deveres do cargo, nomeadamente através de práticas de corrupção, recebimento indevido de vantagem ou tráfico de influências.

No exercício da atividade da Critical, podem ser frequentes as interações com funcionários públicos, administrativos, agentes governamentais e demais organismos públicos, devendo tais interações ser pautadas pela maior retidão, transparência bem como pelo estrito cumprimento de todas as normas legais e deveres deontológicos aplicáveis, e das disposições do presente PCN.

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

Para efeitos do presente PCN, no que aos brindes e ofertas comerciais respeita, apenas poderão ser realizadas ofertas que se enquadrem nas condutas socialmente adequadas e conformes aos usos e costumes em estrito cumprimento do Código de Conduta. Um benefício é considerado socialmente aceitável se for oferecido como sinal de educação e boas maneiras, conforme os usos e costumes locais, na medida em que esse benefício esteja relacionado com a atividade profissional e não tenha intenção ou propósito de persuadir ou obter um tratamento preferencial ou vantagem ilegítima do destinatário ou de influenciar indevidamente o seu comportamento.

Com o objetivo de assegurar que os terceiros contratados pela Critical respeitam o presente PCN e a legislação existente em matéria de prevenção de corrupção e infrações conexas, a Critical define um conjunto de princípios e regras que, sem prejuízo da aplicação das normas legais ou de quaisquer outras normas internas aplicáveis, devem ser observados nos processos de contratação.

Para os devidos efeitos, devem ser observados, nomeadamente, os seguintes princípios:

a. A contratação de terceiros pressupõe uma necessidade legítima dos bens ou serviços a adquirir;

b. A escolha dos potenciais fornecedores assenta em critérios objetivos, claros e imparciais, e divulgados de forma transparente;

c. a escolha dos potenciais fornecedores é precedida de uma análise sobre o nível de exposição ao risco de corrupção;

d. as condições aceites pela Critical (incluindo preço e condições de pagamento) estão em linha com as práticas de mercado;

e. os terceiros contratados aceitam o Código e Conduta da Critical.

O incumprimento das regras constantes no PCN ou no Código de Conduta por qualquer colaborador(a) será considerado uma infração grave, a qual, dependendo do grau de culpa do infrator e da gravidade da infração, poderá dar lugar à aplicação das seguintes sanções disciplinares, as quais podem ser aplicadas, com ou sem divulgação no âmbito da empresa:

a. Repreensão não registada;

b. Repreensão registada;

c. Sanção pecuniária;

d. Perda de dias de férias;

e. Suspensão do trabalho com perda de retribuição e de antiguidade;

f. Despedimento com justa causa.

3.2. CANAL DE DENÚNCIA

A Critical dispõe de um canal de denúncia Interna cujo regulamento se encontra em documento próprio – Anexo 4 - e dá seguimento a denúncias de atos de corrupção e infrações conexas, nos termos do disposto na legislação que transpõe a Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União.

A receção e o reencaminhamento de denúncias seguem o procedimento aplicável às denúncias estabelecido no Regulamento de Comunicação de Infrações, disponível em www.criticalsoftware.com

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

4. POLÍTICA DE FORMAÇÃO DE PREVENÇÃO DA CORRUPÇÃO E INFRAÇÕES CONEXAS

A Critical assegura, nos termos do artigo 9.º do RGPC, a realização de um programa de formação interna periódica sobre o conteúdo do presente PCN, a todos os colaboradores, com vista ao conhecimento e compreensão de todas as normas e procedimentos no âmbito da prevenção da corrupção e infrações conexas.

A formação deve ser adaptada às funções desempenhadas pelos colaboradores em causa, tendo em conta os diversos graus de exposição aos riscos identificados. As necessidades de formação, neste âmbito, são analisadas e aferidas pelo RCN, com base no perfil de competências do colaborador e na avaliação do exercício efetivo das funções:

- No momento de admissão de qualquer colaborador;
- Numa base anual para todos os colaboradores que desempenham funções de uma forma contínua.

O Departamento de Recursos Humanos da Critical, departamento que efetua a gestão da formação, mantém, em pasta própria, o arquivo com informação relativa a cada ação formativa frequentada pelos colaboradores. O referido arquivo é conservado e deve conter, para cada ação de formação, a seguinte informação:

- Descrição e Objetivos;
- Data, local, duração (período e número de horas da formação);
- Natureza da formação (Interna ou externa) e forma (presencial ou à distância);
- Identificação do Formador;
- Lista de presença dos participantes com as respetivas assinaturas, identificando as respetivas funções desempenhadas na Critical.

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

ANEXO 1- MATRIZ DE RISCO

ANEXO 2 – FICHA DE IDENTIFICAÇÃO DE PESSOA COLECTIVA

ANEXO 3 – CÓDIGO DE CONDUTA CRITICAL

ANEXO 4 – REGULAMENTO CANAL DENÚNCIA

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

ANEXOS

Matriz de Risco

		Probabilidade	Impacto	Medidas Correctivas/Preventivas
TRANSVERSAL				
	Conflito de interesses	Média	Médio	Código de conduta define o procedimento a adoptar em caso de conflito de interesses
	Ocorrência de situações integráveis no conceito de fraude	Baixa	Alto	(i) Código de conduta define o comportamento esperado dos diferentes stakeholders da organização; (ii) cultura corporativa
	Favorecimento na escolha de fornecedores/parceiros com o objectivo de retirar benefícios indevidos para o próprio ou para terceiros	Baixa	Médio	Código de conduta define as regras para a escolha de fornecedores e parceiros
	Fuga de informação; violação de obrigação de confidencialidade; utilização indevida de informação confidencial	Média	Alto	(i) mecanismos de encriptação de informação; (ii) acesso restrito à informação
CONSELHO DE ADMINISTRAÇÃO				
	Sujeição da actuação do CA a pressões externas	Baixa	Médio	(i) diferentes intervenientes na tomada de decisão;
	Utilização indevida de recursos ou competências para finalidades diferentes das atribuições legais da organização	Baixa	Médio	(i) diferentes intervenientes na tomada de decisão; (ii) canal de denúncia
	Utilização/divulgação indevida de informação privilegiada	Baixa	Médio	(i) acesso restrito a informação; (ii) certificações especiais para acesso a informação sensível
	Deliberações não conformes com a legalidade ou procedimentos internos	Baixa	Alto	(i) diferentes intervenientes na tomada de decisão; (ii) deliberações exaradas em ata
DIVISÕES				
Automotive, Railway and Medical Systems (ARMS)				
Processo de escolha de agentes comerciais	Favorecimento ilícito na escolha de agentes comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Médio	(i) processo de selecção e contratação tem vários níveis de decisão e revisão com diferentes intervenientes
Elaboração de propostas comerciais (Clientes)	Favorecimento ilícito na fixação das condições comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Médio	(i) Processo de aprovação de propostas com vários intervenientes (ii) código de conduta com definição clara dos comportamentos permitidos e fronteiras bem delimitadas (iii) múltiplos canais de denúncia de casos suspeitos, incluindo ombundsperson e canal de whistleblowing
Aviation, Space and Defence Systems (ASDS)				
Processo de escolha de agentes comerciais	Favorecimento ilícito na escolha de agentes comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Baixo	(i) processo de selecção e contratação tem vários níveis de decisão e revisão com diferentes intervenientes
Elaboração de propostas comerciais (Clientes)	Favorecimento ilícito na fixação das condições comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Médio	(i) Processo de aprovação de propostas com vários intervenientes (ii) código de conduta com definição clara dos comportamentos permitidos e fronteiras bem delimitadas (iii) múltiplos canais de denúncia de casos suspeitos, incluindo ombundsperson e canal de whistleblowing
Digital Engineering Services (DES)				
Processo de escolha de agentes comerciais	Favorecimento ilícito na escolha de agentes comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Baixo	(i) processo de selecção e contratação tem vários níveis de decisão e revisão com diferentes intervenientes
Elaboração de propostas comerciais (Clientes)	Favorecimento ilícito na fixação das condições comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Baixo	(i) Processo de aprovação de propostas com vários intervenientes (ii) código de conduta com definição clara dos comportamentos permitidos e fronteiras bem delimitadas (iii) múltiplos canais de denúncia de casos suspeitos, incluindo ombundsperson e canal de whistleblowing
Smart Technology Solutions (STS)				
Processo de escolha de agentes comerciais	Favorecimento ilícito na escolha de agentes comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Baixo	(i) não participação no processo de seleção em caso de conflito de interesses; (ii) vários níveis de aprovação para a aquisição dos serviços
Elaboração de propostas comerciais (Clientes)	Favorecimento ilícito na fixação das condições comerciais em troca de benefícios para o próprio ou para terceiro	Baixa	Médio	(i) não participação no processo de seleção em caso de conflito de interesses; (ii) vários níveis de aprovação prévia à submissão de proposta (PM, BDM, BDD, DD
FINANCE				
LEGAL				
	Favorecimento de fornecedores de serviços jurídicos com o objetivo de retirar benefícios próprios ou para terceiros	Baixa	Baixo	(i) não participação no processo de seleção em caso de conflito de interesses; (ii) vários níveis de aprovação para a aquisição dos serviços
Gestão de processos de aquisição de bens e serviços e controlo de qualidade dos serviços prestados	Risco de acesso impróprio a informações - quebra de sigilo	Baixa	Médio	(i) acesso à informação limitado por área; (ii) autorizações prévias para acesso a informação confidencial; (iii) certificações especiais para acesso a informação confidencial sensível
ACCOUNTING AND TREASURY				
Planeamentos financeiros	Adulteração e/ou emissão de informação que condicione a representação, de forma verídica e transparente, da situação financeira da CSW	Baixo	Médio	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
	Aceitação ilícita de benefícios e/ou favorecimentos em troca da cedência de vantagens e/ou benefícios imerecidos	Baixo	Baixo	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
Controlo orçamental	Adulteração e/ou emissão de informação que condicione a representação, de forma verídica e transparente, da situação financeira da CSW	Baixo	Baixo	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
	Aceitação ilícita de benefícios e/ou favorecimentos em troca da cedência de vantagens e/ou benefícios imerecidos	Baixo	Baixo	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
Gestão contabilística	Adulteração e/ou emissão de informação que condicione a representação, de forma verídica e transparente, da situação financeira da CSW	Baixo	Médio	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
	Aceitação ilícita de benefícios e/ou favorecimentos em troca da cedência de vantagens e/ou benefícios imerecidos	Baixo	Baixo	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
Gestão de tesouraria	Adulteração e/ou emissão de informação que condicione a representação, de forma verídica e transparente, da situação financeira da CSW	Baixo	Médio	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
	Aceitação ilícita de benefícios e/ou favorecimentos em troca da cedência de vantagens e/ou benefícios imerecidos	Baixo	Baixo	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais
	Autorizar/realizar despesas não aprovadas com numerário em caixa	Baixo	Baixo	(i) vários níveis de supervisão e controlo em funcionamento e sistemas capazes de detetar desvios ou alterações anormais. (ii) Os valores em caixa e numerário na CSW são muito baixos
	Desvio de dinheiros e valores	Médio	Alto	(i) vários níveis de supervisão e controlo em funcionamento e sistemas capazes de detetar desvios ou alterações anormais

PROCUREMENT				
Gestão de processos de aquisição de bens e serviços e controlo de qualidade dos serviços prestados	Favorecimento de fornecedores de bens e/ou serviços com o objectivo de retirar benefícios próprios ou para terceiros	Baixo	Baixo	(i) vários níveis de supervisão e controlo em funcionamento. Para além disso, temos sistemas que efetuam a gestão de todo o processo de compra
	Divulgação de informação confidencial	Baixo	Baixo	(i) acesso à informação é limitado; (ii) autorizações prévias para acesso a informação confidencial.
	Aquisição ou desvio de bens da CSW para proveito próprio ou de terceiros	Baixo	Baixo	(i) vários níveis de supervisão e controlo em funcionamento. Para além disso, temos sistemas que efetuam a gestão de todo o processo de compra
FACILITIES MANAGEMENT				
Controlo de instalações	Acesso indevido às instalações da CSW	Médio	Médio	(i) os atuais mecanismos de acesso aos edifícios restringem a circulação de pessoas que não pertencem à organização; (ii) segurança e vigilância nos edifícios com maior movimento
	Manipulação e/ou omissão de informação relevante para o bom funcionamento das actividades da CSW	Baixo	Baixo	(i) acesso à informação é limitado; (ii) autorizações prévias para acesso a informação confidencial.
Gestão de correspondência	Violação da correspondência em troca de regalias e/ou benefícios	Baixo	Baixo	(i) vários níveis de supervisão e controlo em funcionamento e sistemas capazes de detetar situações anómalas
	Risco de acesso impróprio a informações - quebra de sigilo	Médio	Baixo	(i) acesso à informação limitado por área; (ii) autorizações prévias para acesso a informação confidencial.
Gestão de inventário/economato	Aquisição, manipulação ou desvio de bens em inventário para proveito próprio ou para terceiros Inventário não contabilizado para benefício próprio ou de terceiros	Médio	Baixo	(i) vários níveis de supervisão e controlo em funcionamento e sistemas capazes de detetar situações anómalas
PEOPLE				
Processo de recrutamento e seleção	Favorecimento ilícito na escolha dos recursos humanos a contratar	Baixa	Baixo	(i) verificação prévia da existência de conflito de interesses dos vários intervenientes no processo de seleção; (ii) não participação no processo de seleção em caso de conflito de interesses; (iii) vários níveis de aprovação do candidato
	Divulgação de informação confidencial	Média	Médio	(i) Processo documentado num ATS com regras de acesso restrito à equipa de recrutamento, DD's e DOD's. No entanto, os CV's e os dados pessoais são partilhados com os entrevistadores - exigimos-lhes que eliminem os ficheiros após a conclusão dos processos, mas não temos uma forma de impor esta melhor prática.
	Critérios de seleção ambíguos	Média	Médio	(i) selecção envolve vários intervenientes
	Conflito de interesses em algum dos envolvidos no processo de recrutamento	Baixa	Baixo	(i) verificação prévia da existência de conflito de interesses dos vários intervenientes no processo de seleção; (ii) não participação no processo de seleção em caso de conflito de interesses; (iii) vários níveis de aprovação do candidato
Progressão de carreira	Criação desajustada de estruturas e/ou categorias profissionais com o propósito de extrair benefícios indevidos	Baixa	Baixo	(i) processo complexo; (ii) definição de papéis e percursos de carreira (iii) processo supervisionado com muitos intervenientes.
	Aceitação de benefícios ilícitos em troca de cedência de vantagens indevidas a colaboradores na sua progressão profissional	Baixa	Baixo	(i) processo com vários níveis de validação
Processo de avaliação e desempenho	Aproveitamento de benefícios ilegítimos em troca de vantagens ilícitas a colaboradores aquando da sua avaliação de desempenho	Baixa	Baixo	(i) vários níveis de validação do processo de avaliação do desempenho.
	Adulteração de documentos e valores	Baixa	Baixo	(i) informações em plataformas cuja alteração obedece a regras
Desenvolvimento e formação profissional dos recursos humanos da CSW	Favorecimento ilícito de formadores/entidades formadoras com o objbjectivo de retirar benefícios próprios ou para terceiros	Baixa	Médio	(i) critérios de avaliação bem definidos; (ii) vários intervenientes no processo de validação dos fornecedores.
	Falsificação de documentos/certificados de formação	Baixa	Baixo	(i) Documentos/certificados são automaticamente gerados por ferramentas.
Processamento de remunerações, abonos, descontos e processos individuais de colaboradores	Aceitação de favores e/ou favorecimentos ilícitos em troca de vantagens indevidas a colaboradores na sua remuneração	Baixa	Baixo	(i) regras para a definição de remuneração e pagamento na CSW estão claramente definidas e aprovadas; (ii) vários níveis de aprovações necessárias para poder alterar qualquer coisa nos sistemas (por exemplo, Pulsar e NAV).
	Manipulação da informação de modo a facilitar o pagamento indevido de benifícios e compensações	Baixa	Baixo	(i) regras para a definição de remuneração e pagamento na CSW estão claramente definidas e aprovadas; (ii) vários níveis de aprovações necessárias para poder alterar qualquer coisa nos sistemas (por exemplo, Pulsar e NAV).
Gestão dos processos de estágio	Acesso impróprio às informações pessoais dos colaboradores	Média	Médio	(i) acessos a dados pessoais restritos a determinadas áreas; (ii) obrigações de confidencialidade são norma para todos os colaboradores da CSW
	Favorecimento ilícitio na escolha dos estagiários	Baixa	Baixo	(i) todos os estagiários passam pelo mesmo processo de recrutamento; (ii) processo é confidencial e baseado no mérito e adaptação às posições em aberto; (iii) não participação no processo em caso de conflito de interesses; (iv) verificação prévia de situações que possam configurar conflito de interesses
	Aceitação ilícita de benefícios e/ou favorecimentos em troca da cedência de vantagens	Baixa	Baixo	(i) processo com vários níveis de validação
QUALIS				
SISTEMAS DE INFORMAÇÃO				
Gestão de software e harware	Favorecimento de fornecedores de software e/ou hardware com o objectivo de retirar benefícios próprios ou para terceiros	Baixa	Baixo	Existencia de controlos no processo de compra, tais como segregaçao de funçoes/aprovaçao por várias pessoas, que minimizam o risco de favorecimento de fornecedores. Nenhuma decisão é tomada individualmente.
	Aquisição ou apropriação de hardware e/ou software licenciado da CSW para proveito próprio ou de terceiros	Baixa	Baixo	Existencia de politicas e medidas de segurança (e.g. Controlo de acesso, atribuição de licenças seguindo um processo controlado e gerido pela equipa de IT) para minimizar o risco de roubo de propriedade intelectual ou utilizaçao indevida de SW licenciado pela CSW.
Gestão de operações de sistemas de informação	Favorecimento de fornecedores de aquisição de Sistemas de informação com o objectivo de retirar benefícios próprios ou para terceiros	Baixa	Baixo	Existencia de controlos no processo de compra, tais como segregaçao de funçoes/aprovaçao por várias pessoas, que minimizam o risco de favorecimento de fornecedores. Nenhuma decisão é tomada individualmente.
SECURITY				
Gestão de operações de sistemas de informação	Risco de acesso impróprio às informações pessoais/quebra de sigilo	Baixa	Baixo	(i) acesso à informação limitado por área; (ii) autorizações prévias para acesso a informação confidencial.
QUALIDADE				
Gestão de processos de aquisição de serviços e controlo de qualidade dos serviços prestados	favorecimento de fornecedores de bens e/ou serviços com o objectivo de retirar benefícios próprios ou para terceiros	Baixa	Baixo	Existencia de controlos no processo de compra, tais como segregaçao de funçoes/aprovaçao por várias pessoas, que minimizam o risco de favorecimento de fornecedores. Nenhuma decisão é tomada individualmente. Volume de compra nao é significativo para causar impacto.

Processos de auditoria interna	Divulgação de informação confidencial	Baixa	Baixo	Existencia de medidas de seguraça organizativas, processuais e técnicas desenhadas e implementadas para prevenir acesso indevido a informação confidencial/pessoal.
MARCOM				
Gestão de processos de aquisição de serviços e controlo de qualidade dos serviços prestados	Favorecimento de fornecedores de bens e/ou serviços com o objectivo de retirar benefícios próprios ou para terceiros	Baixa	Alto	(i) Código de conduta contém regras relativamente à contratação de fornecedores
Gestão da comunicação	Divulgação de informação confidencial	Baixa	Médio	(i) Cumprimento das regras do RGPD; (ii) auditorias regulares; (iii) Controlo regular pelo Data Controller
SUSTAINABILITY				
Processo de seleção de entidades	Favorecimento na escolha das entidades apoiadas no âmbito de actividades de responsabilidade social com o objectivo de retirar benefícios próprios ou para terceiros	Baixa	Alto	(i) Código de conduta contém regras para a escolha das entidades
	Critérios de seleção ambíguos	Baixa	Médio	(i) regras do código de conduta; (ii) melhoria continua nos procedimentos internos para escolha das entidades; (iii)

Probabilidade de ocorrência:	**Impacto previsível:**
Baixa: Possibilidade de ocorrência, mas com hipótese de obviar o evento com o controlo existente para o tratar	Baixo: Afetação da otimização do desempenho ou das atividades operacionais, requerendo revisão de procedimentos ou de calendarizações.
Média: Possibilidade de ocorrência, mas com hipóteses de obviar o evento através de decisões e ações adicionais	Médio: Impacto moderado na imagem institucional ou sobre o desempenho
Alta: Forte possibilidade de ocorrência e escassez de hipóteses de obviar o evento mesmo com decisões e ações adicionais essenciais	Alto: Prejuízo na imagem e reputação institucional, ou impacto significativo sobre a estratégia, o desempenho e atividades operacionais.

FICHA DE IDENTIFICAÇÃO DE PESSOA COLETIVA

TIPOLOGIA DE PESSOA COLETIVA

Cliente	☐	Entidade	☐

IDENTIFICAÇÃO, ATIVIDADE E CONTACTOS

Denominação :	
Grupo Económico:	
País de Constituição:	
Data de Constituição:	_____/_____/_____
Data de início de atividade:	_____/_____/_____
Código de Identificação (NIPC) (ou equivalente, se estrangeiro):	
Conservatória / País:	
Código de Atividade Económica (CAE Principal e Secundários):	
Mercados Principais:	
Forma Jurídica:	
Capital Social:	
Morada da Sede:	
País da Sede:	
Outras Instalações:	

ESTRUTURA SOCIETÁRIA

Sócios/acionistas (igual ou superior a 5% de participação de capital / direitos de voto):	
Nome Completo:	
NIPC:	
País:	
Participação social:	_____ **%**

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

ESTRUTURA SOCIETÁRIA

Direitos de voto:	_____ **%**
Beneficiários efetivos:	
Nome Completo:	
NIPC:	
País:	
Participação:	_____ **%**
Empresas detidas (> 25% de participação):	
Denominação:	
NIPC:	
País:	
Participação:	_____ **%**

ORGÃOS SOCIAIS

Gerentes/Administradores:	
Nome Completo:	
NIF:	
Outros membros relevantes com poder de gestão:	
Nome Completo:	
NIF:	
Cargo:	

Notas:

- É necessário o preenchimento de todos os quadros. Caso exista algum campo não aplicável, assinalar com N.A.

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

Declaro sob compromisso de honra que são verdadeiros os elementos indicados.

Assinatura do Representante Legal:

_____

Local de Assinatura: _____ Data: _____

Colaborador Critical: _____ Data: _____

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

Aviso de privacidade para a recolha e tratamento de dados pessoais no âmbito da Lei nº 58/2020, de 31 de agosto

Este aviso de privacidade visa esclarecer e enquadrar o fundamento para a recolha de dados pessoais, pela Critical, ao abrigo do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, doravante RGPD, e do Decreto-Lei 109 – E/2021 de 9 dezembro, na sua redação atual, que estabelece medidas de prevenção da corrupção e infrações conexas.

Neste âmbito, os dados pessoais, por nós solicitados nos presentes documentos, destinam-se exclusivamente à necessidade da Critical em cumprir as medidas de caracter preventivo e repressivo no combate a corrupção e infrações conexas, fundamentando a licitude deste tratamento, no cumprimento de uma obrigação legal, conforme o preconizado no art.º 18.º do Decreto-Lei 109 – E/2021 de 9 dezembro, e na alínea c) do artigo 6.º do RGPD.

A Critical não partilha nem divulga os dados pessoais supra referidos, salvo se a isso for obrigada por imposição legal ou regulamentar, nomeadamente para as situações previstas no Decreto-Lei 109 – E/2021.

Para o efeito a Critical, enquanto responsável pelo tratamento dos dados, utiliza as técnicas e as medidas organizativas e de segurança adequadas para proteger as informações pessoais tratadas e garantir a sua confidencialidade.

Os Titulares dos Dados poderão exercer os seus direitos, contactando o Encarregado da Proteção de Dados da Critical, que responderá às suas questões (exceto as que lhe estão vedadas por obrigação legal ou regulamentar) através dos seguintes contactos:

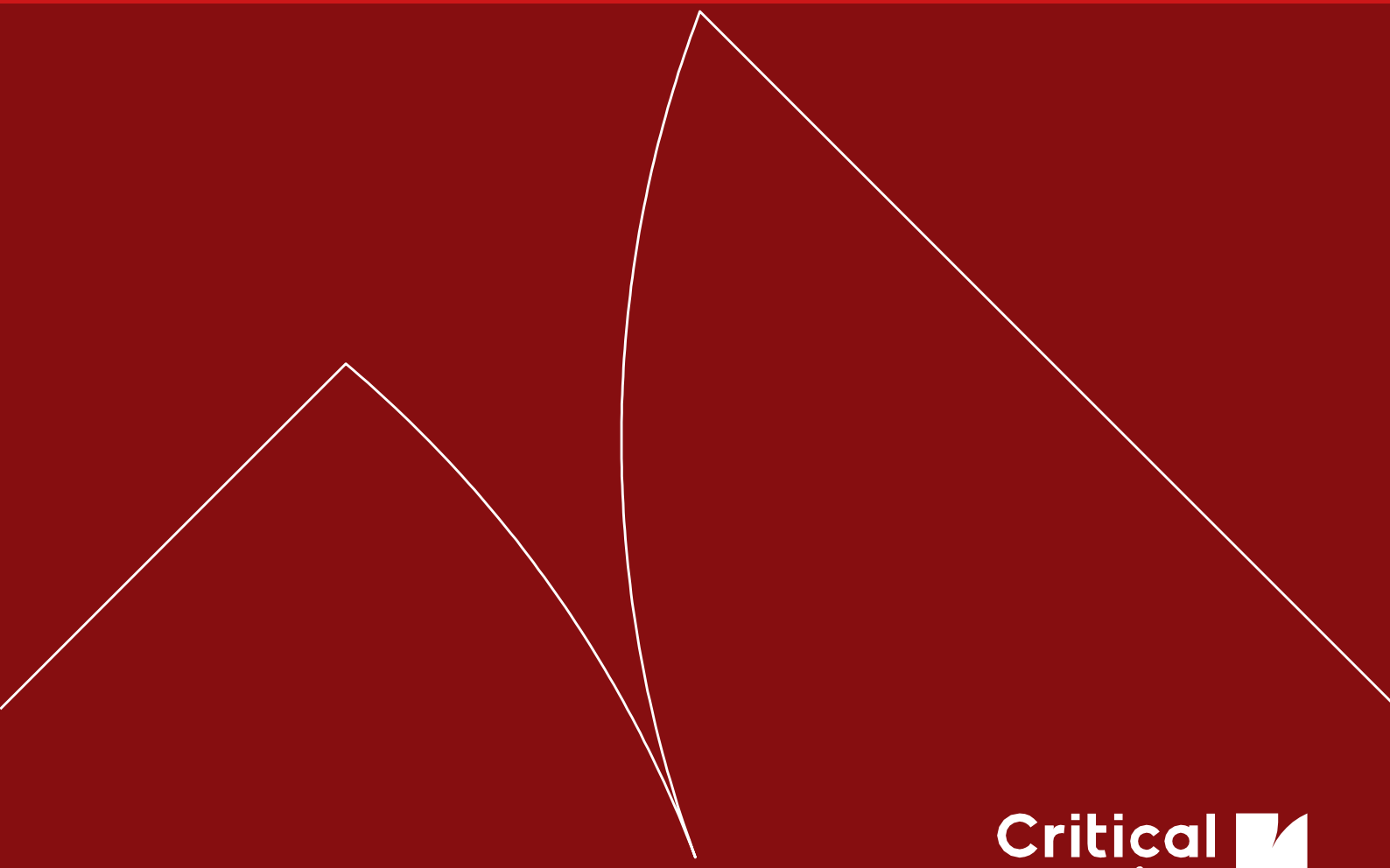
Email: xxxx
Carta/presencial: xxxx

Poderá ainda ser consultada a nossa política de privacidade através do site xxxx

©2023 COPYRIGHT CRITICAL SOFTWARE S.A. ALL RIGHTS RESERVED.

Código de Conduta

Critical Software



1. Visão geral 3
2. Objetivo e âmbito de aplicação 3
a. Valores 3
3. Relações 4
a. Relações com clientes 4
b. Relações com fornecedores 5
c. Relações com o Governo e outras Entidades Públicas 6
d. Relações com partidos e organizações políticas 6
e. Relações com Organizações Não-Governamentais (ONGs) 7
4. Anti Facilitação de Evasão Fiscal e Lavagem de Dinheiro 7
5. Presentes, Refeições e Pagamentos Indevidos 8
6. Saúde, Segurança e Ambiente 9
a. Uso de Álcool, Drogas e Armas de Fogo 9
7. Funcionários 9
8. Compromisso de Separação dos Acionistas e da Gestão Executiva 10
9. Conflitos de interesses 11
a. Conflitos de Interesses que envolvem Fornecedores ou Outras Entidades Externas 11
b. Conflitos de Interesses entre Funcionários 11
c. Conflitos de Interesse que envolvem posições de liderança de topo dentro da empresa 12
10. Igualdade de oportunidades 12
a. Recrutamento 13
b. Ajuste 14
c. Formação e Desenvolvimento de Carreira 14
d. Discriminação 14
e. Trabalho a Tempo Parcial e Contrato a termo 15
f. Reclamações 15
11. Anti Assédio e Anti Bullying 15
a. O que é assédio? 15
b. O que é Bullying? 16
c. Se estiver a ser assediado ou intimidado 17
d. Proteção e Apoio às Partes Envolvidas 17
e. Manutenção de Registos 17
12. Procedimento de queixa e ação disciplinar 17
13. Proteção de dados e propriedade intelectual 18
14. Responsabilidade Social das Empresas 18
15. Esclarecimentos e Omissões 18

Código de Conduta

Critical Software

1. Visão geral

Um pilar central do desenvolvimento da Critical Software SA (daqui em diante referida como CSW ou empresa e incluindo todas as suas filiais) é a nossa ética de conduta. Incorpora os princípios que fazem parte do nosso ADN. As políticas expressas neste Código de Conduta (Código) detalham o nosso compromisso ético nas relações com clientes, funcionários, fornecedores, autoridades governamentais, meios de comunicação social, comunidades e sociedade em geral.
A aprovação deste código e quaisquer outras atualizações são da responsabilidade do Conselho de Administração (CA) da CSW.
Este Código de Conduta é um documento público. Pode ser alterado a qualquer altura.

2. Objetivo e âmbito de aplicação

O objetivo deste Código é expressar os princípios éticos pelos quais a CSW se rege. Acreditamos firmemente que o comportamento ético é um requisito para a construção da confiança e é, portanto, crucial para o desenvolvimento sustentável da empresa. O nosso Código é fundamental para apoiar a prosperidade e fazer avançar a busca constante da excelência da empresa.
Acreditamos que este Código pode inspirar relações honestas, imparciais e transparentes que respeitem clientes, fornecedores, funcionários, sociedade e o ambiente.
A aplicação deste código é obrigatória para os funcionários da empresa, outsourcers, estagiários, e qualquer pessoa que trabalhe como parte das nossas equipas de projeto, independentemente da relação contratual estabelecida. O Código deve também servir de referência para subcontratantes, conselheiros, parceiros comerciais e comunitários. Sem pretender cobrir todas as possibilidades inerentes às operações diárias da empresa, pretende oferecer diretrizes claras e não negociáveis. É também um documento dinâmico que será sujeito a atualizações periódicas.

a. Valores

A CSW tem quatro valores centrais; o quarto é o principal impulsionador por detrás do presente documento.

Engenhamos a criatividade, e adoramos um desafio.

Os desafios criam mudança, permitindo-nos inventar coisas novas, estimular as nossas ideias e alcançar a grandeza. Os desafios ajudam-nos a servir os nossos clientes, na nossa incansável busca de "fazer o melhor". O que quer que tenhamos conseguido, estamos sempre sedentos e ambiciosos por mais, sempre a fazer novas perguntas, e sempre a inovar.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

Acreditamos que somos mais fortes juntos.

Trabalhamos árdua e eficazmente, uns para com os outros e para com o mundo à nossa volta. Acreditamos que todos com quem trabalhamos e tudo o que fazemos é importante. Orgulhamo-nos da nossa energia e estamos comprometidos a cumprir as nossas promessas. Preocupamo-nos profundamente com o nosso trabalho e somos apaixonados por atrair e nutrir os melhores talentos.

Ouvimos, pensamos, e agimos: corajosamente.

Quando as coisas são mais importantes, tomamos a iniciativa. Como equipa e como indivíduos, confiamos na nossa perícia, o que nos capacita a ser decisivos, corajosos e empenhados no nosso trabalho. Somos determinados e resilientes: nem tudo na vida é fácil, mas não quereríamos que fosse de outra forma.

Preocupamo-nos com a forma como chegamos ao topo.

A confiança está ligada a tudo o que fazemos. Somos guiados pela nossa dedicação, honestidade e integridade em todos os momentos - uns aos outros, a todos os nossos clientes e fornecedores, e às comunidades das quais somos uma parte importante. Estes princípios estão no cerne da nossa organização. Sabemos que não há atalhos para o sucesso, e estamos dispostos a percorrer a distância para nos certificarmos de que fazemos as coisas da forma correta.

3. Relações

a. Relação com clientes

A CSW compromete-se a criar valor para os seus clientes, satisfazendo e excedendo as suas expectativas e desenvolvendo soluções inovadoras e dignas de confiança. Os requisitos e expectativas dos clientes devem ser sempre considerados, e todos os requisitos acordados devem ser cumpridos escrupulosamente. A informação sobre os nossos produtos, serviços e execução de projetos fornecida pela Critical em qualquer fase da interação com os seus clientes deve ser sempre clara e autêntica, segundo o nosso melhor conhecimento. Os dados técnicos, especialmente requisitos de segurança, saúde e ambientais, devem ser comunicados aos clientes. Cada produto ou serviço deve cumprir as exigências legais relevantes do mercado e do país a que se destina.

O material promocional da empresa, produtos e serviços deve evitar exageros e preconceitos. Devem também garantir a veracidade das informações comunicadas. A CSW desaprova as comunicações enganosas. As iniciativas de comunicação da empresa devem cumprir a legislação, ética e regulamentos locais e internacionais relevantes.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

A CSW não discrimina nenhum cliente devido à sua origem, dimensão económica ou localização. Contudo, reserva-se o direito de rejeitar ou reavaliar qualquer relação comercial sempre que essa relação não seja do seu melhor interesse ou quando represente um risco legal, social, ambiental ou ético que a empresa considere injustificado.

Os pagamentos indevidos a representantes de clientes são estritamente proibidos. Presentes e refeições podem ser oferecidos (ver Secção 5. Presentes, Refeições e Pagamentos Indevidos).

A CSW compromete-se a proteger os dados confidenciais do seu cliente, fornecendo-os às instituições estatais apenas como estritamente exigido pela lei e termos contratuais aplicáveis.

b. Relação com fornecedores

A relação da CSW com os fornecedores é fundada no respeito e para permitir o desenvolvimento de produtos e serviços que acrescentam valor à empresa. Mas vai para além disso. A CSW preocupa-se com os seus fornecedores. A empresa está empenhada em envolver-se com os fornecedores locais (em relação às geografias das suas instalações) e fará parcerias com eles para desenvolver ainda mais a sua sustentabilidade.

A CSW não é a favor de monopólios - estrangulam a concorrência, eliminam oportunidades e prejudicam a capacidade humana de criatividade quando confrontada com um desafio como mudar o mundo. Pela mesma razão, a empresa acredita que deve promover a concorrência entre os seus fornecedores - o que significa que evita o estabelecimento de relações exclusivas com qualquer fornecedor.

Os fornecedores da CSW são avaliados por meio de critérios claros e sem discriminação. Todas as decisões devem ter apoio técnico, de serviço ao cliente e económico, não permitindo favorecimentos injustos de qualquer tipo. Os critérios de sustentabilidade e, em geral, os princípios enunciados neste código também são tidos em conta quando a CSW seleciona os seus fornecedores.

Os fornecedores devem assegurar uma remuneração adequada aos seus funcionários, de acordo com a legislação em vigor e acordos coletivos de trabalho, quando aplicável, que deverá ser paga atempadamente, respeitando os salários mínimos estabelecidos em cada país, assegurando o pagamento de horas extraordinárias e outras compensações, bem como as contribuições para a segurança social e os impostos devidos.

O trabalho infantil em fornecedores ou nos seus subcontratados, instalações ou locais de produção, ou em quaisquer circunstâncias sob a responsabilidade direta ou indireta dos fornecedores é proibido. Além disso, nenhum funcionário pode ser obrigado a trabalhar contra a sua vontade ou como escravo/trabalho forçado, e nenhum funcionário deve ser sujeito a castigos corporais ou coerção de qualquer tipo.

A CSW espera clareza e transparência dos seus fornecedores na descrição dos produtos e serviços, e em termos de ética, saúde, segurança e ambiente.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

Os pagamentos indevidos recebidos de um fornecedor são estritamente proibidos (ver Secção 5. Presentes, Refeições e Pagamentos Indevidos). Os fornecedores devem ser informados sobre este Código - incluindo a política que estabelece em relação a presentes, oferendas ou refeições - e a CSW espera que as suas atividades sejam compatíveis com os princípios aqui estabelecidos.

A CSW reavaliará uma relação comercial com um fornecedor sempre que seja prejudicial aos seus interesses ou se as questões éticas, legais, fiscais, ambientais e de saúde e segurança no trabalho forem desconsideradas, respeitando todas as condições legislativas e contratuais.

A CSW compromete-se a proteger os dados confidenciais do seu fornecedor, dentro das disposições estritas da lei aplicável e dos termos contratuais.

c. Relações com o Governo e outras Entidades Públicas

A CSW honra a legislação e as autoridades de todas as jurisdições governamentais onde conduz negócios e respeita as diretrizes das Nações Unidas e da União Europeia quando aplicável.

No âmbito das suas obrigações, a CSW fornece às instituições governamentais dados de empresas, conforme exigido por lei, a nível local, nacional e internacional. A CSW compromete-se a fornecer informações completas e precisas, em rigorosa conformidade com as normas legais aplicáveis.

Pagamentos indevidos a funcionários de qualquer governo não serão aceitáveis. Presentes e refeições podem ser oferecidos (ver Secção 5. Presentes, Refeições e Pagamentos Indevidos).

A empresa reserva-se o direito de manifestar publicamente a sua opinião sobre as políticas e decisões governamentais que afetam, ou podem afetar, o progresso dos negócios e das relações com os funcionários, clientes ou outros interessados, para além do cumprimento deste Código. Esta representação só pode ser exercida pelo Presidente do Conselho de Administração da empresa ou pelo Diretor Executivo, a menos que outro porta-voz seja explicitamente autorizado.

d. Relações com partidos e organizações políticas

A CSW adota o princípio de evitar a atividade político-partidária e não participa em eventos políticos externos. Ninguém a atuar em nome da empresa, funcionário ou não, pode dar qualquer contribuição, sob qualquer forma, a partidos políticos e organizações similares que se candidatem a eleições. A CSW não aceita pedidos de visita por parte de partidos políticos às nossas instalações durante qualquer período de campanha ou de campanha pré-eleitoral, entendido como os seis meses que antecedem as eleições.

Os representantes dos partidos políticos e organizações similares que concorrem às eleições serão recebidos sempre que os seus pedidos forem considerados apropriados, fora do período pré-eleitoral de seis meses. Fora desse período, a empresa está também disponível para receber representantes de entidades políticas que procuram a nossa contribuição sobre as preocupações, aspirações e perspetivas de empresas como a nossa.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

Pagamentos indevidos a funcionários de qualquer partido político não serão aceitáveis. Presentes e refeições podem ser oferecidos (ver Secção 5. Presentes, Refeições e Pagamentos Indevidos).

A empresa reserva-se o direito de manifestar publicamente a sua opinião sobre políticas e decisões políticas que afetem, ou possam afetar o progresso dos negócios e relações com funcionários, clientes ou outros interessados, e o cumprimento do presente Código. Esta representação só pode ser exercida pelo Presidente do Conselho de Administração da empresa ou pelo Diretor Executivo, a menos que outro porta-voz seja explicitamente autorizado.

Os funcionários da CSW são, evidentemente, livres de se envolverem nas atividades políticas da sua escolha quando atuam como cidadãos individuais, por oposição aos representantes da empresa, mas essa participação deve ocorrer no seu tempo livre, às suas próprias custas e deve ser tomado um cuidado razoável para evitar associar a CSW às suas próprias opiniões políticas, evitando a associação direta ou indireta à CSW, por exemplo através de vestuário ou outros elementos que tornem explícita a marca CSW. Os recursos, instalações e imagem da empresa não podem ser utilizados para interesses políticos pessoais ou relacionados com partidos, exceto conforme determinado por lei, por exemplo, no que diz respeito a atividades sindicais.

e. Relações com Organizações Não-Governamentais (ONGs)

A CSW apoia e está empenhada em trabalhar com ONGs sempre que a empresa considere que a sua missão é louvável e alinhada com a sua ambição de ajudar a tornar o mundo um lugar melhor e mais seguro.

Os pagamentos indevidos a uma ONG ou a qualquer um dos seus membros são inaceitáveis. Presentes e refeições podem ser oferecidos (ver Secção 5. Presentes, Refeições e Pagamentos Indevidos).

4. Anti Facilitação de Evasão Fiscal e Lavagem de Dinheiro

A CSW está comprometida em pagar impostos nos países onde a sua atividade tem lugar e adota uma abordagem de tolerância zero em relação à facilitação da evasão fiscal.

A evasão fiscal é o crime de fraude às receitas públicas ou de evasão fiscal fraudulenta. A evasão fiscal não é o mesmo que a elisão fiscal ou o planeamento fiscal, que são legais. Facilitar a evasão fiscal é um ato deliberado, ou uma omissão com intenção desonesta, para permitir a evasão fiscal, no país de origem do indivíduo ou da empresa ou no estrangeiro.

Todas as pessoas que trabalham para ou com a CSW devem comunicar imediatamente qualquer pedido ou exigência de qualquer pessoa, incluindo terceiros, para facilitar a evasão fiscal, ou qualquer suspeita de evasão fraudulenta de impostos por outra pessoa.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

Qualquer facilitação de evasão fiscal, não comunicação de suspeita de evasão fiscal, e ignorar atividades suspeitas será considerada uma infração deste Código, levando a CSW a tomar medidas disciplinares formais, incluindo o despedimento.

A empresa está também plenamente empenhada em cumprir toda a legislação aplicável e diretrizes adequadas para efeitos de combate à atividade de branqueamento de capitais e de financiamento do terrorismo ou de qualquer outra atividade criminosa.

5. Presentes, Refeições e Pagamentos Indevidos

Como referência, nenhum presente acima de 30 euros pode ser oferecido por qualquer pessoa da CSW ou em nome da CSW, a menos que constituam uma prática comercial normal e legítima.

Da mesma forma, um valor limite de referência para refeições, que pode ser pago para efeitos de uma reunião de negócios normal, é de 50 euros por pessoa.

Nenhuma despesa pode ser feita a não ser para fins lícitos. Ninguém a atuar em nome da empresa, funcionário ou não, pode fazer pagamentos indevidos (incluindo, mas não se limitando a, representantes de clientes, funcionários de qualquer governo, funcionários de um partido político, ONGs) ou realizar qualquer ato que possa ser interpretado como suborno, mesmo que isso signifique perder oportunidades de negócio.

Um pagamento indevido é um pagamento, sob qualquer forma, que está para além dos termos contratuais, requisitos legais ou práticas comerciais formalmente aprovadas pelos órgãos de gestão da CSW.

Em nenhuma circunstância pode ser oferecido dinheiro às partes acima referidas, direta ou indiretamente, independentemente do montante.

Por outro lado, os funcionários da CSW não devem receber presentes devido à sua filiação na CSW se constituírem qualquer tipo de suborno - incluindo, mas não limitado a presentes que possam ser oferecidos por fornecedores. Em geral, os funcionários não podem aceitar presentes ou vantagens em seu nome ou em nome da sua família ou amigos. Um valor limite de referência para presentes a serem aceites é de 30 euros.

As refeições só podem ser aceites se coincidirem com uma reunião de negócios normal, com um valor limite de referência de 50 euros por pessoa.

Os objetos recebidos como bónus, presentes e ofertas gratuitas que representam, direta ou indiretamente, distinção ou tributo pago à CSW devem ser dirigidos à direção de Departamento, ou aos Diretores de Área.

Os funcionários devem informar as entidades com as quais mantêm relações em nome da empresa sobre a política da CSW em relação a ofertas ou presentes.

Nenhum tipo de suborno é tolerado. As pessoas envolvidas serão despedidas, sem prejuízo de outras medidas legais.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

6. Saúde, Segurança e Ambiente

A saúde e integridade física dos funcionários, e de todos os que trabalham na ou para a empresa, e a proteção do ambiente, são prioridades para a empresa. A CSW trata de forma transparente toda a informação relativa a saúde, segurança e ambiente que possa ter impacto sobre os seus funcionários, quaisquer outras comunidades ou ecossistemas. A CSW está empenhada na sua própria contribuição para os objetivos do Acordo de Paris no âmbito da Convenção das Nações Unidas sobre Alterações Climáticas e, por conseguinte, está a trabalhar no sentido de se tornar carbono neutra e alinhada com os Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas. As políticas da CSW neste âmbito são detalhadas na sua declaração de política de Ambiente, Saúde e Segurança.

a. Uso de Álcool, Drogas e Armas de Fogo

A ingestão de bebidas alcoólicas enquanto se trabalha, e a entrada na empresa em estado de intoxicação, ou a trabalhar em tal estado, é inaceitável. As bebidas alcoólicas podem ser consumidas moderadamente durante as refeições e nos momentos festivos em zonas adequadas das instalações da CSW. Os funcionários também estão proibidos de utilizar ou transportar drogas ilegais, e de permanecer no local de trabalho num estado alterado causado por essas substâncias, o que poderia afetar a segurança ou o desempenho dos outros funcionários; isto também se aplica a qualquer visitante. Não é permitido qualquer tipo de arma de fogo nas instalações da empresa, exceto para os profissionais expressamente autorizados.

7. Funcionários

A CSW deve tratar os seus funcionários com dignidade, proporcionando um ambiente de trabalho com oportunidades iguais de crescimento profissional e pessoal, com respeito pela liberdade individual.
A CSW acredita que a riqueza que consegue gerar deve ser distribuída de uma forma justa, comprometendo-se assim com a regra de que, na empresa, o salário mais elevado não pode ser mais de 10 vezes superior ao salário mais baixo.
Não aceitamos trabalho infantil e trabalhamos ativamente contra ele. Nenhum funcionário é obrigado a trabalhar contra a sua vontade ou como escravo/trabalho forçado, e nenhum funcionário é sujeito a castigos corporais ou a coerção de qualquer tipo. É inaceitável que funcionários, subcontratados e funcionários dos subcontratados se envolvam em atividades relacionadas com o tráfico de seres humanos.
A CSW recusa todo o tipo de mecanismos de pagamento ilegais aos funcionários.

Erros ou equívocos resultantes de ações bem intencionadas são vistos como oportunidades de aprendizagem e crescimento e devem receber uma orientação construtiva. A CSW acredita que só através de erros é que podemos crescer, ser criativos e desenvolver-nos individual ou coletivamente. No entanto, a repetição de tais erros ou equívocos resultantes de descuido, negligência, falta de interesse ou mesmo desonestidade, não será aceite pela CSW.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

A CSW acredita e está empenhada num ambiente de trabalho aberto, honesto e transparente, nomeadamente no que diz respeito ao desenvolvimento da carreira e às aspirações dos funcionários. Como exemplo, a manifestação de interesse de qualquer funcionário em participar num processo de recrutamento interno é vista pelo seu gestor como uma alternativa normal de desenvolvimento de carreira e não acarretará qualquer tipo de preconceito ou reação negativa ou afetará negativamente as aspirações de carreira do funcionário.

A empresa incentiva a liberdade de expressão, respeita a livre associação, reconhece as entidades sindicais como representantes legais dos funcionários e procura um diálogo constante para a resolução de conflitos de natureza laboral ou sindical.

Os funcionários não podem utilizar o nome da empresa para seu benefício pessoal no tratamento de assuntos pessoais de qualquer natureza com o governo ou entidades da administração pública.

Os pagamentos indevidos recebidos por um funcionário são estritamente proibidos (ver Secção 5. Presentes, Refeições e Pagamentos Indevidos).

8. Compromisso de Separação dos Acionistas e da Gestão Executiva

A CSW acredita que, a fim de promover a transparência, responsabilidade, equidade, boa governança e sustentabilidade a longo prazo, o Conselho de Administração da empresa deve ser composto estritamente por indivíduos que se destacam pelos seus próprios méritos. Estes indivíduos não devem ter laços familiares estreitos com os acionistas, que têm o seu legítimo lugar no Conselho de Administração.

A natureza empresarial e a história da CSW determinou que, atualmente, a partir de 2020, os fundadores e acionistas-chave continuam a estar profundamente envolvidos nas operações da empresa e do Conselho de Administração. No entanto, a empresa compromete-se a estabelecer uma política, o mais rapidamente possível, para separar os acionistas e familiares do Conselho de Administração da empresa.

Neste contexto, os acionistas são definidos como indivíduos que possuem direta ou indiretamente mais de 5% das ações da CSW e excluem os planos de incentivos de ações relacionados com a gestão.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

9. Conflitos de interesse

a. Conflitos de Interesses que envolvem Fornecedores ou Outras Entidades Externas

Existe conflito de interesses na relação funcionário-empresa (por exemplo, com um fornecedor) quando os funcionários da CSW podem ser tentados a não agir no melhor interesse da empresa mas, em vez disso, a usar a sua influência ou a agir em benefício dos seus próprios interesses pessoais ou de terceiros, ou a causar danos aos interesses de terceiros. Isto inclui, mas não está limitado a relações familiares e outras relações estreitas, positivas ou negativas.

Todos os funcionários da CSW devem assegurar-se de que não têm qualquer participação em qualquer negociação em que tal conflito de interesses possa surgir ou, se não forem capazes de o assegurar, devem revelar a situação aos Gestores Imediatos e ao Chefe de Departamento ou Área, ou ao Diretor Executivo ou ao Presidente do Conselho de Administração, dependendo de quem está na melhor posição para tomar as providências necessárias para garantir que não haja interferência de qualquer tipo. Se não o fizer, será considerado uma infração do presente Código e poderá levar a CSW a tomar medidas disciplinares formais, incluindo o despedimento.

Os funcionários da CSW não podem empreender atividades profissionais externas independentes, tais como serviços de consultoria ou outras colaborações profissionais independentes de qualquer tipo, com clientes, fornecedores, concorrentes ou outros terceiros que tenham relações com a CSW. As exceções devem ter o consentimento prévio por escrito do Conselho de Administração da empresa.

b. Conflitos de Interesses entre Funcionários

A Critical compreende que, como comunidade viva, os funcionários podem ter relações pessoais de amor ou ódio, ser membros da mesma família ou ter interesses em comum. Sempre que estas circunstâncias possam influenciar o julgamento profissional, todos os funcionários da CSW devem assegurar-se de que se afastam de qualquer situação em que este tipo de parcialidade possa ocorrer. No caso de o funcionário não conseguir fazê-lo por si próprio, deve revelar a situação ao <Provedor >, que deve envolver quem estiver na melhor posição para tomar as medidas necessárias para garantir a ausência do referido enviesamento (por exemplo, Chefes Hierárquicos, Chefe de Departamento ou Área, ou ao Diretor Executivo ou ao Presidente do Conselho de Administração).

Os funcionários podem ser convidados a colaborar ativamente na procura e aplicação de uma solução que proteja contra qualquer conflito de interesses, por exemplo, impedindo as partes de trabalharem em conjunto, ou tendo qualquer ligação direta ou indireta de comunicação.

Qualquer pessoa com uma relação pessoal com alguém, de natureza familiar ou outra e apesar de tal relação ser positiva ou negativa, pode referir essa pessoa para ser considerada para uma vaga, mas não pode participar no respetivo processo de recrutamento em nenhuma circunstância e de nenhuma forma.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

O não cumprimento do disposto nesta secção será considerado uma infração do presente Código e poderá levar a CSW a tomar medidas disciplinares formais, incluindo o despedimento.

c. Conflitos de interesse que envolvem posições de liderança de topo dentro da empresa

Os conflitos de interesse descritos na secção anterior envolvendo um membro da Diretoria, Conselho de Administração, outros órgãos estatutários, ou qualquer diretor da empresa ("Top Positions (Posições de topo)"), estão sujeitos a uma política mais estrita. A CSW acredita que a natureza destes cargos, o seu nível de responsabilidade e visibilidade para o resto da empresa tornam-nos particularmente responsáveis por padrões mais elevados, delineados da seguinte forma:

Princípio de evasão: Os membros da Diretoria, Conselho de Administração e outros órgãos estatutários da empresa compreendem plenamente que os conflitos de interesse, de qualquer natureza - nomeadamente amigo ou inimigo, amor ou ódio - não são desejáveis e devem ser evitados. Por conseguinte, estão sujeitos a uma responsabilidade fiduciária para com a empresa e são encorajados a agir prontamente a fim de prevenir e evitar - na medida do possível - qualquer conflito de interesses que possa surgir.

Princípio de divulgação: Na medida em que não se consiga evitar, a CSW exige que qualquer membro da Diretoria, Conselho de Administração e outros órgãos estatutários da empresa revele imediata e integralmente qualquer conflito de interesses com qualquer funcionário da empresa ou candidato a uma oportunidade de trabalho na empresa. A não divulgação será considerada uma violação do Código e poderá levar a CSW a tomar medidas disciplinares formais, incluindo o despedimento. A divulgação é feita a todos os membros do conselho a que a pessoa envolvida pertence, e à pessoa/ conselho que procurará a reparação, tal como indicado no parágrafo seguinte.

Remediação: Se surgir um conflito de interesses envolvendo um membro da Diretoria, Conselho de Administração e outros órgãos estatutários, será procurada uma solução que atenue a situação. Os conflitos no seio do Conselho de Administração serão mediados e resolvidos pelo Diretor Executivo. Os conflitos com o Diretor Executivo e outros órgãos estatutários para além do Conselho de Administração serão mediados e resolvidos pelo Conselho de Administração. Conflitos no seio do BoD (Conselho de Administração) serão mediados e resolvidos pelo <Provedor >.

10. Igualdade de Oportunidades

A CSW promove a diversidade e a inclusão, e não permite a discriminação ou preconceito de qualquer natureza, incluindo gravidez ou paternidade, deficiência, etnia, cor, origem étnica ou nacional, nacionalidade, religião, crença ou filiação política, filiação ou não filiação sindical, género, mudança de género, orientação sexual, condição física, idade, estado civil ou matrimonial, etc., doravante designados coletivamente por Características Protegidas.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

Nos processos de recrutamento, seleção e promoção, os candidatos devem ser avaliados exclusivamente em função da sua capacidade de satisfazer e adaptar-se às exigências do cargo.
As pessoas portadoras de deficiência ou que se tornem portadores de deficiência são encorajadas a revelar a sua condição à empresa para que esta possa considerar quais os ajustes ou apoios razoáveis que podem ser apropriados. As questões de saúde ou de deficiência podem ser incluídas nos formulários de monitorização da igualdade de oportunidades, que não devem ser utilizados para efeitos de seleção ou de tomada de decisões.

A empresa promoverá ativamente a igualdade de oportunidades nos seus negócios para assegurar que os indivíduos recebam tratamento justo, equitativo e consistente com as suas aptidões, potenciais aptidões e capacidades relevantes. Todos os funcionários têm a responsabilidade pessoal de aderir aos princípios da igualdade de oportunidades.

Entre os seus esforços para promover a diversidade e a inclusão, a CSW está empenhada em promover proativamente a igualdade de género. A igualdade de género é um tema essencial para a empresa, não só ao nível das comunidades tecnológicas, mas também no âmbito da gestão de topo. As comunidades tecnológicas são conhecidas pela prevalência de homens dentro delas, uma situação que se torna percetível a nível universitário; isto cria uma assimetria acentuada, sensível ao género, que as empresas tecnológicas herdam e é difícil de corrigir. A CSW investe energia e recursos para superar este desafio de forma abrangente.
A empresa controlará regularmente as suas políticas de modo a assegurar-se de que persegue efetivamente um ambiente de igualdade de oportunidades. Além disso, reconhece as suas obrigações ao abrigo das leis aplicáveis em cada país onde opera.

a. Recrutamento
As vagas devem ser profusamente publicitadas dentro do mercado de trabalho. Os anúncios devem evitar estereótipos ou utilizar formulações que possam desencorajar a candidatura de determinados grupos.

O recrutamento é efetuado unicamente com base nas capacidades do candidato e na sua aptidão para o trabalho. Não devem ser colocadas questões aos candidatos, que possam sugerir uma intenção de discriminação com base numa Característica Protegida.

Por exemplo, os candidatos, se do sexo feminino, não deverão ser questionados se estão grávidas ou se planeiam ter filhos. Os candidatos não devem ser questionados sobre as condições de saúde ou incapacidade, exceto nas circunstâncias muito limitadas permitidas por lei. Por exemplo, para verificar se um candidato pode desempenhar uma parte intrínseca do trabalho (tendo em conta quaisquer ajustes razoáveis), ou para ver se podem ser necessários quaisquer ajustes aos procedimentos de candidatura para garantir que não estão em desvantagem devido à deficiência - mas garantindo sempre que este procedimento não resulte em qualquer tipo de discriminação. Quando necessário, as ofertas de trabalho podem depender de um controlo médico aceitável, mas uma deficiência não justificará, por si só, o não recrutamento de um candidato.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

b. Ajuste

Quando um funcionário portador de deficiência começa a trabalhar, ou um funcionário existente se torna portador de deficiência, a empresa, em consulta com o funcionário portador de deficiência, assegurará que sejam feitos os ajustes razoáveis necessários para lhe permitir trabalhar de forma segura e eficaz e para assegurar a igualdade de acesso aos benefícios do trabalho. A principal responsabilidade de organizar os ajustes adequados caberá à empresa que consultará o funcionário em questão, cujo conhecimento sobre a sua própria deficiência será reconhecido.
O acordo do funcionário será procurado ao longo de todo o processo. Caso a empresa não disponha dos conhecimentos necessários para resolver o problema, consultará, sempre que necessário, um especialista externo.

c. Formação e Desenvolvimento de Carreira

A empresa irá formar, desenvolver e promover indivíduos com base no mérito e capacidade, e encorajar funcionários e candidatos com todos os tipos de Características Protegidas. A promoção e a formação serão tornadas acessíveis a todos, incluindo funcionários com deficiência, para os quais serão feitos ajustes sempre que necessário.

d. Discriminação

A discriminação não é tolerada na CSW, incluindo entre atuais e antigos funcionários, candidatos às vagas de emprego, clientes, fornecedores, visitantes ou qualquer outro indivíduo. Isto aplica-se no local de trabalho, fora do local de trabalho (ao lidar com clientes, fornecedores ou quaisquer outras pessoas), e em viagens ou eventos relacionados, incluindo eventos sociais.
As seguintes formas de discriminação são estritamente proibidas:

(a) Discriminação direta: tratar alguém de forma menos favorável por causa de uma Característica Protegida. Por exemplo, rejeitar um candidato ao trabalho devido às suas opiniões religiosas ou devido à sua orientação sexual.
(b) Discriminação indireta: uma disposição, critério ou prática que se aplica a todos mas que afeta negativamente as pessoas com uma determinada Característica Protegida mais do que outras e não se justifica. Por exemplo, exigir que um trabalho seja efetuado a tempo inteiro em vez de a tempo parcial afetaria negativamente os pais que têm compromissos de guarda de crianças. Tal exigência seria discriminatória, a menos que pudesse ser justificada.
(c) Vitimização: retaliação contra alguém que se tenha queixado ou apoiado a queixa de outra pessoa sobre, por exemplo, discriminação, conflito de interesses, assédio ou intimidação.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

e. Trabalho a Tempo Parcial e Contrato a termo

Os funcionários a tempo parcial e a contrato a termo devem ser tratados da mesma forma que os funcionários comparáveis a tempo inteiro ou permanente e beneficiar de termos e condições não menos favoráveis (numa base pro-rata, quando apropriado), a menos que um tratamento diferente se justifique.

f. Reclamações

Qualquer funcionário que acredite ter sido injustamente discriminado devido a uma Característica Protegida ou por razões relacionadas com o fato de ter uma Característica Protegida, ou por qualquer outro tipo de razão (por exemplo, conflito de interesses, assédio ou intimidação), pode utilizar o procedimento de queixa (ver secção 12. Procedimento de queixa e Ação Disciplinar).

As infrações graves desta política serão consideradas como infração grave e podem levar a CSW a tomar medidas disciplinares formais, incluindo o despedimento.

11. Anti Assédio e Anti Bullying

A CSW está empenhada em proporcionar um ambiente de trabalho livre de assédio e intimidação e em assegurar que todo o pessoal seja tratado, e trate os outros, com dignidade e respeito.
Esta política abrange o assédio ou intimidação que ocorre tanto no trabalho como fora do local de trabalho, tais como em viagens de negócios ou em eventos relacionados com o trabalho ou funções sociais. Abrange o assédio e o assédio por funcionários (que pode incluir consultores, empreiteiros e funcionários de agências) e também por terceiros, tais como clientes, fornecedores ou visitantes das nossas instalações.
Esta política preenche os requisitos das leis aplicáveis dos países em que opera.

a. O que é assédio?

O assédio é um comportamento não solicitado e indesejado no local de trabalho que afeta negativamente a dignidade do destinatário. Consiste em conduta física, verbal ou não verbal repetida que tenha o propósito ou efeito de violar a dignidade de uma pessoa ou criar um ambiente intimidante, hostil, degradante, humilhante ou ofensivo para ela.
Um único incidente pode equivaler a assédio se for suficientemente grave. Também inclui tratar alguém de forma menos favorável porque se submeteu ou se recusou a submeter-se a tal comportamento no passado.
O assédio pode envolver conduta de natureza sexual (assédio sexual), ou pode estar relacionado com a idade, deficiência, género, etnia, ou qualquer outra característica protegida, ou em geral com o simples direito a um ambiente de trabalho saudável e produtivo (assédio moral).

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

O assédio pode incluir, por exemplo:

a) Conduta física indesejada ou "brincadeira", incluindo tocar, beliscar, empurrar e agarrar.
b) Avanços sexuais indesejados ou comportamentos sugestivos (que o assediador pode perceber como inofensivos).
c) Sugestões de que os favores sexuais podem favorecer a carreira de uma pessoa, ou que a recusa pode dificultar a mesma.
d) Observações derrogatórias ou degradantes baseadas no género, ou a exibição de material sexualmente explícito no local de trabalho.
e) Piadas sobre a etnia.
f) Referências a pessoas que utilizam descrições racistas ofensivas.
g) Nomes ofensivos.
h) Abusos verbais ou físicos devido à etnia ou cor de pele de uma pessoa.
i) E-mails ofensivos, mensagens de texto ou conteúdos das redes sociais.
j) Utilizar ideias, projetos ou propostas de colegas ou outros, sem identificar os autores.
k) Esconder a informação necessária para os colegas completarem tarefas, enquanto a divulgam a outros.
l) Escarnecer, imitar ou depreciar o desempenho profissional, deficiência ou personalidade de uma pessoa.

Uma pessoa pode ser assediada mesmo que não fosse o "alvo" pretendido. Por exemplo, uma pessoa pode ser assediada por piadas racistas sobre um grupo étnico diferente, se as piadas criarem um ambiente ofensivo.

b. O que é Bullying?

A intimidação é um comportamento ofensivo, intimidante, malicioso ou insultuoso envolvendo o abuso de poder que pode fazer uma pessoa sentir-se vulnerável, perturbada, humilhada, prejudicada ou ameaçada. Poder nem sempre significa estar numa posição de autoridade, mas pode incluir tanto a força pessoal como o poder de coagir através do medo ou da intimidação.
A intimidação pode assumir a forma de conduta física, verbal e não-verbal. Bullying pode incluir, por exemplo:

a) Ameaças físicas ou psicológicas.
b) Níveis de supervisão excessivos e intimidantes.
c) Imposição de tarefas ou prazos impraticáveis.
d) Promover o isolamento social de alguém.
e) Observações depreciativas inapropriadas sobre o desempenho de alguém.

Uma crítica legítima, razoável e construtiva do desempenho ou comportamento de um funcionário, ou instruções razoáveis dadas aos funcionários no decurso do seu trabalho, não equivale a assédio moral.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

c. Se estiver a ser assediado ou intimidado

Se estiver a ser assediado ou intimidado, considere se pode abordar o problema informalmente com a pessoa responsável. Deve explicar-lhe claramente que o seu comportamento não é bem recebido ou que o deixa desconfortável. Se tal for demasiado difícil ou embaraçoso, deve falar com o seu superior hierárquico, que pode prestar aconselhamento e assistência confidencial na resolução formal ou informal do problema.
Se as medidas informais não forem apropriadas ou não tiverem sido bem-sucedidas, deverá abordar a questão formalmente ao abrigo do nosso Procedimento de Queixa (ver secção 12. Procedimento de queixa e ação disciplinar).
Qualquer forma de assédio ou intimidação é uma potencial questão disciplinar.

d. Proteção e Apoio às Partes Envolvidas

Funcionários que apresentem queixas ou que participem de boa-fé em qualquer investigação não deverão sofrer qualquer forma de retaliação ou vitimização como resultado. Qualquer pessoa que se comprove ter retaliado ou vitimizado alguém desta forma será sujeito a ação disciplinar ao abrigo do nosso Processo Disciplinar.

e. Manutenção de registos

As informações sobre uma queixa por ou sobre um funcionário podem ser arquivadas no processo pessoal do funcionário, juntamente com um registo do resultado e de quaisquer notas ou outros documentos compilados durante o processo.
Estas serão processadas de acordo com a nossa Política de Proteção de Dados.

12. Procedimento de queixa e ação disciplinar

A CSW encoraja os seus funcionários a denunciar infrações ao código, incluindo acusações de conflito de interesses, discriminação, assédio, intimidação, fraude, desvio de fundos e suborno, para com a empresa < Provedor >. Mais do que um direito, é um dever de cada membro da CSW abordar estas questões.

Qualquer acusação de infração recebida pela empresa será tratada como confidencial. Os funcionários não serão sujeitos a qualquer forma de retaliação se estiverem a relatar fatos de boa-fé. Fazer uma alegação falsa de má-fé será tratada como má conduta e tratada de acordo com o Procedimento Disciplinar da empresa.

Os casos graves de infração deliberada e/ou falsas alegações de má-fé podem equivaler a uma infração grave resultando em despedimento.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

13. Proteção de dados e propriedade intelectual

Respeitamos estritamente a propriedade intelectual e a confidencialidade dos dados e informações do cliente.

Os funcionários que, devido à sua posição ou responsabilidades, tenham acesso a informações confidenciais que ainda não tenham sido tornadas públicas, não devem partilhar ou transferir essas informações para terceiros não autorizados durante o período de confidencialidade e devem respeitar quaisquer outros requisitos contratuais.

Em geral, as informações pessoais só devem ser utilizadas para os fins para os quais foram fornecidas.
A CSW está em total conformidade com o Regulamento Geral de Proteção de Dados da União Europeia (RGPD).

14. Responsabilidade Social das Empresas

A CSW está empenhada no desenvolvimento das comunidades onde está localizada e mantém canais permanentemente abertos de diálogo com elas. A empresa fornece incentivos aos funcionários para participarem em programas de voluntariado e de apoio à comunidade e estabeleceu objetivos e políticas ambientais que são reunidas no Programa de Responsabilidade Social Empresarial da CSW.

15. Esclarecimentos e Omissões

O objetivo deste código é cobrir a maioria das situações que podem ocorrer na vida quotidiana na CSW. Contudo, poderão existir situações que não estejam incluídas neste documento, ou em regulamentos internos, e a sua interpretação poderá não ser clara. As perguntas devem ser dirigidas ao Conselho de Administração ou ao < Provedor>.

©202020 COPYRIGHT CRITICAL SOFTWARE S.A. TODOS OS DIREITOS RESERVADOS

Critical
software



Critical Software

The Critical Employee Ombudsperson

ORG13 GOVERNANCE

DOCUMENT ID: CSWPT-2020-CPD-00303

VERSION: 01

DATE: 2020-01-22

INFORMATION CLASSIFICATION: INTERNAL

IMS (24.13)

PAGES: 9

DISCLAIMER

The work described in this report was performed by Critical Software and the responsibility for the contents resides in the author or organisation that prepared it.

© 2022 Copyright Critical Software. All Rights Reserved.

TABLE OF CONTENTS

SUMMARY 3
MAIN DESCRIPTION 3
1. Chapter I 3
1.1. General provisions 3
2. Chapter II 3
2.1. Statute 3
3. Chapter III 5
3.1. Procedures 5
4. Approval 7
5. Copyright 7
6. Authors and Contributors 7
7. Revision History 7

© 2022 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

SUMMARY

Critical Software and its subsidiaries (hereinafter collectively referred as "CSW" or "company") has an Employee Ombudsperson, a role that adheres to the following rules.

- CSWPT-2020-CPD-00303

MAIN DESCRIPTION

1. Chapter I

1.1. GENERAL PROVISIONS

1.1.1. ARTICLE 1 - DUTIES AND SCOPE OF ACTIVITY

1 - The CSW Employee Ombudsperson, hereinafter referred to as Ombudsperson, has the objective, without executive power, of defending and promoting the rights and legitimate interests of the company's employees, and to promote a healthy work environment.

2 - The Ombudsperson enjoys full autonomy and can assist and intervene across all areas of the company, including in professional relationships.

1.1.2. ARTICLE 2 - REPORTING ISSUES TO THE OMBUDSPERSON

1 - The employees of the company, individually or collectively, can report concerns and issues to the Ombudsperson where local resolution has not been successful or is deemed inappropriate.

2 - The procedure to report issues, whether they concern individuals or otherwise, are described under Article 11 hereto.

2. Chapter II

2.1. STATUTE

2.1.1. ARTICLE 3 - APPOINTMENT AND MANDATE

1 - The Ombudsperson is chosen by the Board of Directors.

2 - The Ombudsperson's term lasts for three years.

3 - The maximum duration of the exercise of the Ombudsperson's duties is six years.

4 - The Ombudsperson shall remain in office until the appointment and commencement of the term of his or her successor.

2.1.2. ARTICLE 4 - JURISDICTION

1 - The Ombudsperson:

a) Considers issues reported by employees and can issue recommendations across all levels of the company, in order to address, repeal or assist with acts adversely affecting employees' rights, and for the improvement of professional relationships in the company.

b) Gives advice on any matters within his or her scope, from their own initiative or at the request of the Board of Directors or Management Board.

© 2022 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

c) Can directly request the participation of any parties involved in a relevant situation being examined if he or she deems necessary, in order to perform the necessary steps to understand and resolve any relevant situation.

2.1.3. ARTICLE 5 - OMBUDSPERSON'S DUTIES

1 - The Ombudsperson will be responsible for processing, according to all applicable laws, any data communicated to him or her in the pursuit of his or her duties, particularly those relating to processing and archiving.

2 - The Ombudsperson shall inform employees about the various mechanisms and instruments they can use to solve any reported problems.

3 - The Ombudsperson shall prepare an annual report of activities, according to Article 19 of this Regulation.

4 - The Ombudsperson shall have stated office hours during which he or she is available to employees.

2.1.4. ARTICLE 6 - POWERS OF THE OMBUDSPERSON

1 - The Ombudsperson is empowered to:

a) Make, with or without notice, visits to offices, meetings with employees, information requests or visibility of any documents he or she deems appropriate or necessary.

b) Where necessary, make recommendations to the Management Board and the Board of Directors, and other levels of the company.

c) Seek, in collaboration with the Board of Directors and the Management Board and other responsible persons, the solutions most appropriate to the protection of employees' interests.

2.1.5. ARTICLE 7 - DUTY OF CONFIDENTIALITY

1 - The Ombudsperson is subject to secrecy under the law regarding the data collected that may compromise privacy.

2 - Third parties involved in any issues or investigations are subject to a confidentiality commitment to all facts and information to which they have had access during any assessment or enquiries.

3 - The Ombudsperson must ensure the preservation of the identity of anyone reporting an issue.

4 - The exemptions from the provisions of the preceding paragraph apply in the following situations:

a) the case cannot be investigated without the disclosure of the identity of the individual reporting it;

b) there is a legal requirement to provide information relating to the issue;

c) Article 18 is applied.

5 - When paragraph a) above applies, the Ombudsperson must notify the individual who reported the issue that the investigation is not possible without disclosure of identity, setting a deadline for the individual to decide whether to consent to identification in order to continue the process.

6 - For the purposes of the preceding paragraph, the process will be terminated in case of a lack of response by the deadline or the individual's insistence on maintaining the non-disclosure of his or her identification, unless the seriousness of the situation requires further treatment.

2.1.6. ARTICLE 8 - DUTY OF COOPERATION

1 - All employees of the company must cooperate with the Ombudsperson, in particular to provide all clarifications and information requested by the Ombudsperson as part of his or her duties.

2 - The Ombudsperson may set, in writing, a deadline of not less than five working days to receive an answer to requests.

3 - The Ombudsperson may also request information from employees concerned or connected with the case and/or request their presence at a hearing.

4 - Any unjustified breach of the duty of cooperation can lead to further disciplinary procedures.

© 2022 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

2.1.7. ARTICLE 9 - RESOURCES

1 - The Board of Directors and the Management Board provide to the Ombudsperson the physical, administrative, financial and technical resources required by his or her function.

2 - The Ombudsperson performs his or her role autonomously in terms of the management of appropriate resources.

3. Chapter III

3.1. PROCEDURES

3.1.1. ARTICLE 10 - INITIATIVE

1 - The Ombudsperson shall perform his or her duties based on:

a) Reports of issues from employees relating to either themselves or to other employees of CSW or other individuals the company may come into contact with.

b) Information that somehow comes to its attention and justifies an intervention, typically of a preventive nature.

2 - Reports of issues can be submitted either individually or as a group.

3 - With reports involving a group, the Ombudsperson will work to identify a lead, typically the individual who first reported the issue, to whom all communication is directed.

3.1.2. ARTICLE 11 - REQUIREMENTS FOR ISSUE ANALYSIS

1 - Issues should be reported to the Ombudsperson in writing, preferably by electronic means, and should include at least the following elements:

a) Description of the acts or facts that give rise to the issue, and the identification, where applicable, of any related individuals.

b) Explanation of the reasons that the reporter considers the act or omission as detrimental, for example, to the legitimate interests of any other employees concerned.

2 - The reporter of the issue may choose to identify him/herself.

3 - The report should be submitted no later than 180 days from the date the individual submitting the report became aware of the circumstances that relate to it.

3.1.3. ARTICLE 12 - PRELIMINARY ASSESSMENT

1 - Reports of issues are subject to a preliminary analysis of the Ombudsperson for an assessment of their admissibility.

2 - Reports of issues are rejected outright in the following circumstances:

a) The issue that the reporter wants to see addressed is not understandable.

b) The report has no clear basis or is clearly presented in bad faith.

c) The Ombudsperson has already handled the subject of the report.

d) The issue raised does not fall within the Ombudsperson scope, set out in Article 1.

3 - If the reporter of the issue has identified him/herself, when issues do not meet the requirements set out in Article 11 or are presented in terms that are considered incorrect or inadequate, the Ombudsperson should invite the individual to address those aspects in order to better assess the issue.

4 - When any of the situations listed in Article 12, section 2 arise, the Ombudsperson shall notify the individual in writing that issued the report (if identified) the reasons for deciding not to proceed with any further action.

© 2022 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

3.1.4. ARTICLE 13 - INSTRUCTION

1 - All accepted issues reported will give rise to a duly identified and numbered process, after which the Ombudsperson shall take such steps that may be necessary and appropriate to establish the facts, in order to analyse and assess them and, where appropriate, to formulate a recommendation, an opinion or to write a report.

2 - The process shall use informal means wherever possible, when it is most appropriate to quickly solve a particular issue.

3.1.5. ARTICLE 14 - REGISTER

Issues reported must be registered.

3.1.6. ARTICLE 15 - PRELIMINARY HEARING

Before arriving at any conclusions, the Ombudsperson should hear, in person or in writing, from any individuals for which the issue reported relates to, giving them the right to provide all necessary explanations and perspectives, typically within five working days.

3.1.7. ARTICLE 16 - DECISIONS AND OUTCOMES

After examination of an issue that the Ombudsperson decides requires an intervention, there are typically three outcomes:

a) Simply drawing attention to the issue to relevant individuals, in less serious cases.

b) A recommendation, according to Article 17 of this Regulation.

c) A participation, according to Article 18 of this Regulation.

3.1.8. ARTICLE 17 - RECOMMENDATIONS

1 - The Ombudsperson's recommendations are addressed to those individuals that should look to correct or resolve any act or situation.

2 - The body and/or persons receiving the recommendation shall, within 30 straight days after notification, communicate to the Ombudsperson the action that was taken, or the action plan that was defined and started.

3 - When a recommendation is not met and the reasons given are not considered sufficient by the Ombudsperson, it should report the situation to the Board of Directors.

4 - Whenever no reason is given for non-compliance with its recommendation or the Ombudsperson is not able to obtain the necessary cooperation, it must communicate the situation to the Board of Directors.

5 - Recommendations and opinions of a general nature, as well as the Ombudsperson's yearly reports, are communicated to the Management Board and the Board of Directors.

3.1.9. ARTICLE 18 - PARTICIPATIONS

1 - If, in the course of any procedure, sufficient evidence arises of offences of a serious disciplinary nature, the Ombudsperson must send notice to the Management Board or, if justified, to the Board of Directors.

2 - If the facts established appear to indicate violations of criminal law, the Ombudsperson must report them to the Management Board and the Board of Directors, unless a more restricted distribution is justified.

3.1.10. ARTICLE 19 - ACTIVITIES REPORT

The Ombudsperson shall prepare an annual report, submitted to the Board of Directors by 31st March each year, describing his or her activity and indicating, inter alia, the number of issue reports received, the kind of issues raised, the type of decisions taken and their acceptance by those involved.

3.1.11. ARTICLE 20 - IMPLEMENTATION

This Regulation shall enter into force on the day after it is made public within the company.

© 2022 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

Accessing the Critical Employee Ombudsperson is via:

- The Critical Employee Ombudsperson platform: https://sites.google.com/view/critical-ombudsperson/ombudsperson
- The Critical Employee Ombudsperson e-mail address: csw.ombudsperson@gmail.com

4. Approval

Version	Name	Function	Signature	Date
01	Abel Pinto	Ombudsperson		2020-01-22
01	Gonçalo Quadros	Chairman		2020-01-22

5. Copyright

The contents of this document are under copyright of Critical Software, released on condition that it shall not be copied in whole, in part or otherwise reproduced (whether by photographic or any other method) and therefore shall not be divulged to any person other than the addressee (save to other authorized offices of the addressee organization having the need to know such contents, for the purpose for which disclosure is made) without prior written consent of the CSW Quality department.

6. Authors and Contributors

Name	Description	Date
Abel Pinto	Author	2020-01-22
Gonçalo Quadros	Author	2020-01-22

7. Revision History

Version	Date	Description	Author
01	2020-01-22	Exported from intranet to IMS Portal. Initial Version.	Abel Pinto

© 2022 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

© 2022 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

Critical software

We are CMMI Maturity Level 5 rated.

For a list of our certifications & standards visit our website.



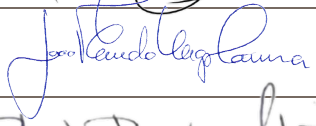
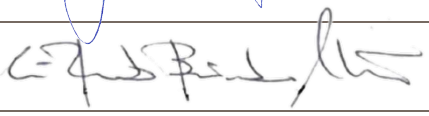
www.criticalsoftware.com

Critical Software
PROGRAMA DE CUMPRIMENTO NORMATIVO
RELATÓRIO DE AVALIAÇÃO ANUAL 2025

DATA: 2026-04-30
ESTADO: APROVADO
PÁGINAS: 6
CLASSIFICAÇÃO DA INFORMAÇÃO: PÚBLICA
VERSÃO: 1

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

APROVAÇÃO

VERSÃO	NOME	FUNÇÃO	ASSINATURA	DATA
V1	Manuel Gonçalo Lopes de Almeida Quadros	Presidente do Conselho de Administração		2026-04-30
V1	João Fernando Viegas Carreira	Vice-Presidente do Conselho de Administração		2026-04-30
V1	Rui Pedro Bairrada Murtinho	Vogal do Conselho de Administração		2026-04-30

AUTORES E CONTRIBUIÇÕES

NOME	ASSINATURA	DATA
Joana Guerra		2026-04-30

COPYRIGHT

O conteúdo deste documento está protegido por direitos autorais da Critical Software S.A., liberalizado na condição de não ser copiado no seu todo, em parte ou de outra forma (seja por fotografia ou qualquer outro método) e, portanto, não deve ser divulgado a qualquer outra pessoa que não o destinatário (exceto para outros escritórios autorizados da organização que tenham a necessidade de conhecer tais conteúdos, com a finalidade para a qual a divulgação é feita) sem o consentimento prévio por escrito do Responsável pelo Cumprimento Normativo da CSW.

ÍNDICE

1. INTRODUÇÃO 4
2. IMPLEMENTAÇÃO DO PLANO DE GESTÃO DE RISCOS E DE INFRAÇÕES CONEXAS (PPR) 4
2.1. Código de Conduta 4
2.2. Canal de Denúncias Interno 4
2.3. Formação e Comunicação para a Integridade 5
2.4. Matriz de Risco 5
3. SITUAÇÕES IDENTIFICADAS DE RISCO ELEVADO OU MUITO ELEVADO DE CORRUPÇÃO OU INFRAÇÕES CONEXAS 5
4. MEDIDAS PREVENTIVAS E CORRETIVAS TOMADAS 5
5. CONCLUSÕES 5

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

1. INTRODUÇÃO

A Critical Software está consciente da sua responsabilidade no âmbito da prevenção da corrupção e infrações conexas.

Com efeito a Critical Software tem procurado atuar de acordo com regras de transparência e integridade as quais estão no topo das preocupações dos acionistas, Conselho de Administração e colaboradores.

A gestão do risco de corrupção assume um carácter transversal sendo uma responsabilidade de todos os colaboradores da Critical Software.

Desde 2021 vigora no grupo Critical o Código de Conduta com a definição clara dos valores e princípios éticos que norteiam a comunidade Critical.

O ano de 2023 foi o ano de implementação do novo Programa de Cumprimento Normativo, especificamente o Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (adiante denominado PPR) com o qual se visa uma maior transparência no controlo dos referidos riscos.

O Relatório de Avaliação Anual do PPR (2025) tem como principal objetivo apresentar os resultados e conclusões da avaliação dos riscos dos vários clusters da Critical Software, bem como as medidas de prevenção e resposta aos riscos identificados.

A coordenação do processo de preparação e elaboração do Relatório de Execução do PPR foi levada a cabo pelo Departamento Jurídico (DJ). O presente documento foi aprovado pelo Conselho de Administração.

2. IMPLEMENTAÇÃO DO PLANO DE GESTÃO DE RISCOS E DE INFRAÇÕES CONEXAS (PPR)

Durante o ano de 2025, a Critical Software deu continuidade à implementação do Programa de Prevenção de Riscos de Corrupção e Infrações Conexas (PPR), consolidando mecanismos de integridade e boas práticas de governação corporativa.

2.1. CÓDIGO DE CONDUTA

O Código de Conduta foi atualizado em **29 de julho de 2024**, com a introdução da secção **Sustainable Value Chain**, assegurando que todos os stakeholders relevantes estão cientes das nossas práticas de sustentabilidade e dos comportamentos esperados. Esta revisão reforça o compromisso da organização em integrar a sustentabilidade na sua cultura ética e nas suas relações com parceiros externos.

Em 2025, foi disponibilizada a toda a empresa, em formato e-learning, uma formação obrigatória sobre o Código de Conduta e Anti-Corrupção. A formação registou 1.380 conclusões, num universo de 1.448 trabalhadores a 31 de dezembro de 2025, o que corresponde a uma taxa de adesão de 95,3%. Esta iniciativa visou reforçar o conhecimento e a compreensão, por parte de todos os colaboradores, dos princípios éticos e das normas de prevenção da corrupção que regem a atuação da Critical Software, contribuindo para uma cultura organizacional assente na integridade e na conformidade normativa.

2.2. CANAL DE DENÚNCIAS INTERNO

No decurso do ano civil de 2025, não foram registadas quaisquer denúncias no Canal de Denúncias Interno nem junto do Provedor da Critical relacionadas com situações de corrupção ou infrações conexas. Este resultado é indicativo do compromisso generalizado da organização com os valores éticos e de integridade promovidos pelo Código de Conduta e pelo PPR.

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

A Critical Software mantém o Canal de Denúncias disponível e acessível a todos os colaboradores, assegurando a confidencialidade e a proteção dos denunciantes, em conformidade com a legislação aplicável.

2.3. FORMAÇÃO E COMUNICAÇÃO PARA A INTEGRIDADE

Em 2025, destaca-se a disponibilização, em formato e-learning e com carácter obrigatório para toda a empresa, de formação em Código de Conduta e Anti-Corrupção, que registou 1.380 conclusões num universo de 1.448 trabalhadores (taxa de adesão de 95,3%), reforçando a cultura de integridade e de prevenção da corrupção. Em 2025, a Critical Software reforçou o seu compromisso com a integridade através da promoção de diversas sessões de awareness e workshops em áreas estratégicas para a cultura organizacional. Os temas abordados incluíram Diversidade, Equidade e Inclusão (DEI), Saúde Mental, Inteligência Emocional, Sustentabilidade e Assédio Moral e Sexual no local de trabalho. Estas iniciativas tiveram como principal objetivo proporcionar aos colaboradores oportunidades para compreender diferentes perspetivas, fortalecer o bem-estar individual e coletivo e adotar práticas alinhadas com os valores de responsabilidade e sustentabilidade da empresa.

No total, foram dinamizadas 2.787,59 horas de formação, com 1.275 participações, destacando-se a forte adesão às sessões de DEI e Inteligência Emocional.

Em paralelo, a empresa manteve a sua participação ativa em redes de reflexão sobre ética empresarial, consolidando o seu compromisso enquanto membro patrocinador do Fórum de Ética da Católica Porto Business School.

2.4. MATRIZ DE RISCO

Correspondendo 2025 ao 3.º ano de implementação do PPR, procedeu-se à revisão integral da Matriz de Risco, assegurando a sua atualização e alinhamento com os riscos emergentes e as melhores práticas de gestão preventiva. Concluída a referida revisão, verificou-se que a Matriz de Risco não carecia de alteração, dado que as operações de base da organização não sofreram modificações desde a última revisão e não foram registadas quaisquer ocorrências no período em análise.

3. SITUAÇÕES IDENTIFICADAS DE RISCO ELEVADO OU MUITO ELEVADO DE CORRUPÇÃO OU INFRAÇÕES CONEXAS

Durante os meses abrangidos pela análise não foram registados incidentes, pelo que consideramos que as medidas preventivas mantêm-se adequadas.

4. MEDIDAS PREVENTIVAS E CORRETIVAS TOMADAS

Durante os meses abrangidos pela análise não foram registados incidentes, pelo que não foram implementadas quaisquer medidas corretivas.

5. CONCLUSÕES

Uma vez que, até à presente data, não existem registos de incidentes de corrupção ou infrações conexas, consideram-se para já suficientes as medidas preventivas em execução do PPR.

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

Sem prejuízo do acima referido, o responsável pela execução, controlo e revisão do PPR promoverá as medidas que se considerem necessárias caso se detetem, no futuro, situações de risco elevado ou muito elevado de corrupção ou infrações conexas promovendo-se um reforço de prevenção.

O presente Relatório de Execução será, em cumprimento do disposto no Regime Geral de Prevenção da Corrupção, divulgado na página da interna da Critical Software bem como no sítio da Internet.

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

Critical software

We are CMMI Maturity Level 5 rated.

For a list of our certifications & standards visit our website.



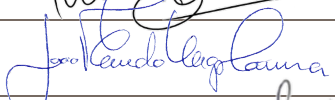
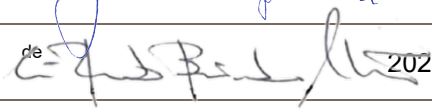
www.criticalsoftware.com

Critical Software
PROGRAMA DE CUMPRIMENTO NORMATIVO
RELATÓRIO DE AVALIAÇÃO INTERCALAR 2025

DATA: 2025-10-31
ESTADO: APROVADO
PÁGINAS: 6
CLASSIFICAÇÃO DA INFORMAÇÃO: PÚBLICA
VERSÃO: 1

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

APROVAÇÃO

VERSÃO	NOME	FUNÇÃO	ASSINATURA	DATA
V1	Manuel Gonçalo Lopes de Almeida Quadros	Presidente do Conselho de Administração		2025-10-31
V1	João Fernando Viegas Carreira	Vice-Presidente do Conselho de Administração		2025-10-31
V1	Rui Pedro Bairrada Murtinho	Vogal do Conselho de Administração		2025-10-31

AUTORES E CONTRIBUIÇÕES

NOME	DESCRIÇÃO	DATA
Joana Guerra		2025-10-31

COPYRIGHT

O conteúdo deste documento está protegido por direitos autorais da Critical Software S.A., liberalizado na condição de não ser copiado no seu todo, em parte ou de outra forma (seja por fotografia ou qualquer outro método) e, portanto, não deve ser divulgado a qualquer outra pessoa que não o destinatário (exceto para outros escritórios autorizados da organização que tenham a necessidade de conhecer tais conteúdos, com a finalidade para a qual a divulgação é feita) sem o consentimento prévio por escrito do Responsável pelo Cumprimento Normativo da CSW.

ÍNDICE

1. INTRODUÇÃO 4
2. SITUAÇÕES IDENTIFICADAS DE RISCO ELEVADO OU MUITO ELEVADO DE CORRUPÇÃO OU INFRAÇÕES CONEXAS 4
3. MEDIDAS PREVENTIVAS E CORRETIVAS TOMADAS 4
4. CONCLUSÕES 4

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

1. INTRODUÇÃO

A Critical Software reconhece a sua responsabilidade na prevenção da corrupção e de infrações conexas. Neste sentido, tem pautado a sua atuação por elevados padrões de **transparência** e **integridade**, valores que constituem prioridades para os acionistas, o Conselho de Administração e todos os colaboradores.

A gestão do risco de corrupção é transversal a toda a organização, sendo assumida como uma responsabilidade coletiva. Desde 2021, o grupo Critical adotou um **Código de Conduta** que define de forma clara os valores e princípios éticos que orientam a sua comunidade.

Em Abril de 2023, foi implementado o novo **Programa de Cumprimento Normativo (PCN)**, com destaque para o **Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPR)**, que visa reforçar a transparência e o controlo dos riscos identificados.

O presente **Relatório de Execução Intercalar do PPR (2025)** tem como objetivo apresentar os resultados da avaliação de riscos nas diversas Divisões Comerciais (DC) e Áreas de Suporte (AS), bem como as medidas de prevenção e resposta adotadas.

A coordenação da preparação e elaboração do relatório foi assegurada pelo **Departamento Jurídico (DJ)**, em estreita articulação com as DC e AS. O documento foi aprovado pelo **Conselho de Administração**.

2. SITUAÇÕES IDENTIFICADAS DE RISCO ELEVADO OU MUITO ELEVADO DE CORRUPÇÃO OU INFRAÇÕES CONEXAS

Durante os meses abrangidos pela análise não foram registados incidentes, pelo que consideramos que as medidas preventivas mantêm-se adequadas.

Departamento/Área	Risco	Probabilidade	Impacto	Medidas Corretivas/Preventivas	Avaliação Intercalar
TRANSVERSAL					
	Fuga de informação; violação de obrigação de confidencialidade; utilização indevida de informação confidencial	Média	Alto	(i) mecanismos de encriptação de informação; (ii) acesso restrito à informação	Não foram registados incidentes. Medidas preventivas mantêm-se adequadas.
FINANCE					
ACCOUNTING AND TREASURY					
	Desvio de dinheiros e valores	Média	Alto	(i) vários níveis de supervisão em funcionamento e sistemas capazes de detetar desvios ou alterações anormais	Não foram registados incidentes. Medidas preventivas mantêm-se adequadas.

3. MEDIDAS PREVENTIVAS E CORRETIVAS TOMADAS

Em virtude de não se terem registado incidentes não foram implementadas quaisquer medidas corretivas.

4. CONCLUSÕES

Uma vez que, até à presente data, não existem registos de incidentes de corrupção ou infrações conexas, consideram-se para já suficientes as medidas preventivas em execução do PPR.

©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

Sem prejuízo do acima referido, o responsável pela execução, controlo e revisão do PPR promoverá as medidas que se considerem necessárias caso se detetem, no futuro, situações de risco elevado ou muito elevado de corrupção ou infrações conexas promovendo-se um reforço de prevenção.

O presente Relatório de Execução será, em cumprimento do disposto no Regime Geral de Prevenção da Corrupção, divulgado na página da interna da Critical Software bem como no sítio da Internet.



©2025 COPYRIGHT CRITICAL SOFTWARE. ALL RIGHTS RESERVED.

Critical software

We are CMMI Maturity Level 5 rated.
For a list of our certifications & standards visit our website.



www.criticalsoftware.com