brighten
simplify your business.
together.

PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS (PPR).

Biénio 2024-2026

Brighten entidade certificada em ISO/IEC 27001

Code/Unit: 40.RGPC.003	**Type**: Digital
Confidentiality: Internal	**Available on:** Microsoft Teams / Sharepoint

Version Control

Date	Version	created / edited by	Update Description	Approved (A) by: Date:
Sep.2024	1.0	SB	Documento base	**A:** Managing Director **Data:** Sep 2024

INDICE

Figuras

1. Introdução

O Decreto-Lei n.º 109-E/2021, de 9 de dezembro, que cria o Mecanismo Nacional Anticorrupção (MENAC) e estabelece o regime geral de prevenção da corrupção (RGPC), introduziu mudanças significativas em termos de conteúdo e relativamente à forma de tratamento legislativo desta matéria. Este regime determina a implementação de sistemas de controlo interno que assegurem a efetividade dos instrumentos integrantes do programa de cumprimento normativo, bem como a transparência e imparcialidade dos procedimentos e decisões, prevendo-se igualmente um regime sancionatório próprio.

Neste sentido, entidades abrangidas pelo RGPC devem adotar e implementar um programa de cumprimento normativo, que deve incluir:

- um Plano de Prevenção de Riscos de Corrupção e Infrações Conexas ("PPR" ou "Plano");
- um código de ética e conduta;
- um canal de denúncias; e
- um plano de formação

Entre outras medidas específicas para entidades do setor público e do setor privado. O RGPC, que entrou em vigor em junho de 2022, é aplicável às pessoas coletivas com sede em Portugal que empreguem 50 ou mais trabalhadores e às sucursais em território nacional de pessoas coletivas com sede fora de Portugal que empreguem 50 ou mais trabalhadores.

Considerando este âmbito, a Brighten S.A. (adiante apenas Brighten) elaborou o seu Plano de Prevenção de Riscos e Infrações Conexas (PPR) que, seguindo a estrutura sugerida no guião disponibilizado pelo CPC[1] , compreende três partes principais:

- Estrutura Organizacional;
- Identificação dos riscos de corrupção e infrações conexas e respetivas medidas preventivas;
- Monitorização, Revisão e Aplicação do Plano

O presente Plano procura cumprir as obrigações previstas no RGPC, nomeadamente no seu art. 6º, bem como promover uma cultura de integridade e transparência pela qual a Brighten se preza.

O PPR resulta de uma análise extensiva de toda a organização da Brighten, em que foram identificados os riscos em cada uma das áreas de atividade, bem como as medidas preventivas e corretivas para mitigar esses riscos.

CPC – Conselho de Prevenção da Corrupção

O PPR aplica-se a todos os colaboradores da Brighten e demais elementos que, independentemente do seu vínculo jurídico-funcional, lhe prestem trabalho ou serviços, e constitui um instrumento de gestão fundamental que permite reforçar e consolidar os procedimentos e mecanismos de prevenção e deteção da corrupção e infrações conexas.

2. Objetivos

Com a implementação do presente Plano, a Brighten pretende dar continuidade ao seu compromisso com a prevenção e mitigação de riscos de corrupção e infrações conexas, estabelecendo como objetivos:

1. identificar, analisar e classificar os riscos de atos de corrupção e infrações conexas a que a organização está exposta, garantindo uma atuação firme e rigorosa sobre quaisquer suspeitas deste tipo de crimes;
2. desenvolver atividades de controlo e mitigação dos riscos identificados, nomeadamente identificar e implementar medidas preventivas e corretivas que permitam reduzir a probabilidade de ocorrência e o grau de impacto dos riscos;
3. aumentar a consciencialização e formação dos colaboradores;
4. monitorizar a execução do PPR, periodicamente, ou sempre que se verifiquem alterações que justifiquem a revisão;
5. A designação do responsável geral pela execução, controlo e revisão do PPR (que pode ser o responsável pelo cumprimento normativo).

A Brigthen assegura que o PPR é do conhecimento dos seus Colaboradores, publicando o mesmo na sua intranet e dando conhecimento generalizado dessa publicação via e-mail no prazo de 10 dias contados desde a sua aprovação e respetivas revisões ou elaboração.

3. Caracterização da Brighten

A Brighten hoje é o resultado da junção de 3 projectos: Procensus (1998), LCG EA (2009) e Oak Peak (2020) . Os dois primeiros projectos juntaram-se em 2015. Nesta data, o então Procensus, assume o moto **Simplify your business. Together.** e inicia um processo de reposicionamento, crescimento, diversificação, internacionalização em 2023 com a Brighten GmbH.

3.1. Missão e Lema

O nosso lema: Simplify your business. Together.

Simplify

Significa resolver desafios reais para sectores e indústrias, desde a concepção até à execução, sempre apoiados pelas soluções tecnológicas mais adequadas.

Together

A nossa abordagem e metodologia de concepção coloca o cliente no centro de toda a nossa operação, tendo a sua realidade como ponto de partida e os seus desafios como objectivo a ser ultrapassado. O cliente é o alvo e o agente activo no processo de concepção de uma solução que identifica os seus desafios e que responde às suas necessidades e melhores expectativas. Promovemos uma relação de confiança, proximidade e acompanhamento contínuo.

3.2. Valores

A Brighten assume o compromisso de desenvolver a sua atividade de acordo com uma estrutura de padrões éticos e profissionais robusta, bem como em cumprimento com as leis, regulamentos, políticas internas e os seguintes valores fundamentais:

- Veste a camisa (dos nossos clientes e a nossa)
- Desafie-se todos os dias
- Acrescenta sempre valor
- Ajuda primeiro
- Simplifica
- Faz o que diz

3.3. Estrutura Organica

3.3.1. Estrutura de Processos de Negócio

A Brighten está organizada em Linhas de Serviço ("SL" – Service Lines), que correspondem às áreas de negócio que oferecemos ao mercado (Desenvolvimento, Manutenção e Projeto) e são reforçados através de processos de suporte (IT & Segurança, People, Marketing, Shared Services & Financeira e Legal) existentes na Brighten.

Processos Core	Gestão Comercial	JC
	Planeamento & Staffing de projetos	AC, JMC
	Gestão e entrega de projetos (Projetos Fechados, Outsourcing, T&M)	RF/FB, JMC
	Suporte aplicacional & Nearshore (Gestão de centros de entrega)	SC, AN
	Análise e Fecho de projetos	FV
Processos de Suporte	People (gestão administrativa e estratégica)	CLB
	Financeira, controlo de Gestão e suporte administrativo	TL
	Marketing	TP
	Legal	Management
	IT	TL/AN
	Qualidade & Segurança de Informação	AC/JC/ SPL/SB

Figura 1 - Processos Core e Processos Suporte

3.3.2. Organograma

A estrutura organizacional da Brighten assenta numa definição coerente, clara e objetiva das linhas de reporte e de autonomia, das competências de cada área, bem como do grau e âmbito de cooperação entre si.

Todas as decisões na Brighten são, em última instância, da responsabilidade da Administração que, em colaboração com Comité Executico, definem o rumo da Brighten, a visão de futuro e as nossas principais apostas.

Além de outras responsabilidades, a Administração tem como missão definir, prosseguir e supervisionar as políticas, estratégias, direção e gestão da Brighten.

A atual estrutura orgânica da Brighten é a que consta do seguinte organograma:

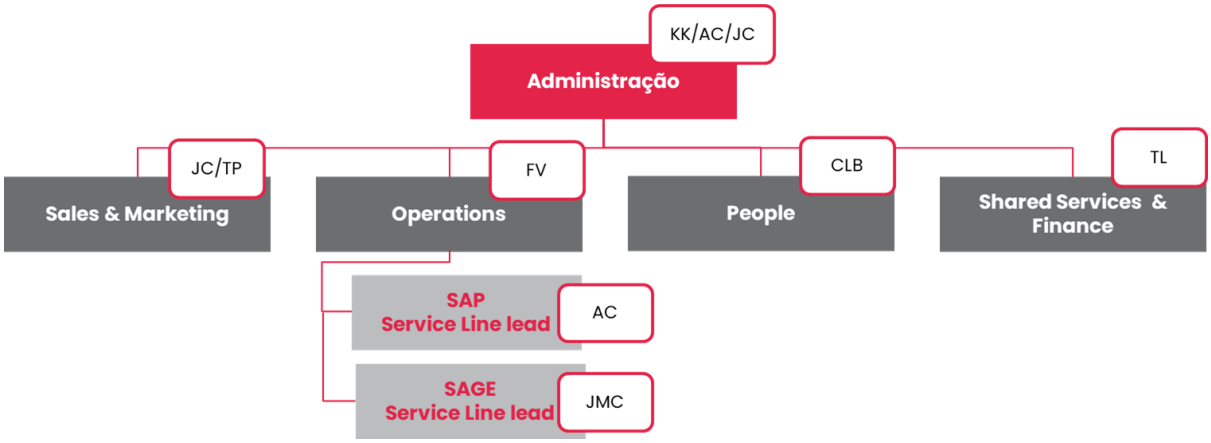

Figura 2 - Organograma Brighten

A Administração nomeou um responsável pela área de Conduta e Ética de negócio, que tem por responsabilidade coordenar a equipa que acompanha temas relacionados com comportamentos éticos, supervisiona processos de acompanhamento e formação e reporta regularmente à Administração dados relevantes da área.

A Administração nomeou ainda um Responsável pela Segurança da Informação (RSI) e um Encarregado de Proteção de Dados (EDP/DPO);

- O primeiro com responsabilidades ao nível da implementação de processos, procedimentos e Políticas relacionadas com o Sistema de Gestão de Segurança de Informação (SGSI) no âmbito da certificação da Brighten em ISO/IEC 27001 - Information security, cybersecurity and privacy protection — Information security management systems; e
- O segundo com as funções decorrentes da legislação aplicável, incluindo as responsabilidades ao nível do Sistema de Gestão de Proteção de Dados (SGPD), que visa garantir a proteção de dados pessoais de clientes e das demais partes interessadas, bem como o cumprimento legal.

A estrutura organizacional da Brighten baseia-se em definições claras e objetivas das linhas de reporte, autonomia, competências de cada área e cooperação entre si. Adicionalmente, contempla uma adequada segregação de funções para identificar antecipadamente, minimizar e monitorizar potenciais conflitos de interesses de forma independente.

4. Sistema de Controlo Interno de Riscos e Instrumentos de Gestão

4.1. Gestão dos Riscos

A Brighten integra a gestão de risco em todas as atividades e funções através do Sistema de Gestão de Segurança de Informação (SGSI). A estrutura do SGSI definida de acordo com o modelo PDCA e com a norma ISO/IEC 27001 concilia os nosso compromisso com a gestão de riscos e descreve como as atividades de gestão de riscos estão incorporadas nas nossas práticas de negócios, sistemas, processos e comportamentos, em todos os níveis da Brighten.

Compete ao RSI garantir a existência de um SGSI eficaz e robusto através de:

- um programa SGSI que está integrado no nosso negócio;
- processos de negócio que são apropriados, que promovem e facilitam a entrega de serviços de qualidade e que cumprem todos os padrões e requisitos profissionais aplicáveis pela Brighten; e
- políticas, procedimentos, processos e sistemas para gerir e reportar incidentes que possam impactar a Brighten.

O RSI em articulaçãoo com o Risk Manager e a Administração, demonstram o seu compromisso contínuo com a gestão de riscos através de:

- avaliação regular dos riscos associados à nossa estratégia;
- integração da gestão de riscos na tomada de decisões;
- atribuição e comunicação das responsabilidades e obrigações de gestão de risco; e
- desenvolvimento de medidas de desempenho para apoiar uma gestão eficaz dos riscos.

4.2. Instrumentos de Gestão e Mecanismos de Controlo

A Brighten desenvolve a sua atividade com suporte em vários instrumentos de gestão, bem como num conjunto de instrumentos adequados ao controlo da Operação e que servem de suporte às tomadas de decisão e avaliação da atividade.

No domínio **estratégico** as atividades de gestão são orientadas e suportadas pelos seguintes instrumentos:

- Objetivos estratégicos;

- Plano Estratégico: instrumento que procura definir as linhas orientadoras e as ações a implementar para o atingir desses objetivos.

No domínio da **gestão administrativa e financeira e controlo de gestão** são elaborados os seguintes instrumentos de gestão:

- Orçamento Anual;
- Plano Anual de Atividades: documento, que apresenta as propostas de atividades/projetos anuais de modo a atingir os objetivos definidos;
- Relatório de Atividades e Contas: documento que expressa as atividades anuais realizadas face ao que tinha sido estabelecido no Plano de Atividades;

No âmbito das suas políticas de gestão importa ainda destacar um conjunto de políticas e práticas pelos quais a Brighten se pauta, designadamente:

- Manual de Onboarding;
- Código de Conduta e Ética;
- Politica de Segurança de Informação;
- Politica de Proteção de Dados;
- Politica Anticorrupção;
- Canal de comunicação de irregularidades e respetiva política;
- Notificações / Comunicações / Políticas / Instruções de Trabalho e Templates: Documentos específicos orientados à execução de determinadas tarefas de carácter operacional e de suporte. São detalhes ou partes específicas de procedimentos, explicitando o **"como" fazer**. Enquadram-se neste âmbito os processos ***"Brighten_ Way"*** desenvolvidos de forma transversal para todas as Service Line (Operações e Suporte).

5. Identificação dos Riscos de Corrupção e Infrações Conexas, Metodologia e Medidas de Mitigação

5.1. Metodologia de avaliação do Risco de Corrupção e IC

A Organização Internacional de Normalização (ou *International Organization for Standardization*, "ISO"), apresenta o risco como um efeito de incerteza sobre determinados objetivos, frequentemente expresso como a combinação da probabilidade de um acontecimento com as suas consequências/impactos (incluindo mudanças nas circunstâncias)[2].

[2] *ISO Guide 73:2009 Risk management – Vocabulary*

Risco: evento, situação ou circunstância futura com probabilidade de ocorrência e potencial consequência positiva ou negativa na conquista dos objetivos de uma unidades de negócio.

Gestão do Risco: um processo de análise metódica dos riscos inerentes às atividades de execução das responsabilidades e competências das organizações, tendo por objetivo a defesa e proteção de cada interveniente nos diversos processos, salvaguardando-se, assim, o interesse coletivo.

Nível do risco: é uma combinação do grau de probabilidade com a gravidade da consequência (impacto) da respectiva ocorrência, de que resulta a graduação do risco.

Plano de Gestão de Riscos de Corrupção e Infrações Conexas: dado a tipologia de riscos que o compõem, constitui um instrumento para a gestão do risco não financeiro.

5.2. Identificação, Avaliação e Tratamento dos Riscos de Corrupção e IC

A metodologia adotada na elaboração do PPR, nomeadamente na identificação e na classificação e avaliação dos riscos de corrupção e infrações conexas compreende um processo de identificação (fase 1); avaliação (fase 2); tratamento do risco (fase 3), medidas corretivas e monitorização/reporte.

Fase 1: Identificação das ameaças ou fatores de risco de corrupção e infrações conexas – Nesta fase, realiza-se uma análise detalhada das áreas e atividades da Brighten para identificar competências ou responsabilidades que possam representar riscos de corrupção e infrações conexas. Estes são depois classificados quanto à probabilidade de ocorrência, e respetiva gravidade de consequências (impacto).

O **impacto** pode ser entendido como a consequência expectável da ocorrência de um evento que afeta os objetivos estratégicos da Brighten. Quanto à **probabilidade de ocorrência**, a mesma pode ser entendida como a possibilidade de um evento ocorrer ou não ocorrer num dado período.

Os três critérios de probabilidade de ocorrência e de impacto podem ser definidos da seguinte forma:

Probabilidade da Ocorrência (PO)	Baixa (Fator 1)	Média (fator 2)	Alta (fator 3)
Fatores de graduação	Possibilidade de ocorrência, mas com hipótese de evitar o evento com o controlo e os procedimentos existentes.	Possibilidade de ocorrência, mas com hipóteses de evitar o evento através de decisões e ações adicionais.	Forte possibilidade de ocorrência e escassez de hipóteses de evitar o evento, mesmo com decisões e ações adicionais essenciais.

Impacto Previsto (IP)	Baixo (Fator 1)	Médio (fator 2)	Alto (fator 3)
Fatores de graduação	O impacto financeiro sobre a organização não é relevante. Impacto baixo sobre a estratégia ou atividades operacionais da organização. Pouca preocupação dos intervenientes.	O impacto financeiro sobre a organização é relevante. Impacto moderado sobre a estratégia ou atividades operacionais da organização. Preocupação moderada dos intervenientes.	Prejuízo na imagem e reputação de integridade institucional, bem como na eficácia e desempenho da sua missão. Impacto financeiro é significativo. Grande preocupação dos intervenientes.

Figura 3 - Criterios de graduação Probabilidade e Impacto

Fase 2: Avaliação e Classificação do Risco – decorre da combinação da probabilidade de ocorrência das situações que comportam o risco com a severidade do seu impacto previsto, a qual resulta num grau de risco que segue uma escala com cinco níveis (muito baixo, baixo, moderado, elevado, máximo), sendo em termos gráficos geralmente atribuída, respetivamente, a cor verde, amarela ou vermelha. Estratégias de resposta distintas serão definidas em função de cada nível. A esquematização na escala de probabilidade e impacto é efetuada de acordo com a seguinte matriz de riscos:

		Probabilidade		
		Baixa (1)	Média (2)	Alta (3)
Impacto	Alto (3)	Moderado (3x1=3)	Elevado (3x2=6)	Maximo (3x3=9)
	Médio (2)	Baixo (2x1=2)	Moderado (2x2=4)	Elevado (2x3=6)
	Baixo (1)	Muito Baixo (1x1=1)	Baixo (1x2=2)	Moderado (1x3=3)

Figura 4 - Matriz de Riscos

Fase 3: Tratamento do risco – após avaliados os riscos, são definidas as respostas adequadas aos mesmos, de forma a garantir que a Brighten não fica exposta a riscos residuais acima do definido. Tais respostas podem assentar em três estratégias alternativas, nomeadamente

- Evitar o risco, eliminando a sua causa;
- Tratar o risco, procurando minimizar a probabilidade de ocorrência do risco ou do seu impacto negativo;
- Aceitar o risco e os seus efeitos;

Os perfis associados aos níveis de riscos que constam na matriz têm a seguinte interpretação:

Valor [1-2] – Aceitar	Valor [3-4] – Controlar / Prevenir	Valor [6-9] – Evitar / Transferir
Nível 1	Nível 2	Nível 3
Risco Muito Baixo / Baixo	Risco Moderado	Risco Elevado / Maximo
Controlo de riscos de corrupção largamente garantido. Poderá ser necessário implementar medidas de ajustamento pessoal e/ou organizacional tais como boas práticas ou formação.	Controlo de riscos de corrupção parcialmente garantido. Necessidade de medidas corretivas e/ou preventivas (tais como definição/ atualização de procedimentos e ações de formação específica).	Alto Risco. Necessidade urgente de medidas corretivas e/ou preventivas. Eventual incumprimento de requisitos legais.

Figura 5 - Interpretação dos níveis da matriz de risco

5.3. Identificação das Medidas de Mitigação do Risco

Sendo uma empresa certificada em ISO/IEC 27001, a Brighten implementou um conjunto de processos, que garantem não apenas uma estrutura robusta para proteção de informação e de dados pessoais, mas que também promove uma cultura de integridade e transparência na organização.

Os processos implementados para cumprimento normativo da ISO/IEC 27001 ajudam a mitigar riscos de corrupção e infrações conexas de várias formas, incluindo: a implementação de uma cultura de gestão de riscos; implementação de controlos de segurança; segregação de funções; monitorização e auditorias; definição de políticas e procedimentos.

Desta forma, algumas das medidas preventivas implementadas na Brighten, que mitigam os riscos de corrupção e de infrações conexas identificados, de forma transversal e abrangente a todas as Service Line e áreas de suporte, incluem mas não estão limitadas a:

- Código de Conduta e Ética aplicável a todos os colaboradores Brighten;
- Canal de Denúncia e Politica associada;
- Política Anticorrupção;
- Políticas de Recursos Humanos;
- Politica de Segurança de Informação;
- Politica de Gestão de Riscos e Planos de Tratamento;
- Processos para identificação e comunicação de incidentes de seguraça / *data breaches;*

- Monitorização de eventos para identificar comportamentos suspeitos, anomalias ou desvios aos processos implementados;
- Estrutura de processos e procedimentos definidos para cada uma das diferentes áreas de serviço e negócio - '**Brighten Way**';
- Preparação e tomada de decisões assente numa estrutura de validações hierárquicas;
- Segregação de funções;
- Controlos gerais dos sistemas informáticos e de controlos aplicacionais;
- Registo e restrição de acesso a sistemas e documentos;
- Legislação e normativos de enquadramento da atividade;
- Acompanhamento da atividade e supervisão por parte da Administração;
- Programação de ações de formação adequada e de sensibilização;
- Procedimentos disciplinares;
- Auditorias Internas e Externas de acordo com o plano de auditorias anual do ISO/IEC27001, com acompanhamento das ações de melhoria continua do Sistema de Gestão tendo por base o ciclo PDCA;
- Divulgação interna de Políticas, estratégias e objetivos organizacionais.

6. Monotorização e Revisão do Plano

De acordo com o definido no RGPC artigo 6º, nº5, este plano será revisto de três em três anos ou sempre que se verifiquem alterações legislativas aplicáveis à Brighten designadamente aquelas que tenham impacto na sua estrutura, atribuições, objetivos, ou alteração de atividades, serviços, ou sempre que sejam identificados novos riscos ou a necessidade da sua reavaliação, em função do resultado de relatórios de execução ou de outros mecanismos de acompanhamento.

7. Anexo – Plano de Prevenção de Riscos de Corrupção e Infrações Conexas por Unidade de Negocio

Como resultado da identificação e da avaliação dos riscos, a Brighten elaborou, com o envolvimento das suas várias áreas, a matriz de riscos apresentada, na qual (i) são identificados os riscos nas diferentes áreas de atividade da Brighten com exposição aos riscos de corrupção e infrações conexas, (ii) é analisada a probabilidade de ocorrência, o impacto potencial e, consequentemente,

o grau de risco de cada risco identificado e (ii) são identificadas as medidas preventivas e de controlo (implementadas e/ou em implementação associadas à mitigação de cada risco.

A matriz de riscos apresentada infra abrange toda a organização e atividade da Brighten, nos termos do n.º 3 do artigo 6.º do Decreto-Lei n.º 109-E/2021.

ANEXO

Matriz de Riscos de Corrupção e Infrações Conexas

A matriz de riscos apresentada infra abrange toda a organização e atividade da Brighten, nos termos do n.º 3 do artigo 6.º do Decreto-Lei n.º 109-E/2021.

Atividades	Riscos Potenciais	Avaliação do Risco			Medidas preventivas / corretivas
		PO[3]	IP	GR	
Comercial - Linhas de serviço relacionadas com o negócio					
Processo Comercial	Ausência de independência na decisão de angariação comercial de projetos a clientes que são partes relacionadas ou cujo projeto é de interesse pessoal	1	1	Muito Baixo	Segmentação das empresas a angariar é definida pela CE, a angariação é feita pela área de Sales & Marketing. Todos os clientes são registados no CRM - *Hubspot*. *"Annual sales plan"" é atualizado anualmente, numa série de reuniões de "Sales planning" Ponto 3.1.2.2 do Brighten Way of Sales.*
	Ocorrência de eventos de suborno, tráfico de influências e/ou ofertas a funcionários públicos ou do setor privado, com o objetivo de ganhar um concurso (público ou não) ou garantir a adjudicação de um contrato	1	2	Baixo	No sector público todo o processo (quer candidatura, quer pedidos de esclarecimentos) é feito via plataformas digitais (Acingov, Vortal, etc) ao abrigo do concurso publico no particular e da lei da contratação pública no geral. *Código dos Contratos Públicos - CCP - Decreto-Lei n.º 18/2008.* *Todo o processo comercial que envolve a contratação é discutida*

3 *Legenda: PO = probabilidade de ocorrência do risco; IP = impacto previsto; GR = grau de risco.*

					internamente em reunião comerciais. Regras de boas práticas definidas na _Politica Anticorrupção_Brighten .
	Estabelecimento de relações de negócios com clientes: (i) com má imagem, reputação e idoneidade; (ii) associados a investigações e/ou decisões judiciais adversas relacionadas com crimes de corrupção ou de infrações conexas; (iii) alvo de sanções aplicadas pela União Europeia, Nações Unidas ou o governo de um país onde o terceiro atua	1	2	Baixo	As bases de dados de empresas com que a brighten " trabalha" no inicio das suas relações comerciais são fornecidas por entidades credenciadas para esta gestão e controle. *Redução do risco de compliance, face aos alertas enviados pelas entidades fornecedoras dos contatos das empresas. Ie:* ***Informadb*** *Manter a informação dos clientes ativos atualizada com base nos relatórios legais e financeiros fornecido pelas entidades fornecedoras.*
Elaboração e formalização de contratos com clientes	Eventual conflito de interesses entre colaboradores internos da **Brighten** e entidades clientes	1	1	Muito Baixo	Todas as oportunidades são registadas em Hubspot e discutidas em reunião semanal L10 de Sales &Marketing. *Ponto 3.2.2.2 do Brighten Way of Sales - Client Classification & approval* .
	Elaboração e formalização de contratos com condições ambíguas ao nível das condições de pagamento e/ou com um objeto contratual abrangente/ambíguo/pouco claro, dificultando a interpretação/conferência/ fiscalização dos serviços e o controlo dos pagamentos	1	1	Muito Baixo	As propostas e contratos são construídos pela SL com o conhecimento da área de Sales, revistos pelo CE e definidos prazos e limites de pagamento com a área financeira. *Brighten Way of Sales_Pontos 3.4.2.1 - Sales Approval process e Brighten Way of Sales _Ponto 3.4.2.3 – Contracting.*
Negociação e definição dos preços / descontos e outras condições a praticar com clientes	Atribuição de descontos excessivos/ injustificados a clientes e/ou cuja razoabilidade é ambígua, em troca de benefícios alheios à **Brighten**	1	1	Muito Baixo	Mantendo reuniões periodicas entre as Servicelines/Área comercial e administração onde são discutidas as propostas entregues aos clientes e possiveis descontos Foi definido que estas decisões são sempre tomadas em conjunto . *Brighten Way of Sales_Ponto 3.4.2.1 - Sales approval process*
	Negociação e adjudicação de propostas comerciais com clientes pouco vantajosas e	1	1	Muito Baixo	

	/ ou com prejuízo direto para a **Brighten** em troca de benefícios alheios à organização				
Operações - Gestão de projetos e de clientes | Gestão de prestadores de serviço					
Gestão, acompanhamento, monitorização e controlo do cumprimento dos contratos com clientes	Deficiente acompanhamento, monitorização e controlo do cumprimento dos contratos	1	3	Moderado	Controlo de todas as atividades inerentes à execução de um projeto. Desde o kick-off até à sua conclusão, garantindo as diversas vertendes de garantia de um projeto on-time, on-budget, on-scope e on-expectations. *Descrito no documento "Brighten Way - Operações"_Ponto 3.3. 03 - Project Delivery.*
	Uso de informação privilegiada e/ou confidencial sobre a **Brighten** para obtenção de vantagens para si próprio e/ou para outrem	1	2	Baixo	Definição da política de utilização de informação confidencial e /ou priveligiada. *Descrito no documento "Brighten Way - Operações_V0.3"_ Ponto 3.3.2.4 - Execução Governance;* *Aceitação de clausulas de confidencialidade e sigilo no contrato de trabalho e código de conduta e etica (PP_Codigo Conduta e Etica) com penalizações por incumprimento de acordo com o Procedimento Disciplinar em vigor.*
Alocação de Despesas no âmbito profissional e/ou em representação da Brighten	Condicionamento de processos de despesas através de omissão/ manipulação de informação, para benefício próprio	1	2	Baixo	Garantia de legitimidade de inclusão de despesas em projetos. Garantia de revisão e aprovação de despesas em projetos. *Descrito no documento "RH06. Manual de Registo de Despesas";* *Descrito no documento "Brighten Way - Operações"_Ponto 3.3.2.5 - Controlo Projeto (Interno)* *Descrito no documento "PM309_Brighten_Aspiring_User Guide_Customer Projects"*
	Existência de despesas sem cabimento prévio, compromisso, fundos disponíveis ou autorização de responsável	1	3	Moderado	Garantia de aprovação de despesas alocadas a projetos apenas previstas e ou devidamente justificadas. *Descrito no documento "Brighten Way - Operações"_Ponto 3.3.2.5 - Controlo Projeto (Interno);*

					Descrito no documento "PM309_Brighten_Aspiring_User Guide_Customer Projects"_Ponto 7. Forecast
Alocação de horas a projetos em clientes	Eventual conflito de interesses entre colaboradores internos da Brighten e entidades clientes	1	2	Baixo	Controlo alocação de recursos a projetos. *Descrito no documento "Brighten Way - Operações"_Ponto 3.1.2.1 - Staffing (alocar recursos a projeto).*
	Aprovação de alocação de tempos de projeto ou compensações indevidas	1	2	Baixo	Garantia de aprovação de horas alocadas a projetos apenas previstas e ou devidamente justificadas. *Descrito no documento "Brighten Way - Operações", capítulo 3.3.2.5 Controlo Projeto (Interno);* *Descrito no documento "PM309_Brighten_Aspiring_User Guide_Customer Projects", nos pontos: Ponto 5 - Approval of Hours Registered in the Timesheet e Ponto 7- Forecast.*
Gestão de prestadores de serviço	Falta de transparência, isenção e imparcialidade no recrutamento de prestadores de serviço	1	1	Muito Baixo	Fluxograma de aprovações de subcontratação e alocação de recursos a projetos. *Descrito no documento "Brighten Way - Operações"_Ponto 3.1.2.2 - Análise de Mapa de Alocação de Recursos e Ponto 3.1.2.2.1 - Decisão: Subcontratação; Workflow de pedidos de contratação e Talent Solutions.*
	Risco de incumprimento dos procedimentos associados à avaliação de qualidade dos prestadores, para favorecimento nas avaliações de desempenho.	1	3	Moderado	Avaliação de desempenho dos fornecedores. *De acordo com os processos de gestão de fornecedores, todos os prestadores de serviços e fornecedores de serviços que cumprem os criterios (classificados com nivel 2 ou acima) são avaliados em termos da qualidade do serviço prestado.*
Sistemas de Informação (SI/IT)					
Organização, Arquitetura e Governação de SI/IT	Prática ou omissão intencional de atos, em violação das regras e políticas de segurança aplicáveis à atribuição de acessos à rede informática, com o fim de obtenção de vantagens indevida.	1	3	Moderado	*Possibilidade de consulta dos logs na AD para todos os acessos concedidos; Controlo dos acessos à rede, dados, e-mail e sistemas de informação Brighten; Definição da cadeia de responsabilização para atribuição de acessos; Definição de perfis de acesso para sistemas de informação; Revisão dos*

					procedimentos de registo e manutenção de utilizadores onde são definidas as regras para atribuição/alteração/remoção de direitos aos sistemas Brighten incluindo a identificação dos responsáveis pela decisão; Realização regular de auditorias internas e externas para avaliação e Cumprimento dos procedimentos escritos, aprovados no âmbito do SGSI e da certificação em ISO/IEC 27001
	Aceitação de benefícios da parte de potenciais fornecedores ou de fornecedores em troca da concessão de vantagens e/ou favorecimentos	1	2	Baixo	*Implementação da Politica de compras e de processos de gestão de fornecedores; Implementação de Processo Contratação de fornecedores outsourcing e de prestadores de serviços; Realização regular de auditorias internas e externas para avaliação e Cumprimento dos procedimentos escritos, aprovados no âmbito do SGSI e da certificação em ISO/IEC 27001*
Gerir segurança da informação e Gestão de Informação Restrita	Ausência de independência e neutralidade na emissão de pareceres para obtenção de vantagens para si próprio ou em função de outros interesses	1	2	Baixo	*Implementação de Politica de Gestão de incidentes com cadeia de avaliação de incidentes por parte de uma equipa com vários elementos incluindo a Gestão de topo; Realização regular de auditorias internas e externas para avaliação e Cumprimento dos procedimentos escritos, aprovados no âmbito do SGSI e da certificação em ISO/IEC 27001*.
	Condicionamento do processo de decisão, através de omissão/ manipulação de informação ou do adiamento/morosidade de análises e pareceres, para benefício próprio e/ou de terceiros	1	2	Baixo	*Avaliação de eviências registadas relativamente a incidentes verificados e respetivas mediddas de mitigação, em processos de avaliação anual na forma deauditoria Interna e auditoria externa (realizada por auditor independente).*
	Utilização de informação privilegiada e/ou confidencial para a escolha de fornecedores específicos	1	2	Baixo	*Implementação Politica de logging e monitorização de acessos, implementação do Código de conduta e Ética; Realização regular de auditorias internas e externas para avaliação e Cumprimento dos procedimentos escritos, aprovados no âmbito do SGSI e da certificação em ISO/IEC 27001*.
Gestão / Administração					

Planear estratégia e elaborar plano anual e relatório de atividades	Ausência de independência e neutralidade nas análises e propostas em função de outros interesses	1	1	Muito Baixo	Reuniões Semanais de Comité Executivo; Reuniões Semanais com as Service Lines; Reuniões Semanais com as direçoes das áreas de suporte. Envolvimento da administração da brighten nas várias àreas de negócio desenvolvimento de politicas de boas práticas ie: Brighten Way
	Condicionamento de processos de financiamento através de omissão/ manipulação de informação, para benefício próprio e/ou de terceiros	2	1	Baixo	Reuniões Semanais de Comité Executivo; Reuniões Semanais com as Service Lines; Reuniões Semanais com as direçoes das áreas de suporte. Envolvimento da administração da brighten nas várias àreas de negócio desenvolvimento de politicas de boas práticas ie: Brighten Way
	Atribuição de vantagens a terceiros pela intervenção em processos no âmbito das suas competências por troca de benefícios	2	1	Baixo	Reuniões Semanais de Comité Executivo; Reuniões Semanais com as Service Lines; Reuniões Semanais com as direçoes das áreas de suporte. Envolvimento da administração da brighten nas várias àreas de negócio desenvolvimento de politicas de boas práticas ie: Brighten Way
	Uso de informação privilegiada e/ou confidencial sobre a Brighten para obtenção de vantagens para si próprio e/ou para outrem	1	1	Muito Baixo	Reuniões Semanais de Comité Executivo; Reuniões Semanais com as Service Lines; Reuniões Semanais com as direçoes das áreas de suporte. Envolvimento da administração da brighten nas várias àreas de negócio desenvolvimento de politicas de boas práticas ie: Brighten Way
People (RH)					
Seleção de candidaturas	Quebra dos deveres de transparência, isenção e imparcialidade no processo de recrutamento	1	1	Muito Baixo	Estabelecidos critérios de seleção claros e específicos, com base nas competências e qualificações necessárias para o cargo. Divulgar a vaga de forma ampla e clara, com uma descrição detalhada das responsabilidades e requisitos do cargo. *Descrito na Politica interna PP_Hiring.*

	Conflitos de interesse dos colaboradores com responsabilidade pela analise de candidaturas	1	1	Muito Baixo	Desenvolvido e implementado um código de conduta e ética que define conflitos de interesse e as obrigações dos colaboradores para evitar tais situações. *Descrito em PP_Codigo Conduta e Etica*
Execução Operacional (contratação e custos com pessoal; pedidos de licença sem vencimento; comparticipação de estudos; justificação de faltas; entre outros)	Acesso indevido aos processos individuais dos trabalhadores.	1	2	Baixo	Controlo de acessos e gestão dos níveis de acessos dos colaboradores de acordo com as suas funções e responsabilidades. *Gestão de acessos de acordo com os processos implementados ISO 27001*
	Pagamentos indevidos de remunerações ou outros abonos.	1	1	Muito Baixo	Implementado um sistema de gestão de tempo e procedimentos de registo de horas e ausências. *Definido em 'PP_ Registo de horas; e PP_Registo de ausências; e PP_Remunerações e abonos; IT_Gestão de acessos; PP.07 - Política de Gestão de Carreira;* *Fluxo de aprovações - Aprovação efetuada pelo departamento financeiro e administração dependendo do custo em questão.*
Acompanhamento e Formação de Colaboradores	Desvirtualização da avaliação e aplicação de processos disciplinares.	1	1	Muito Baixo	Implementação de um procedimento disciplinar com políticas claras e documentadas para avaliação de processos disciplinares, incluindo os critérios para a aplicação de sanções.Todos os processos e sanções são documentados, organizados e arquivados de forma detalhada e em local de acesso restrito. Dependendo do grau de gravidade é definida uma equipa de avaliação que pode incluir a gestão. *Definido em 'PP_Procedimento Disciplinar*
	Desadequação do plano de formação em relação às necessidades formativas.	1	1	Muito Baixo	Desenvolvimento uma política de formação com critérios claros e objetivos. Avaliação das necessidades de formação junto das Service Lines com criação de um plano de formação anual. *Definido em PP_Plano de Formação.*

	Desaquação de staff face às funções ou da avaliação regular do seu estado geral de saúde.	1	1	Muito Baixo	Todas as etapas do processo de seleção e contratação são documentadas, incluindo os critérios de avaliação e decisões. Foram ainda definidos e implementados critérios claros e mensuráveis para a avaliação de propostas, com base em fatores como o custo, qualidade, experiência e capacidade técnica. *Definidos em 'PP_Hiring ; 02.RH.2_Politica Privacidade Selecao e Recrutamento_site.*
	Utilização/divulgação de informação privilegiada para benefício próprio ou de terceiros	1	1	Muito Baixo	Acordos de Confidencialidade: Todos os colaboradores assinam acordos de confidencialidade, comprometendo-se a não usar ou divulgar informações privilegiada. *Definido em PP_08.1.A_Medidas Seguranca IST_colaboradores*
Marketing					
Gerir e acompanhar a contratação de serviços marketing incluindo a Gestão de patrocionios e eventos relacionados	Ausência de isenção na análise de propostas de fornecedores	1	1	Muito Baixo	Critérios objetivos de seleção, processo de auditoria interna periódica ou exporádica. *Suportado pelo processo interno de aprovações com diferentes níveis hierarquicos (Service Line Lead e Administração) e sempre com justificação de negocio.*
	Favorecimento de fornecedores de bens e/ou serviços para obtenção de benefícios próprios e/ou para terceiros	2	1	Baixo	Implementação de uma politica de "nao aceitação de beneficios" para quem adjudica serviços. *Suportado pela FIN_Politica Gestão de Fornecedores.*
	Supressão de procedimentos obrigatórios e incumprimento dos princípios legais de contratação	2	1	Baixo	Manual interno com os procedimentos obrigatórios e normas legais a serem seguidos. Utilização do canal de denúncia interno para relatar possíveis violações de procedimentos. *Suportado pela FIN_Politica Gestão de Fornecedores*.
	Existência de conflitos de interesses que ponham em causa a transparência do processo para beneficio proprio	1	2	Baixo	A proposta é sugerida pela equipa de marketing com justificação de negocio, sendo sujeita ao processo de aprovação interno. Proibição da atribuição de donativos e/ou patrocínios a partidos políticos e campanhas eleitorais.

					- Suportado pelo processo interno de aprovações com diferentes níveis hierarquicos (Service Line Lead e Administração) e *- Processos associados à Politica Anticorrupção_Brighten.*
Gestão Financeira/ Contabilidade e Tesouraria					
Classificação, lançamento e registo de faturas e outros documentos de fornecedores e clientes	Desvio de fundos devido a registo de faturas (i) sem enquadramento contratual, (ii) sem documentação de suporte, (iii) sem evidências de entrega/prestação do produto/serviço, (iv) sem aprovação e/ou (v) inconsistentes com contratos e/ou pedidos de compra sem justificação aparente.	1	1	Muito Baixo	Todas as faturas disponiveis para pagamento são aprovadas por gestores ou direção. As faturas emitidas a clientes tem como base um contracto assinado pelos mesmos. *Suportado por:* *- Workflow de pedidos de compra e aprovação;* *- Controlo automático no sistema, não permitindo o pagamento de bens / serviços acima do valor contratado / requisitado;* *- Exceções aprovadas por duas pessoas (CFO/Finance Manager);* *- Todos os pagamentos acima do* plafond *definido pela Administração e que consta do Brighten Way, bem como transferências bancárias carecem dupla aprovação por parte do CFO e do CEO;* *- Reconciliações bancárias validadas por auditores externos.*
	Emissão de notas de crédito e realização de reembolsos não fundamentados para a obtenção de benefícios alheios à Brighten.	1	1	Muito Baixo	Todas as notas de crédito emitidas para correção da faturação são enviadas e retornadas assinadas e carimbadas pelo cliente. *Suportado por:* *- Auditorias Externas Anuais ao departamento Financeiro.*
	Envio indevido de faturas de fornecedores ou subcontratados para pagamento, para a obtenção de benefícios alheios à Brighten.	1	1	Muito Baixo	Levantamento da necessidade por parte do departamento financeiro, pedidos de propostas aos gestores bancários. É feita a avaliação do crédito e apresentada a administração para adjudicação. *- Controlado e Suportado por Auditorias Externas Anuais ao departamento Financeiro e* *- Processos associados à Politica Anticorrupção_Brighten*

Elaboração de reporte financeiro, preparação de demonstrações financeiras e consolidação	Manipulação das demonstrações financeiras, para a obtenção de benefícios alheios à Brighten	1	2	Baixo	Revisão analítica mensal às rubricas contabilísticas, e realização de comparações face ao orçamento, períodos anteriores e períodos homólogos; *- Monitorização e análise periódica a rubricas contabilísticas com maior propensão para manipulação e para registo de custos indevidos.*
	Manipulação das reconciliações bancárias para a obtenção de benefícios alheios à organização de modo a ocultar/modificar movimentos em contas bancárias que sejam suspeitos e/ou não sejam relacionados com a atividade da Brighten.	1	1	Muito Baixo	Revisão e aprovação das reconciliações bancárias por colaboradores diferentes (CFO/FINANCE MANAGE) e validadas por auditores externos.
Abertura e encerramento de contas bancárias	Desvio indevido de fundos por parte de colaboradores com poderes de movimentação de contas bancárias	1	1	Muito Baixo	Exigência de um mínimo de duas assinaturas (CFO/FINANCE MANAGER) para a abertura de contas bancárias e realização de pagamentos; *- Formalização e condução de procedimentos de abertura e encerramento de contas bancárias - Confronto periódico entre o mapa Base de Dados de Contas do Banco de Portugal, com as contas bancárias abertas na contabilidade*
Gestão de pagamentos e recebimentos incluindo Gestão de Cobranças	Desvio de fundos como forma de obter/conceder vantagem ilícita	2	2	Moderado	*- Existência de controlo em sistema que não permite o envio de faturas para pagamento sem que se verifique o cumprimento dos workflows de pedidos de compras e de aprovação de faturas e de conferência da receção de bens e/ou serviços; - Acesso restrito às credenciais de acesso às contas bancárias; - Realização periódica de reconciliações bancárias; - Realização de controlos de movimentos de caixa através de folhas de caixa / extrato bancário; - Aprovação prévia à atribuição de perfis de acesso aos sistemas com base nas funções desempenhadas e revisão periódica dos mesmos; - Acompanhamento periódico da conta corrente dos fornecedores e clientes com vista à regularização de saldos e análise de divergências.*

	Condicionamento de processos de financiamento através de omissão/ manipulação de informação, para benefício próprio e/ou de terceiros	1	1	Muito Baixo	Todas e quaisquer cobranças são feitas através do sistema onde é feito o registo das faturas e notas de créditos emitidas pela responsável faturação. O respectivo recebimento é registado pela contabilidade. *- O processo envolve vários intervenientes: (i) recebimento (entrada no banco) é comunicada à pessoa responsável pelas cobranças, (ii) é registado e confirmado e (iii) após validação retorna à area financeira para ser consolidado em sistema.* *- Auditorias Externas Anuais ao departamento Financeiro.*
Validação e reembolso de despesas apresentadas por colaboradores	Aprovação de despesas incorridas por colaboradores e elementos da gestão não documentadas, não enquadradas na atividade da Brighten e/ou cujo montante não seja apropriado tendo em conta a natureza da despesa	1	1	Muito Baixo	Despesas de colaboradores são analisadas e aprovadas com diferentes níveis de aprovação incluindo gestores de projeto e recursos humanos. *- Cumprimento de política de apresentação, aprovação e reembolso de despesas a colaboradores;* *- Existência de workflow de aprovação relativo à aprovação de despesas, envolvendo diversas áreas da organização* .
Contratação de fornecedores e subcontratação de terceiros	Contratações/subcontratações não aprovadas ou aprovadas com o nível de delegação de autoridade indevido	2	1	Baixo	*Obrigatoriedade de criação de requisições de compra e registo em sistema e com o preenchimento do âmbito da contratação (justificação de negocio) – aplicação do workflow de Fluxo de pedidos;*
	Elaboração e formalização de contratos com condições de pagamento e objetos contratuais ambíguos, dificultando a interpretação, fiscalização dos serviços e controlo dos pagamentos	1	1	Muito Baixo	*Obrigatoriedade de criação de requisições de compra e registo em sistema e com o preenchimento do âmbito da contratação (justificação de negocio) – aplicação do workflow de Fluxo de pedidos;* *- Envolvimento do jurídico no desenvolvimento de contratos*
	Recebimento de suborno/ vantagem indevida para seleção, contratação e/ou favorecimento de um fornecedor em detrimento de outro	1	1	Muito Baixo	Aplicação e cumprimento de política de compras e do workflow Fluxo Pedidos (Procurement), envolvendo diferentes níveis de aprovação.

Registo de pedidos de compra em sistema	Aquisição de bens que não decorram de reais necessidades para benefícios alheios à organização	1	1	Muito Baixo	Obrigatoriedade de criação de requisições de compras em sistema; - Aplicação e cumprimento de política de compras e do workflow Fluxo Pedidos (Procurement), envolvendo diferentes níveis de aprovação (gestores de projecto e pela direção financeira e administração)
	Fracionamento de compras/despesas, de forma a não serem ultrapassados os plafonds para a aprovação de compras definidos e/ou as delegações de autoridade para aprovação	1	1	Muito Baixo	Aplicação do workflow Fluxo Pedidos (Procurement), envolvendo diferentes níveis de aprovação (independentemente do valor dos serviços a contratar)

www.brightenconsulting.com