Partner
in Payments

Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Versão: 01.02

Data: 2026-01-21

Estado: Final

Classificação: Público

Referência: DCSIBS230261

Ficha Técnica

Referência:	DCSIBS230261
Título do Documento:	Plano de Prevenção de Riscos de Corrupção e Infrações Conexas
Versão:	01.02
Estado:	Final
Classificação:	Público
Área Funcional Responsável:	Compliance

Revisões

Versão	Data	Descrição	Autor
01.00	2023-06-30	Criação do documento.	SIBS
01.01	2023-12-06	Atualização classificação para “público”.	SIBS
01.02	2026-01-21	Atualização do plano de prevenção de riscos de corrupção e infrações conexas	ARC

Índice

Índice de Figuras

Índice de Tabelas

1 Enquadramento

Na sequência da aprovação da Estratégia Nacional Anticorrupção 2020-2024, foi criado através o Decreto-Lei n.º 109-E/2021, de 9 de dezembro, o Mecanismo Nacional Anticorrupção (MENAC), e o Regime Geral de Prevenção da Corrupção (RGPC), que se aplica a pessoas coletivas com sede em Portugal que empreguem 50 ou mais trabalhadores.

Dando cumprimento ao disposto no Decreto-Lei n. º109-E/2021, de 9 de dezembro, as empresas do Grupo SIBS adotam um Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPR) único, reconhecendo a importância e o valor deste instrumento de gestão na prevenção e no combate à corrupção e infrações conexas, e a utilidade na identificação e avaliação do risco associado, sendo, por isso, uma importante ferramenta no controlo e gestão do seu risco interno.

O presente Plano é aplicável ao Grupo SIBS, tendo como Responsável pelo Cumprimento Normativo (RCN) o *Head of Compliance*, que está contactável pelo e-mail compliance@sibs.pt. O RCN exerce as funções de modo independente, permanente e com autonomia decisória, dispondo da informação interna e dos meios humanos e técnicos necessários ao bom desempenho da sua função.

A SIBS possui um Código de Ética, recentemente revisto, que responde parcialmente às necessidades apresentadas pelo RGPC, e, consequentemente, ao PPR, o qual é de conhecimento obrigatório por parte de todos os colaboradores.

São abrangidos todos os colaboradores de todas as empresas do Grupo SIBS, pois, tal como foi referido *supra*, existe um PPR único, que é referente a toda a organização e atividade, incluindo áreas de administração, de direção, operacionais ou de suporte das entidades do Grupo.

2 O Grupo SIBS

A SIBS é uma *holding* tecnológica que disponibiliza uma multiplicidade de serviços financeiros através do desenvolvimento e gestão de soluções de pagamento, processamento, segurança, *business process outsourcing* e de produção e personalização de cartões.

Foi a primeira *fintech* a surgir em Portugal, há quatro décadas atrás, sendo hoje uma das maiores e mais completas em toda a cadeira de valor da indústria de pagamentos. Neste momento, a SIBS oferece serviços a mais de 300 milhões de utilizadores, dispersos em 20 países e 3 continentes.

A SIBS é a empresa responsável pela gestão das Redes ATM Express e Multibanco, estabeleceu-se como um dos principais processadores e pagamentos na Europa e presta serviços na área de prevenção, deteção e investigação de fraude.

Em 2015 foi criado o MB WAY, o MULTIBANCO no telemóvel, que permite hoje, a cerca de 5 milhões de utilizadores, fazer compras físicas e online, transferências imediatas e levantamentos, entre outras operações, utilizando apenas o *smartphone*.

De forma empenhada e constante, a SIBS prossegue a sua missão de ser o parceiro de referência de entidades públicas e privadas, criando valor para a sociedade, através do desenvolvimento e gestão de soluções de pagamento, processos e serviços conexos baseados em tecnologia que combinem segurança, conveniência e inovação, respeitando os bons princípios comportamentais e as condições de sustentabilidade.

Esta oferta é disponibilizada pelas empresas que compõem o Grupo:

- A SIBS SGPS, a *holding* do Grupo responsável pela gestão de várias participadas, empresas especializadas em áreas de serviços críticas que atuam essencialmente no setor de pagamentos;
- A SIBS FPS, a empresa responsável pelo processamento e soluções de pagamento;
- A SIBS Pagamentos, que é uma instituição de pagamento licenciada e regulamentada pelo Banco de Portugal;
- A SIBS MB, que gere a marca MB e sistema de pagamentos europeu MB;
- A SIBS Cartões, a empresa que disponibiliza um serviço especializado na área de produção e personalização de cartões e atividades complementares;
- A SIBS Processos, que tem como objetivo a conceção, implementação e gestão de soluções de *Business Process Outsourcing (BPO)* através do desenvolvimento de tecnologias inovadoras e soluções de otimização para fazer face aos desafios do processamento intensivo, proporcionando mais eficiência aos clientes;
- A SIBS International, a empresa do Grupo que exporta o *know-how* adquirido ao longo dos anos, através da oferta de soluções de pagamento inovadoras, seguras e flexíveis nos mercados internacionais;
- A Multicert, que tem consolidado o seu posicionamento no desenvolvimento de várias soluções na área de Cibersegurança, Certificados Digitais, Soluções Avançadas de Identificação Eletrónica, Gestão de Informação e Soluções de Voto Eletrónico;
- A SIBS Gest, que gere os serviços partilhados e o património do Grupo;
- A SIBS Romania, a empresa líder no processamento de operações com cartões na Roménia;
- A PayTel, um fornecedor de serviços de pagamentos eletrónicos na Polónia, que oferece soluções direcionadas a pequenos e médios comerciantes;
- As empresas Kar-tel I e II, duas Instituições de Pagamento que disponibilizam terminais de pagamento automático e diversos serviços adicionais para comerciantes;
- A DeFinancy, que se dedica ao desenvolvimento de soluções e gestão de ativos virtuais.

3 Metodologia de gestão de riscos de Corrupção e Infrações Conexas

3.1 Princípios basilares

No Grupo SIBS, a Gestão de Risco é um elemento central no conjunto de instrumentos para a gestão estratégica da organização, que deve proporcionar:

- Uma visão de conjunto dos riscos da organização no momento presente;
- Uma antecipação da sua situação num cenário futuro;
- A adoção de processos consistentes que contribuam para que o risco seja gerido de forma eficiente, eficaz e coerente em toda a organização.

Uma Gestão de Risco eficiente, eficaz e coerente poderá assim permitir à organização aumentar a verosimilhança de atingir os seus objetivos, desenvolvendo uma gestão mais proactiva, que permita:

- Garantir o foco na identificação de oportunidades e ameaças de forma sistemática;
- Melhorar a governação, estabelecendo uma base fiável para a tomada de decisões e planeamento, alinhada com o perfil e apetite pelo risco da organização;
- Melhorar a eficiência e eficácia operacionais, afetando os recursos proporcionados no tratamento do risco de forma eficaz, aperfeiçoando a prevenção de perdas e a gestão de incidentes, minimizando umas e outros e, como corolário, incrementando a resiliência organizacional;
- Garantir o cumprimento das obrigações legais e regulamentares e normas internacionais aplicáveis;
- Monitorizar eficazmente o perfil de risco da organização, através do acompanhamento de indicadores de risco definidos em conjunto com as unidades geradoras de riscos, inerentes à atividade e objetos da organização;
- Aumentar a confiança das partes interessadas e a credibilidade geral da organização.

3.2 Modelo de governo da Gestão de Risco

A Gestão de Risco do Grupo SIBS é da responsabilidade da Comissão Executiva da SIBS SGPS, a *holding* do Grupo SIBS, a qual delega na Área Funcional Gestão de Risco, com funções transversais para as empresas do Grupo SIBS, o acompanhamento e cumprimento dos processos aprovados no "Manual de Gestão de Risco do Grupo SIBS", tendo como pressuposto básico uma intervenção ativa da Gestão de Risco junto dos diversos interlocutores relevantes, nomeadamente interagindo na

gestão e controlo dos diversos riscos com os Responsáveis de UE e com todos os colaboradores que por estes forem designados como Donos de Risco.

Tais processos conduzem ao seguinte Modelo de Governação da Gestão de Risco no Grupo SIBS:

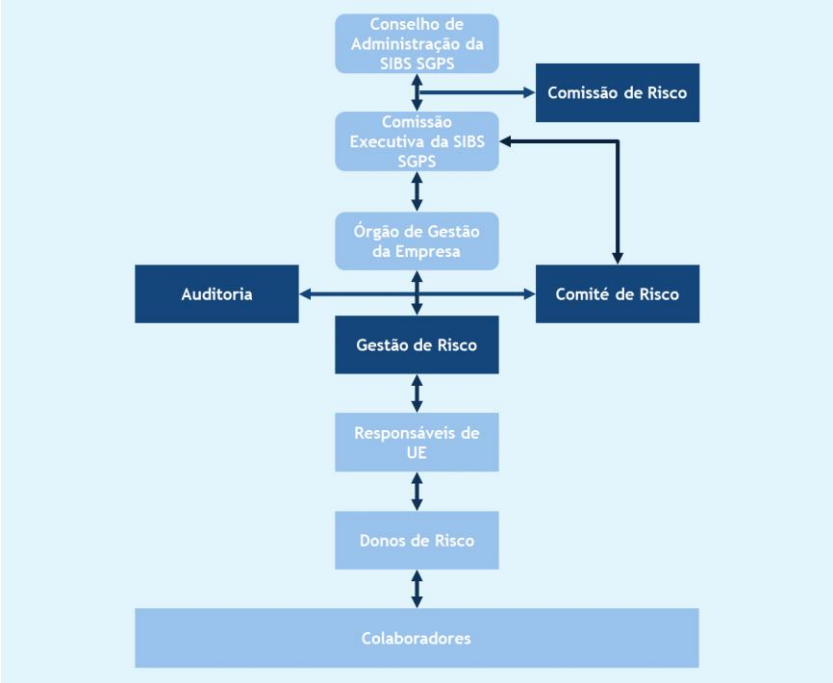


Figura 1 - Modelo de Governação da Gestão de Risco do Grupo SIBS

A missão e responsabilidades que são inerentes a cada área estão descritas em documento interno próprio para o efeito, a "Política de Gestão de Risco do Grupo SIBS".

3.3 Ciclo da Gestão de Risco

Uma Gestão de Risco que proteja e acrescente valor à organização exige uma efetiva e exata definição de responsabilidades, suportadas em processos claros e eficientes. Nesse sentido, no Grupo SIBS é desenvolvido um Ciclo de Gestão de Risco, composto por seis etapas principais, assentes numa indispensável comunicação transversal com todos os intervenientes nos diversos processos, e identificando claramente as responsabilidades de todos os intervenientes e as tarefas que lhes são, por conseguinte, inerentes e que garantem que a estratégia definida para a Gestão de Risco é atingida da forma e no momento planeado, porque são anulados ou, pelo menos, minimizados os efeitos perversos das ameaças que sobre ela impendem.

De forma ilustrativa, temos então o seguinte *workflow* do Ciclo de Gestão de Risco, alinhado com a Norma ISO 31000 e outras boas práticas internacionais:

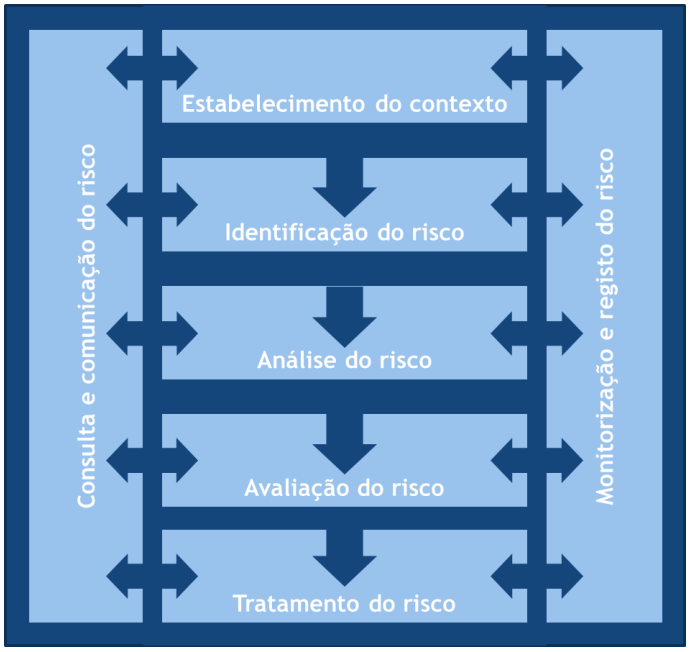


Figura 2 – Ciclo da Gestão de Risco no Grupo SIBS

Tal Ciclo de Gestão de Risco, bem como os processos e procedimentos que dão corpo ao seu estrito cumprimento, estão detalhados em documento interno próprio para o efeito, o "Manual de Gestão de Risco do Grupo SIBS".

3.4 Análise e avaliação dos riscos

Para avaliação dos riscos associados à Corrupção e Infrações Conexas o Grupo SIBS utiliza os critérios de risco, definidos e aprovados através do "Manual de Gestão de Risco do Grupo SIBS", que são transversais a todas as empresas que o compõem.

A Probabilidade é estimada tendo em consideração a seguinte tabela de possibilidades:

Tabela 1 – Probabilidade estimada

Probabilidade	Descrição
1 – Altamente improvável	O risco existe, mas apenas se pode materializar em situações raras ou em condições excecionais.
2 - Improvável	O risco não é frequente e é improvável que o evento aconteça num período de 2 anos.
3 - Provável	O risco pode materializar-se com alguma frequência, podendo ocorrer pelo menos uma vez nos próximos 2 anos.
4 – Altamente provável	O risco pode materializar-se com frequência, isto é, pode existir uma ou mais ocorrências nos próximos 12 meses.

O Impacto de um dado evento de risco é calculado de acordo com a grelha de fatores presente no quadro seguinte:

Tabela 2 – Impacto estimado

Impacto	Financeiro (F)	Serviço (S)	Reputação (R)	Regulação (C)
1 – Baixo	Perda de valor no negócio ou penalizações consideradas reduzidas. Valor inferior a 2,5% dos proveitos operacionais da empresa no ano anterior.	Indisponibilidade reduzida do Serviço. É possível assegurar pelo menos 95% do serviço sem falhas ou atrasos. Sem disrupções para o cliente ou para terceiros.	Sem cobertura negativa nos média e/ou sem reclamações de clientes, resultando em impacto momentâneo e com dano temporário.	Impacto reduzido internalizado.
2 - Médio	Perda de valor no negócio ou penalizações consideradas moderadas. Valor superior a 2,5%, mas inferior a 5% dos proveitos operacionais da empresa no ano anterior.	indisponibilidade moderada do Serviço. É possível assegurar pelo menos 90% do serviço sem falhas ou atrasos. Disrupções sem efeitos no negócio do cliente ou de terceiros.	Cobertura negativa nos média por período reduzido e/ou reclamações de poucos clientes, sem pedidos de indemnização, resultando em dano para a reputação apenas no curto prazo.	Infração moderada, resultando em possíveis sanções ao negócio.
3 -Alto	Perda de valor no negócio ou penalizações consideradas graves. Valor superior a 5%, mas inferior ou igual a 10% dos proveitos operacionais da empresa no ano anterior.	Indisponibilidade grave do Serviço. É possível assegurar pelo menos 85% do serviço sem falhas ou atrasos. Disrupções com efeitos graves no negócio do cliente ou de terceiros.	Cobertura negativa nos média a nível nacional e/ou reclamação de vários clientes, com eventuais pedidos de indemnização, resultando em dano para a reputação no curto/médio prazo.	Infração grave, resultando em sanções ao negócio.
4 – Muito alto	Perda de valor no negócio ou penalizações consideradas muito graves. Valor superior a 10% dos proveitos operacionais da empresa no ano anterior.	Indisponibilidade muito grave do Serviço. É impossível assegurar 85% do serviço sem falhas ou atrasos. Disrupções com efeitos muito graves no negócio do cliente ou de terceiros.	Cobertura muito negativa nos média a nível nacional e/ou reclamação de todos os clientes, com múltiplos pedidos de indemnização, resultando em danos permanentes.	Infração muito grave, resultando em suspensão ou proibição do negócio.

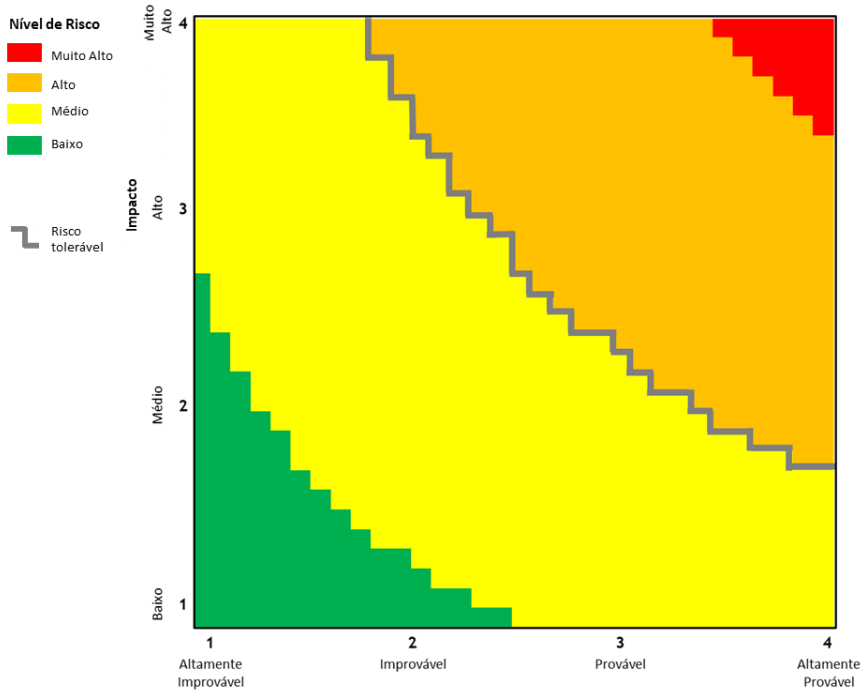
O nível de Impacto final resulta do valor máximo do conjunto de fatores, ou seja, Impacto = MAX (F, S, R, C).

O Nível de Risco estimado é atribuído de acordo com a tabela seguinte:

Tabela 3 - Nível de Risco estimado

Nível de Risco	Descrição
1 – Baixo	Impacto x Probabilidade = 1, 2
2 - Médio	Impacto x Probabilidade = 3, 4, 6
3 -Alto	Impacto x Probabilidade = 8, 9, 12
4 – Muito alto	Impacto x Probabilidade = 16

Os critérios de risco assim definidos, conduzem a um modelo de Matriz de Risco que pode ser ilustrado da seguinte forma:



3.5 Tratamento dos riscos

Os riscos de Corrupção e Infrações Conexas, após identificados e avaliados, são alvo do tratamento que se considere o mais adequado. Conforme descrito no "Manual de Gestão de Risco do Grupo SIBS, o tratamento do risco consiste na seleção e implementação de uma ou mais opções para modificar os riscos cujo Nível de Risco Residual exceda o Nível de Risco Tolerável na empresa, com o objetivo de os posicionar em nível igual, ou inferior ao tolerável e aumentar assim a verossimilhança da empresa atingir os objetivos estabelecidos. Tais opções de tratamento são denominadas por medidas corretivas. Uma vez implementadas, as medidas corretivas proporcionam novos controlos para o risco ou modificam controlos já existentes, tornando-os mais eficazes ou eficientes.

As opções de tratamento do risco não passam, contudo, apenas por controlar o risco através de novos ou mais eficazes controlos, podendo ainda consubstanciar-se em transferir, evitar ou aceitar os riscos identificados.

As opções de tratamento do risco utilizadas são então:

- Controlar o risco: implementar novos controlos, ou aprofundar os controlos já existentes de forma a conduzir o risco para níveis toleráveis.
- Transferir o risco: assegurar que o risco é assumido ou gerido por outrem através, por exemplo, da contratualização de seguros ou do *outsourcing* de serviços.
- Evitar o risco: não iniciar ou continuar a atividade portadora do risco, ou planear essa atividade de forma a que se recorra o menor número possível de vezes a situações geradoras do risco.
- Aceitar o risco: considerar que o risco, mesmo excedendo o nível de tolerância definido, é aceitável face aos objetivos estabelecidos.

As anteriores opções não têm de ser mutuamente exclusivas ou apropriadas em todas as circunstâncias, pelo que se torna essencial selecionar cuidadosamente quais as mais adequadas para cada risco em concreto, comparando os custos e os esforços da sua implementação com os benefícios resultantes e tendo ainda em consideração os requisitos legais, regulamentares e outros que as condicionem.

Em termos esquemáticos, temos as seguintes possibilidades de tratamento de um risco que exceda o Nível de Risco Tolerável na empresa:

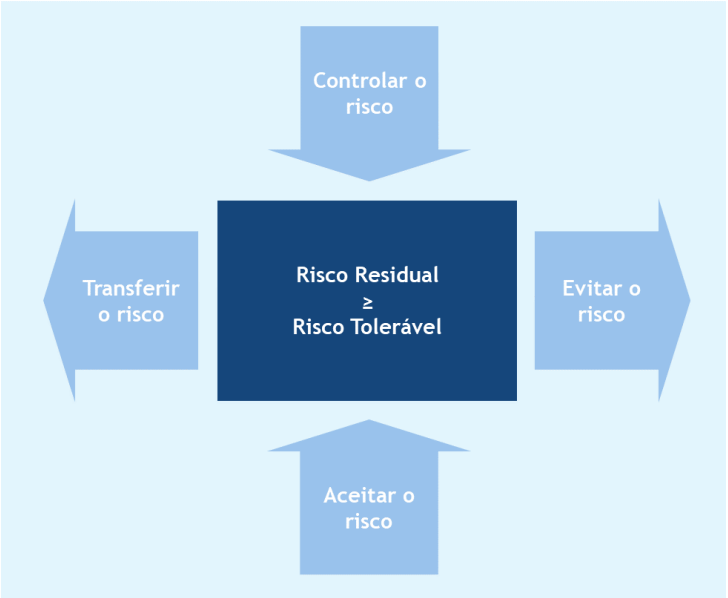


Figura 3 - Tratamento do risco

3.6 Monitorização dos riscos

A monitorização dos Riscos de Corrupção e Infrações Conexas, conforme descrito no "Manual de Gestão de Risco do Grupo SIBS" é um processo de controlo, verificação e vigilância regular dos diversos riscos identificados, analisados e avaliados, através da avaliação dos eventos de risco que, entretanto, se vão materializando, identificados pelos responsáveis operacionais, pela Gestão de Risco, ou pela Auditoria Interna.

O processo de monitorização é constante, procedendo-se ao acompanhamento recorrente das situações de risco materializadas, com o objetivo de:

- Assegurar que os controlos existentes são eficazes;
- Obter informação adicional para melhorar a apreciação do risco, analisando e aprendendo com os eventos, mudanças, tendências, sucessos e falhas e estabelecendo padrões transversais que permitam avaliar necessidades de atuação concreta para dirimir riscos futuros.
- Detetar alterações ao contexto, incluindo alterações necessárias aos critérios presentes no modelo de identificação, análise e avaliação de risco descrito nos pontos anteriores.

Os resultados da monitorização são registados (de forma automática ou manual, dependendo dos tipos de risco e sistemas de alarmística implementados), procurando garantir o acompanhamento eficiente e eficaz de todas as situações de risco, potenciando um processo de aprendizagem contínua da empresa e uma base sólida para a melhoria dos métodos e das ferramentas de gestão de risco.

Em termos esquemáticos temos o seguinte *workflow* para a monitorização e registo do risco:

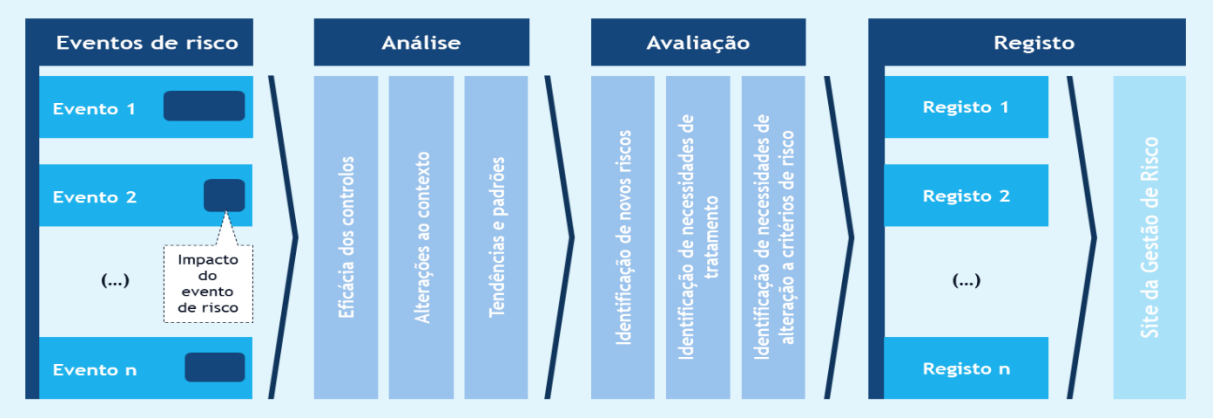


Figura 4 – *Workflow* da monitorização e registo dos riscos

4 Riscos de Corrupção e Infrações Conexas no Grupo SIBS

Seguindo a metodologia descrita no ponto 3, foram mapeados no Grupo SIBS os principais riscos de Corrupção e infrações Conexas, tendo em consideração as atividades/processos onde estes se podem materializar. Neste contexto, foram identificados os seguintes riscos potenciais:

A. Apropriação indevida de ativos imateriais
B. Aquisição de bens/serviços desnecessários ou sobrevalorizados
C. Fraude Informática
D. Falsificação, danificação, ou subtração de documentação
E. Falta de isenção e imparcialidade
F. Utilização indevida de bens da empresa
G. Favorecimento de entidades externas por troca de vantagens/benefícios
H. Pagamentos indevidos
I. Recebimentos indevidos
J. Utilização/Divulgação de informação privilegiada/confidencial
K. Atribuição de acessos indevidos
L. Acesso indevido ao edifício
M. Remoção atempada dos acessos
N. Atribuição de acessos a colaboradores externos
O. Eliminação de informação registada em sistema

Tais riscos podem materializar-se, especialmente, nas seguintes atividades/processos:

Tabela 4 – Atividades geradores de riscos de corrupção e infrações conexas

Atividade	Descrição
Gestão de Fornecedores	Inclui compras de equipamento, matérias primas e material de suporte à atividade, bem como a contratação de serviços externos/internos em regime de outsourcing
Gestão de Clientes	Inclui a gestão corrente de clientes, de reclamações, de incidentes e de pedidos de serviços
Gestão financeira	Inclui a gestão da tesouraria e contabilidade, o processamento salarial, a orçamentação, o controlo e *reporting* financeiro
Gestão de Recursos Humanos	Inclui recrutamento (interno e externo) e a gestão do ciclo de vida do colaborador na empresa

Atividade	Descrição
Gestão de Ativos	Inclui a gestão do património material (Edifícios, bens afetos ao serviço, materiais, peças, consumíveis, etc.) e imaterial (propriedade intelectual) da empresa
Gestão de Relações Institucionais	Inclui a gestão da relação com acionistas, investidores, parceiros em investimentos (M&A), Estado, entidades reguladoras e supervisores e demais entidades externas à empresa que não sejam clientes ou fornecedores
Gestão do Controlo Interno	Inclui todas as atividade e processos que estão subjacentes ao desempenho das responsabilidades atribuídas à Gestão de Risco, Compliance e Auditoria
Gestão da Segurança	Inclui as atividades que se destinam a proteger a segurança e cibersegurança dos serviços prestados e os ativos de informação residentes na SIBS necessários a tal prestação de serviços

Da avaliação da conjugação dos 12 riscos identificados com as 8 atividades/processos em que estes se podem materializar, resultaram 23 ameaças, com os seguintes resultados que seguidamente destacamos:

- Não se detetaram quaisquer riscos inerentes com Nível de Risco "Muito Alto";
- Todos os riscos possuem as mitigações e controlos considerados necessários e suficientes para a sua devida contenção para níveis toleráveis na organização;
- Todos os riscos residuais se encontram contidos em níveis iguais ou inferiores ao nível de risco tolerável no Grupo SIBS (≤Médio).

Numa visão esquemática, podemos ver o posicionamento dos principais riscos em termos inerentes e residuais:

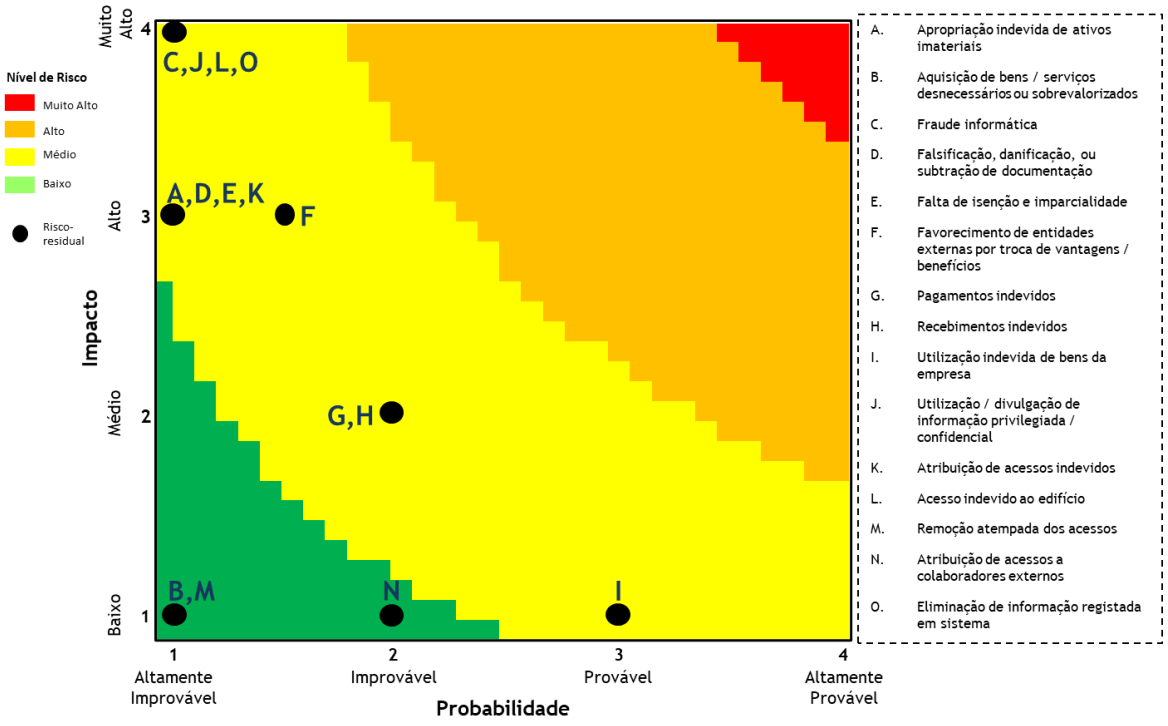


Figura 5 - Matriz de riscos inerentes e residuais

Tendo em consideração as principais atividades/processos onde os riscos se podem materializar, temos o seguinte panorama em termos de risco residual, o qual pode ser consultado em maior detalhe no Anexo 1 deste documento:

Risco	Gestão de Fornecedores	Gestão de Clientes	Gestão financeira	Gestão de Recursos Humanos	Gestão de Ativos	Gestão de Relações Institucionais	Gestão do Controlo Interno	Gestão da Segurança
Apropriação indevida de ativos imateriais					Médio			
Aquisição de bens/serviços desnecessários ou sobrevalorizados					Baixo			
Fraude informática								Médio
Falsificação, danificação, ou subtração de documentação			Baixo				Médio	
Falta de isenção e imparcialidade							Médio	
Favorecimento de entidades externas por troca de vantagens/benefícios	Médio	Médio				Médio		
Pagamentos indevidos			Médio					
Recebimentos indevidos			Médio					
Utilização indevida de bens da empresa					Baixo			
Utilização/Divulgação de informação privilegiada/confidencial	Médio	Médio	Baixo	Médio	Médio	Médio		
Atribuição de acessos indevidos	Médio	Médio	Médio	Baixo	Médio	Médio		Médio
Acesso indevido ao edifício	Médio	Médio	Médio	Médio	Médio	Médio		Médio
Remoção atempada dos acessos					Baixo			
Atribuição de acessos a colaboradores externos								Baixo
Eliminação de informação registada em sistema								Médio

Nível de Risco

Muito Alto | Alto | Médio | Baixo

Figura 6 - Matriz de riscos residuais por atividade

5 Participação de irregularidades

Para prosseguir com a conformidade normativa consoante o RGPC, a SIBS criou um canal de denúncias interno, que dá seguimento a denúncias de atos de corrupção e infrações conexas, sendo que a SIBS responde pelas contraordenações previstas.

As participações enquadradas no âmbito deste Plano podem ser comunicadas através do mail denuncia@sibs.com, tal como referido no Código de Ética do Grupo SIBS, disponível em www.sibs.com.

É mantido um registo detalhado, por local e por natureza, de todas as reclamações, denúncias e ocorrências anómalas referidas, de forma a facilitar a monitorização e prevenção de potenciais atividades ilícitas.

A SIBS mantém uma rígida política de não-retaliação, que não permite que nenhum colaborador sofra, em termos profissionais ou pessoais, por assinalar qualquer problema que ache relevante e possa colocar em causa a conformidade com este Plano.

6 Programa de Formação

Para efeitos do cumprimento com os requisitos estabelecidos no RGPC e fomentação de uma cultura interna de prevenção e combate à corrupção e infrações conexas, a SIBS disponibiliza aos seus colaboradores programas específicos de formação Anticorrupção, com vista a que estes conheçam e compreendam as políticas e procedimentos de prevenção de corrupção e infrações conexas implementados.

7 Monitorização do PPR

A monitorização do PPR é algo imprescindível devido à natureza do mesmo. O PPR funciona como ferramenta de mitigação e identificação de riscos, os quais estão sempre a surgir e a variar em gravidade consoante a atividade da SIBS.

Desta forma, o RCN tem diferentes funções de monitorização para poder manter o PPR atualizado e eficaz. São estas:

- A elaboração, no mês de outubro, de um relatório de avaliação intercalar nas situações de risco com níveis “Alto” ou “Muito alto”, assim como o estado de concretização das medidas de mitigação identificadas como necessárias implementar;
- A elaboração, em abril do ano seguinte a que respeita a execução, de um relatório de avaliação anual, que contenha a qualificação do grau de implementação das medidas de mitigação, sendo preventivas ou corretivas, identificadas, bem como a previsão da sua plena implementação;

- Outras ações de monitorizações que se justifiquem, sempre que se identifiquem riscos com níveis elevados.

8 Vigência, Revisão e Publicidade

O PPR é obrigatoriamente revisto a cada 3 anos. Tal revisão também poderá ocorrer sempre que se opere uma alteração nas atribuições ou na estrutura orgânica/societária da SIBS que a justifique.

O PPR é divulgado na *intranet* da SIBS e na página oficial da *internet* da SIBS no prazo de 10 dias contados desde a sua implementação e respetivas revisões ou elaboração. O mesmo processo de divulgação ocorre com os relatórios de avaliação consequentes da monitorização do PPR.

Anexo A. Avaliação de Risco

A.1. Mapa de riscos

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Apropriação indevida de ativos imateriais	Apropriação indevida de ativos de propriedade intelectual da empresa e sua utilização/divulgação com danos para a mesma	Gestão de Ativos	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Gestão e Comunicação de Documentos	3	1	Médio
Aquisição de bens / serviços desnecessários ou sobrevalorizados	Aquisição de serviços que excedem as necessidades reais ou com preços sobredimensionados em contrapartida de uma benefício/vantagem	Gestão de Ativos	1	2	Baixo	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Qualidade - Processo de Compras • Manual de Procedimentos - Gestão de Ativos • Delegação de competências	1	1	Baixo
Fraude Informática	Interferência no tratamento de dados, estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização, ou intervenção por qualquer outro modo não autorizada no processamento com intenção de obter para si ou para terceiro enriquecimento ilegítimo, ou causar a outra pessoa prejuízo patrimonial	Gestão da Segurança	4	2	Alto	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • PCI DSS Charter • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	4	1	Médio
Falsificação, danificação, ou subtração de documentação	Falsificação, danificação ou subtração intencional de documento com intenção de causar prejuízo à empresa ou a outra pessoa, ou de obter para si ou para outra pessoa benefício ilegítimo	Gestão Financeira	2	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Pagamento de Despesas	2	1	Baixo

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Falsificação, danificação, ou subtração de documentação	Falsificação, danificação ou subtração intencional de documento com intenção de causar prejuízo à empresa ou a outra pessoa, ou de obter para si ou para outra pessoa benefício ilegítimo	Gestão do Controlo Interno	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Regulamento de Auditoria Interna • Política de Gestão de Risco do Grupo SIBS • Manual de Gestão de Risco do Grupo SIBS • Política de Compliance do Grupo SIBS • Manual de Compliance do Grupo SIBS	3	1	Médio
Falta de isenção e imparcialidade	Reporte inadequado, incorreto, ou omisso de desconformidades por parte dos órgãos de Controlo Interno, influenciados por interesses específicos que afetam a isenção e imparcialidade	Gestão do Controlo Interno	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento de Auditoria Interna • Política de Gestão de Risco do Grupo SIBS • Manual de Gestão de Risco do Grupo SIBS • Política de Compliance do Grupo SIBS • Manual de Compliance do Grupo SIBS	3	1	Médio
Favorecimento de entidades externas	Aceitação de favorecimento por parte de entidades externas em troca de concessão de vantagens ou benefícios	Gestão de Fornecedores	3	3	Alto	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Qualidade - Processo de Compras • Delegação de competências	3	2	Médio
Favorecimento de entidades externas	Aceitação de favorecimento por parte de entidades externas em troca de concessão de vantagens ou benefícios	Gestão de Clientes	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Procedimento de Gestão do Tarifário e do Preçário • Delegação de competências	3	1	Médio
Favorecimento de entidades externas	Aceitação de favorecimento por parte de entidades externas em troca de concessão de vantagens ou benefícios	Gestão de Relações Institucionais	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Delegação de competências	3	1	Médio
Pagamentos indevidos	Realização de pagamentos indevidos em detrimento/benefício de interesses específicos ou para benefício próprio ou de terceiro	Gestão Financeira	3	3	Alto	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Processo de Tesouraria e Contabilidade • Política de Pagamento de Despesas • Delegação de competências	3	2	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Recebimentos indevidos	Manipulação da atividade dos recebimentos em benefício próprio ou de terceiros	Gestão Financeira	3	3	Alto	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Processo de Tesouraria e Contabilidade • Delegação de competências	3	2	Médio
Utilização indevida de bens da empresa	Utilização não autorizada de bens da empresa (bens afetos ao serviço, materiais, peças, consumíveis, etc.) com danos financeiros para a mesma	Gestão de Ativos	1	4	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Manual de Procedimentos - Gestão de Ativos	1	2	Baixo
Utilização / Divulgação de informação privilegiada / confidencial	Obtenção de benefícios particulares ou criação de prejuízos à empresa ou a terceiros por divulgação não autorizada de informação privilegiada / confidencial	Gestão de Fornecedores	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Segredo Profissional e Procedimentos versus Autoridades nesse âmbito • Política de Qualidade - Processo de Compras • Normativo orientador e procedimental sobre “Acordos de Confidencialidade” • Regulamento Interno de Proteção de Dados do Grupo SIBS • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Utilização / Divulgação de informação privilegiada / confidencial	Obtenção de benefícios particulares ou criação de prejuízos à empresa ou a terceiros por divulgação não autorizada de informação privilegiada / confidencial	Gestão de Clientes	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Segredo Profissional e Procedimentos versus Autoridades nesse âmbito • Normativo orientador e procedimental sobre "Acordos de Confidencialidade" • Princípios Normativos da Divulgação de Informação a Clientes • Regulamento Interno de Proteção de Dados do Grupo SIBS • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Utilização / Divulgação de informação privilegiada / confidencial	Obtenção de benefícios particulares ou criação de prejuízos à empresa ou a terceiros por divulgação não autorizada de informação privilegiada / confidencial	Gestão Financeira	2	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Segredo Profissional e Procedimentos versus Autoridades nesse âmbito • Normativo orientador e procedimental sobre "Acordos de Confidencialidade" • Princípios Normativos da Divulgação de Informação a Clientes • Regulamento Interno de Proteção de Dados do Grupo SIBS • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	2	1	Baixo

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Utilização / Divulgação de informação privilegiada / confidencial	Obtenção de benefícios particulares ou criação de prejuízos à empresa ou a terceiros por divulgação não autorizada de informação privilegiada / confidencial	Gestão de RH	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Segredo Profissional e Procedimentos versus Autoridades nesse âmbito • Regulamento Interno de Proteção de Dados do Grupo SIBS • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Utilização / Divulgação de informação privilegiada / confidencial	Obtenção de benefícios particulares ou criação de prejuízos à empresa ou a terceiros por divulgação não autorizada de informação privilegiada / confidencial	Gestão de Relações Institucionais	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Segredo Profissional e Procedimentos versus Autoridades nesse âmbito • Política de Qualidade - Processo de Compras • Normativo orientador e procedimental sobre "Acordos de Confidencialidade" • Princípios Normativos da Divulgação de Informação a Clientes • Regulamento Interno de Proteção de Dados do Grupo SIBS • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Utilização / Divulgação de informação privilegiada / confidencial	Obtenção de benefícios particulares ou criação de prejuízos à empresa ou a terceiros por divulgação não autorizada de informação privilegiada / confidencial	Gestão de Ativos	3	2	Médio	• Código de Ética do Grupo SIBS • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Segredo Profissional e Procedimentos versus Autoridades nesse âmbito • Política de Qualidade - Processo de Compras • Manual de Procedimentos - Gestão de Ativos • Normativo orientador e procedimental sobre "Acordos de Confidencialidade" • Regulamento Interno de Proteção de Dados do Grupo SIBS • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos indevidos	Atribuição de acessos, tanto a sistemas como ao edifício, a colaboradores que não necessitam desses mesmos acessos para a realização das suas atividades diárias	Gestão de Fornecedores	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos indevidos	Atribuição de acessos, tanto a sistemas como ao edifício, a colaboradores que não necessitam desses mesmos acessos para a realização das suas atividades diárias	Gestão de Clientes	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos indevidos	Atribuição de acessos, tanto a sistemas como ao edifício, a colaboradores que não necessitam desses mesmos acessos para a realização das suas atividades diárias	Gestão Financeira	3	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos indevidos	Atribuição de acessos, tanto a sistemas como ao edifício, a colaboradores que não necessitam desses mesmos acessos para a realização das suas atividades diárias	Gestão de RH	3	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	2	1	Baixo

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos indevidos	Atribuição de acessos, tanto a sistemas como ao edifício, a colaboradores que não necessitam desses mesmos acessos para a realização das suas atividades diárias	Gestão de Relações Institucionais	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos indevidos	Atribuição de acessos, tanto a sistemas como ao edifício, a colaboradores que não necessitam desses mesmos acessos para a realização das suas atividades diárias	Gestão de Ativos	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos indevidos	Atribuição de acessos, tanto a sistemas como ao edifício, a colaboradores que não necessitam desses mesmos acessos para a realização das suas atividades diárias	Gestão da Segurança	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Acesso indevido ao edifício	Acesso a determinadas zonas restritas do Grupo SIBS, tanto por parte de colaboradores internos e externos, que permitam ter acesso a informação privilegiada	Gestão de Fornecedores	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Acesso indevido ao edifício	Acesso a determinadas zonas restritas do Grupo SIBS, tanto por parte de colaboradores internos e externos, que permitam ter acesso a informação privilegiada	Gestão de Clientes	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Acesso indevido ao edifício	Acesso a determinadas zonas restritas do Grupo SIBS, tanto por parte de colaboradores internos e externos, que permitam ter acesso a informação privilegiada	Gestão Financeira	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Acesso indevido ao edifício	Acesso a determinadas zonas restritas do Grupo SIBS, tanto por parte de colaboradores internos e externos, que permitam ter acesso a informação privilegiada	Gestão de RH	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Acesso indevido ao edifício	Acesso a determinadas zonas restritas do Grupo SIBS, tanto por parte de colaboradores internos e externos, que permitam ter acesso a informação privilegiada	Gestão de Relações Institucionais	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Acesso indevido ao edifício	Acesso a determinadas zonas restritas do Grupo SIBS, tanto por parte de colaboradores internos e externos, que permitam ter acesso a informação privilegiada	Gestão de Ativos	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Acesso indevido ao edifício	Acesso a determinadas zonas restritas do Grupo SIBS, tanto por parte de colaboradores internos e externos, que permitam ter acesso a informação privilegiada	Gestão da Segurança	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação	3	1	Médio

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Remoção atempada dos acessos	Eliminação de acessos de forma tardia, permitindo ao colaborador, que se encontra de saída, acesso a informação que poderá utilizar para benefício próprio	Gestão de Ativos	2	1	Baixo	• Código de Ética e de Conduta do Grupo • Política de Segurança de Informação – Pessoal • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	1	1	Baixo

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Atribuição de acessos a colaboradores externos	Possível existência de colaboradores externos como administradores de sistemas aplicacionais	Gestão da Segurança	1	2	Baixo	• Código de Ética e de Conduta do Grupo • Política de Segurança de Informação – Pessoal • Regulamento Interno de Proteção de Dados do Grupo • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Gestão de Acessos Lógicos • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	1	1	Baixo

Risco	Descrição	Atividade afetada pelo risco	I	P	Risco Inerente	Mitigação e controlos	I	P	Risco Residual
Eliminação de informação registada em sistema	Possibilidade de eliminação de "*logs* de *logs*" em sistema, permitindo assim que possíveis extrações ou acessos não fiquem registados	Gestão da Segurança	4	1	Médio	• Código de Ética e de Conduta do Grupo • Plano de Prevenção de Riscos de Corrupção e Infrações Conexas • Política de Segurança de Informação – Pessoal • Certificação PCI-DSS • Política de Segurança - Controlo de Acessos a Informação e Sistemas • Norma de Segurança - Gestão de Acessos Lógicos • Manual de Segurança de Informação • Sistema de Gestão de Segurança de Informação - Princípios Gerais • Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas	3	1	Médio

A.2. Mitigações e controlos

- Normativo Orientador e Procedimental sobre Contratos - descrição de passos e procedimentos a observar nas boas práticas da gestão jurídico-contratual do Grupo SIBS
- Regulamento de Auditoria Interna - Este regulamento descreve a missão, independência e objetividade, âmbito e responsabilidades, autoridade e regulamentos da função de Auditoria Interna
- PCI DSS Charter - Programa de Conformidade PCI DSS - A Comissão Executiva da SIBS FPS, está empenhada na preservação da confidencialidade, integridade e disponibilidade de toda a informação física ou eletrónica existente na organização de forma a cumprir com os requisitos PCI-DSS. Neste sentido define o presente PCI Charter com os seguintes objetivos: • Atribuir a autoridade e definir as responsabilidades dentro da organização, individuais e das unidades de negócio, na manutenção da conformidade PCI-DSS; • Dar visibilidade à Comissão Executiva sobre o cumprimento do programa de conformidade PCI-DSS; • Assegurar a informação necessária à Comissão Executiva contribuindo para a definição das prioridades estratégicas; • Assegurar a supervisão e acompanhamento da execução do plano de conformidade PCI-DSS.
- Código de Ética do Grupo SIBS - O Código de Ética do Grupo SIBS pretende clarificar, recordar e divulgar um conjunto de normas de conduta e informações complementares que sirvam de instrumento orientador ao desenvolvimento das atividades internas da organização. 1 Por SIBS entenda-se qualquer empresa do Grupo. 2 Entenda-se por colaboradores da SIBS, neste contexto, os membros dos órgãos de administração, e os colaboradores internos e externos de qualquer uma das empresas do Grupo SIBS. Este Código visa atingir os seguintes objetivos: • Formalizar os padrões de comportamento expectáveis dos colaboradores no exercício das suas funções, assegurando a sua compatibilidade e coerência com os valores da SIBS. • Promover a interiorização e o crescimento sustentado dos valores e normas éticas junto de todos os colaboradores. • Solidificar as boas relações entre colaboradores, clientes, fornecedores e demais intervenientes na atividade da SIBS
- Segredo Profissional e Procedimentos versus Autoridades nesse âmbito - Tem o objetivo de delimitar de forma clara, simples e sucinta o dever de segredo profissional a que as sociedades do Grupo SIBS estão sujeitas e, bem assim, quais os casos em que a lei impõe a quebra daquele dever.
- Política de Qualidade - Processo de Compras - A Política de Qualidade aqui descrita tem por objeto dotar as Empresas do Grupo SIBS de um procedimento base de suporte ao Processo de Compra para Seleção e Aquisição de Bens e Serviços, bem como descrever a elaboração, pela Área Funcional de Compras (AF Compras), de um Plano Anual de Compras (PAC), ou seja, uma perspetival global e planeada das compras a efetuar por um período de 12 meses pelo Universo das Empresas do Grupo SIBS.

- Normativo orientador e procedimental sobre 'Acordos de Confidencialidade' – Estabelece que as relações contratuais estabelecidas pela SIBS e Empresas Participadas com os seus parceiros de negócio devem prever, para além do âmbito técnico e financeiro de cada contrato, a salvaguarda de toda a informação relacionada com a atividade comercial da SIBS, das empresas por ela participadas, com ela coligadas ou que estejam com ela em relação de grupo.
- Política de Pagamento de Despesas – Estabelece que qualquer despesa realizada por Colaboradores das Empresas do Grupo SIBS decorrente da aquisição de bens e serviços tem de ser suportada por correspondente comprovativo legal original (fatura) e deve obedecer aos requisitos e termos indicados neste documento.
- Procedimento de Gestão do Tarifário e do Preçário - Este documento determina as atividades de controlo para a correta gestão dos documentos de *Pricing*. São destinatários todas as Unidades de Estrutura que propõem, gerem, ou de alguma forma intervêm na gestão dos documentos de *Pricing*.
- Manual de Procedimentos - Gestão de Ativos - Os procedimentos a implementar pelos diversos intervenientes na Gestão de Ativos, têm como principal objetivo garantir uma correta estrutura da informação, visando o cumprimento de obrigações normativas e de gestão interna das empresas do Grupo SIBS.
- Princípios Normativos da Divulgação de Informação a Clientes – Descreve os princípios normativos da divulgação de informação a Clientes.
- Regulamento Interno de Proteção de Dados do Grupo SIBS - O presente Regulamento Interno de Proteção de Dados (RIPD) visa instituir as condições necessárias para o tratamento de dados pessoais pelo Grupo SIBS (adiante SIBS) e assegurar o nível adequado de proteção de dados pessoais de acordo com o Regulamento Geral de Proteção de Dados da União Europeia (“RGPD”) e demais legislação aplicável
- Política de Gestão e Comunicação de Documentos - A Política de Gestão e Comunicação de Documentos pretende preservar a propriedade intelectual das empresas do Grupo SIBS e reduzir a exposição a riscos de incumprimento regulamentar e legal, através da regulação e orientação das formas como os utilizadores lidam com os documentos em todas as fases do seu ciclo de vida
- Delegação de competências - Este normativo regula os níveis decisórios e respetivas delegações de competências nas empresas do Grupo SIBS.
- Política de Segurança - Controlo de Acessos a Informação e Sistemas - Pretende-se com este documento assegurar que os acessos lógicos aos Sistemas de Informação são realizados de forma controlada, existindo uma associação entre a entidade lógica que efetua o acesso e uma pessoa física. Pretende-se também que os acessos sejam realizados unicamente pelos elementos que têm necessidade de aceder aos recursos, desde que demonstrada a necessidade do acesso (*need-to-know*).

- Política de Segurança de Informação – Pessoal - O objetivo principal do documento é o de definir as regras de segurança que devem ser aplicadas ao longo do ciclo de vida dos colaboradores, de forma a reduzir os riscos de erro humano, roubo, fraude e má utilização dos recursos da SIBS pelos colaboradores.
- Sistema de Gestão de Segurança de Informação - Princípios Gerais - O objetivo geral da segurança de informação é minimizar o risco, reduzindo e antecipando o impacto de ataques ao património de informação de forma eficaz e ao menor custo possível. A Política de Segurança de Informação, quando implementada como prática recomendada, assegura que o património de informação seja protegido contra perdas de confidencialidade, integridade e disponibilidade.
- Norma de Segurança - Gestão de Acessos Lógicos - Este documento tem por objetivo estabelecer e documentar os processos de gestão de concessão, revogação e revisão de acessos lógicos nos sistemas ou repositórios de informação da SIBS ou utilizados pela SIBS.
- Manual de Segurança de Informação - Este documento tem como objetivo apresentar uma visão global (um resumo), das principais regras e recomendações destinadas a proteger os recursos de informação do Grupo SIBS, que se aplicam à generalidade dos indivíduos que acedem, processam ou criam informação institucional, ou interagem com os sistemas e infraestruturas tecnológicas associadas a essa informação.
- Norma de Segurança - Salvaguarda de Informação nas Redes Corporativas - O objetivo deste documento é promover a segurança da SIBS, disponibilizando ao conjunto de colaboradores que acedem às redes corporativas da SIBS, a informação necessária para conhecer: • Onde e como deve ser salvaguardada a informação institucional; • Onde e como deve ser salvaguardada a informação pessoal; • Onde e como pode ser partilhada a informação; • O que não pode (ou não deve) ser guardado nas diferentes áreas de armazenamento.
- Regulamento de Auditoria Interna - Este regulamento descreve a missão, independência e objetividade, âmbito e responsabilidades, autoridade e regulamentos da função de Auditoria Interna
- Política de Gestão de Risco do Grupo SIBS - Descreve os princípios primordiais que regem transversalmente a Gestão de Risco nas empresas do Grupo SIBS
- Manual de Gestão de Risco do Grupo SIBS - Descreve os processos ou procedimentos inerentes à Gestão de Risco
- Política de Compliance do Grupo SIBS - Filosofia e os princípios de atuação que suportam o desenvolvimento eficaz da missão a desempenhar pela Função de Compliance
- Manual de Compliance do Grupo SIBS - Processos ou procedimentos a desenvolver no âmbito (ou em execução concreta) da Função de Compliance

- Processos de Tesouraria e Contabilidade - visa a institucionalização dos processos na área Financeira, de modo a, eficazmente, efetuar a previsão, otimização e controlo de todos os pagamentos e de todos os recebimentos, minimizando os riscos de carência e detenção de liquidez, em qualquer das empresas do Grupo SIBS.