SIRESP - GESTÃO DE REDES DIGITAIS DE SEGURANÇA E EMERGÊNCIA,S.A.

Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Versão aprovada em reunião do Conselho de Administração de 24 de junho de 2020

Índice

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

1. Introdução

O presente documento visa dar cumprimento às deliberações e recomendações emitidas pelo Conselho de Prevenção da Corrupção, doravante designado CPC, sobre a avaliação da estratégia de gestão dos riscos de corrupção e infrações conexas.

No âmbito das recomendações do CPC relativas aos riscos de corrupção e infrações conexas, o Conselho de Administração da SIRESP, S.A. considerou relevante ter em atenção também os riscos de fraude.

Assim, e sendo a gestão do risco um processo transversal ao funcionamento das organizações, o presente documento estabelece as orientações sobre a prevenção de riscos de fraude, corrupção e infrações conexas ao nível dos processos estratégicos, operacionais e de suporte da empresa, os critérios de classificação de risco e as funções e responsabilidades na estrutura organizacional.

Tendo em vista a monitorização do processo de gestão deste tipo de riscos, a empresa remete o presente Plano ao CPC, e também às entidades/órgãos competentes para exercício de controlo, bem como ao Ministério das Finanças, publicitando-o também no sítio da internet da empresa.

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

2. Atribuições, caracterização da empresa, organograma e identificação dos responsáveis

2.1. Caracterização da empesa

A SIRESP - Gestão de Redes Digitais de Segurança e Emergência, S.A., (também designada neste documento por SIRESP, S.A. ou por Empresa) foi constituída em 2005 como parte integrante do Plano de Negócios subjacente ao Contrato SIRESP, assinado em 2006 e renegociado em 2015.

De acordo com o Decreto-Lei n.º 81-A/2019, de 17 de junho, a partir de 1 de dezembro de 2019, a SIRESP, S.A. transformou-se em sociedade anónima de capitais exclusivamente públicos, integrando o Setor Público Empresarial. Foi mantido e reforçado o seu objetivo de responsabilidade pela gestão, operação, manutenção, modernização e ampliação da Rede SIRESP, assegurando o correto funcionamento das redes e equipamentos que a integram.

O capital social da SIRESP, S.A. é de 1.614.500,00 Euros, integralmente subscrito e realizado, representado por 50.000 ações ordinárias, tituladas e nominativas com o valor nominal de 32,39 Euros cada, detidas a 100% pelo Estado, através da Direção-Geral do Tesouro e Finanças.

A gestão da sociedade cabe ao Conselho de Administração, composto por três membros, um dos quais será o Presidente, eleitos por um período de três anos pela Assembleia Geral. A fiscalização da sociedade compete a um Fiscal Único, o qual é eleito pela Assembleia Geral.

2.2. Visão, Missão e Objetivos

VISÃO:

É compromisso da SIRESP, S.A., garantir a Portugal serviços de comunicações móveis "*mission critical*", com a melhor tecnologia disponível e segundo as melhores práticas europeias.

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

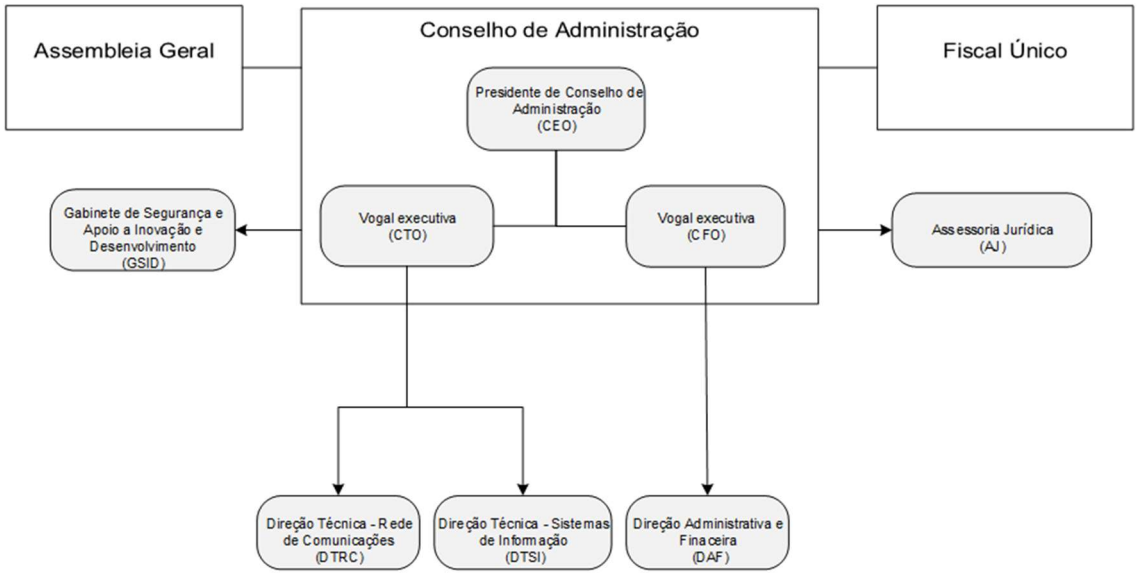
MISSÃO:

Disponibilizar o serviço de comunicações móveis, através do Sistema Integrado das redes de Emergência e Segurança de Portugal - SIRESP.

OBJETIVOS:

1. Assegurar o funcionamento da Rede SIRESP com elevados padrões de qualidade, segurança e fiabilidade;
2. Reforçar a confiança dos utilizadores e melhorar a imagem pública;
3. Propor as funções e responsabilidade para o regime de concessão de serviço público e proceder à sua implementação;
4. Definir a estratégia de evolução para as novas tecnologias e a introdução de novos serviços;
5. Garantir o equilíbrio económico-financeiro;
6. Adaptar-se à nova realidade como empresa do Setor Público Empresarial.

2.3. Organograma da SIRESP, S.A.



SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

2.4. Áreas de Funcionamento

Para concretização do seu objeto social, a SIRESP, S.A. desenvolve a sua atividade através das seguintes áreas operacionais e de suporte, ambas de natureza orgânica. Estas áreas orgânicas respeitam os princípios da colaboração, multidisciplinariedade e segregação de funções quando aplicável pela natureza das mesmas.

2.4.1 Suporte

2.4.1.1 Gabinete de Segurança e Apoio à Inovação e Desenvolvimento (GSID)

Visa garantir o cumprimento da legislação de saúde e segurança no trabalho, a execução e implementação de planos de segurança internos e planos de segurança em projeto e obra, garantindo as medidas técnicas de segurança e respetiva auditoria. Colabora nos processos de informação e formação dos colaboradores, na elaboração de projetos de alteração/construção de novas infraestruturas, bem como nos procedimentos de acompanhamento, intervenção e aceitação final de trabalhos (vertente segurança). Avalia as condições de segurança de locais de instalação, apresentando relatórios e propostas de correções/melhorias. Assegura e controla a atividade de coordenação de segurança subcontratada e respetivos procedimentos. Emite relatórios de atividade de coordenação de segurança. Representa a Empresa em fóruns específicos relacionados com a segurança e a utilização da Rede. Garante a gestão das infraestruturas/instalações da Empresa, através da gestão de controlo de acessos (programação de cartões de acesso e biométrico), e no acompanhamento técnico de manutenção preventiva/corretiva das mesmas. Analisa o mercado no âmbito de projetos e evolução tecnológica, promovendo iniciativas de recolha e divulgação tecnológica.

2.4.1.2. Assessoria Jurídica (AJUR)

Assegura a articulação da assessoria jurídica a nível interno e externo, bem como o apoio jurídico ao Conselho de Administração. Presta assistência jurídica à Empresa, através da emissão de pareceres sobre questões de Direito e realização ou colaboração em estudos, projetos ou contratos que envolvam questões de natureza jurídica e que se mostrem necessários à sua missão. Esta função é exercida em regime de prestação de serviços.

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

2.4.2 Operacionais

2.4.2.1 Direção Técnica – Sistemas de Rede de Comunicações (DTSC)

Assegura a gestão, planeamento e desenvolvimento da Rede SIRESP, nomeadamente na coordenação e controlo dos contratos inerentes ao projeto relativo à rede de telecomunicações. Visa a gestão, controlo e supervisão da implementação e manutenção da Rede SIRESP, através do seu planeamento (capacidade e exploração), configuração e otimização, definição dos locais de instalação, e da gestão e controlo do espectro radioelétrico. Assegura a realização de testes e aceitações e *upgrades* da Rede SIRESP. Garante a gestão e controlo da qualidade do serviço da Rede SIRESP, emitindo relatórios de acompanhamento e supervisão. Garante, ainda, a gestão da operação e manutenção através do controlo de Sistema de O&M adequado, no cumprimento dos contratos de manutenção preventiva da Rede, a sua supervisão, *upgrade* do software e *Help Desk* de 2.ª linha.

2.4.2.2 Direção Técnica – Sistemas de Informação (DTSI)

Concebe a estratégia e arquitetura de tecnologias de informação da Empresa. Assegura a gestão, coordenação e controlo dos contratos de projeto relativos ao subsistema aplicacional e planeia necessidades de SI. Concebe, desenvolve e mantém os sistemas de informação de uso interno da SIRESP. Assegura a integração do sistema e o seu desenvolvimento aplicacional. Coordena as ações de suporte aos utilizadores, tais como a administração dos SI e *Help Desk* interno, de forma a garantir a melhor utilização de toda a infraestrutura e aplicações existentes. Admissão a nível de consolas de despacho e gestão de utilizadores no sistema, *passwords*, novas contas, acessos e servidores de dados. Colabora na contratação e prestação de serviços/produtos. Elabora e implementa medidas necessárias à segurança, confidencialidade e disponibilidade dos dados (pessoais e profissionais) e da informação, bem como os procedimentos para a sua recuperação em casos de falha. Desenvolve procedimentos e políticas operacionais e suas melhores práticas para bom uso das mesmas. Colabora no planeamento e definição da infraestrutura tecnológica, I&D de novos produtos e serviços adequados às reais necessidades da Empresa e complementares à Rede SIRESP.

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

2.4.2.3 Direção Administrativa e Financeira (DAF)

Assegura o planeamento e controlo da atividade, através da gestão, coordenação e supervisão do contrato de gestão e dos contratos de financiamento. Elabora e atualiza o plano de negócio e gere o controlo orçamental. Assegura a gestão financeira e controlo de tesouraria, através da gestão financeira do projeto e na elaboração/atualização de orçamentos de tesouraria e de financiamento. Gere as cobranças (interface com o MAI e novos clientes) e a relação com entidades bancárias. Prepara e disponibiliza informação de gestão e financeira ao acionista – Estado, através da DGTF – ao MAI e aos Bancos. Regista e controla o processamento contabilístico, elaborando a contabilidade analítica por centros de responsabilidade e a contabilidade geral e financeira. Gere e monitoriza o sistema de informação de gestão, utilizando *software* aplicacional adequado para executar funções, tarefas ou atividades inerentes ao DAF. Assegura o controlo interno e respetivas auditorias, através da elaboração/atualização de políticas e procedimentos apropriados; procede às auditorias internas e externas necessárias. Assegura as atividades relativas à gestão de RH, nomeadamente no processamento de salários, execução e controlo dos contratos de trabalho, organização e atualização de processos individuais, avaliação de desempenho, controlo de mapa de férias, assiduidade e ajudas de custo. Assegura todas as necessidades de compras da empresa. Articula, com as diferentes áreas envolvidas, o lançamento de consultas, a definição de parâmetros e critérios requeridos para a adjudicação dos bens ou serviços e avalia os fornecedores. Faz a gestão e controlo do economato.

3. Gestão do risco

3.1. Enquadramento

A SIRESP, S.A. desenvolve a sua atividade de acordo com os mais altos padrões éticos e no estrito cumprimento das regras legais, regulamentares e estatutárias, pelo que considera serem fatores críticos de sucesso a integridade e a diligência dos seus administradores, colaboradores, clientes, fornecedores e demais parceiros com os quais se relaciona (doravante designados como “Partes Interessadas”), bem como o integral respeito pela segregação de funções, adequação de comportamento relacional e contributo para a preservação, integridade e confidencialidade de dados e de informações, nomeadamente pessoais, e o seu compromisso com a Empresa.

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

O Conselho de Administração considera que as Partes Interessadas e a sociedade em geral esperam que os administradores e colaboradores ajam de forma profissional, competente e merecedora de confiança, no melhor interesse da Empresa e dos seus "*stakeholders*".

3.2. Identificação dos riscos de fraude, de corrupção e infrações conexas

Tendo em conta o enquadramento da SIRESP, S.A. como sociedade de capitais públicos e a missão e objetivos constantes dos seus Estatutos, a Empresa adota um modelo de gestão dos riscos com foco especial nos riscos de fraude, corrupção e infrações conexas, implícitos nos tipos criminais descritos no Código Penal, nomeadamente nos artigo 335º *Tráfico de influência*, artigo 372º *Recebimento indevido de vantagem*, artigo 373º *Corrupção passiva*, artigo 375º *Peculato*, artigo 376º *Peculato de uso*, artigo 377º *Participação económica em negócio*, artigo 382º *Abuso de poder*, artigo 383º *Violação de segredo por funcionário*, e na Política de Gestão de Risco de Fraude da Empresa.

3.3 Conflito de Interesses

Na sua recomendação de 7 de novembro de 2012, o CPC adverte para a necessidade de implementação de mecanismos de acompanhamento e de gestão de conflitos de interesses integrados nos planos de prevenção de riscos de corrupção e infrações conexas, mecanismos esses que devem ser divulgados dentro da organização – a todas as áreas de atuação e para cada área funcional da estrutura da Empresa. Deve ser parte integrante da cultura organizacional, promovendo a inexistência de situações de conflito de interesses.

O CPC, em 8 de janeiro de 2020, salienta que o conceito de conflito de interesses inclui qualquer situação, real, aparente ou potencial, de sobreposição de interesses privados sobre os interesses públicos, e que por essa via prejudiquem a isenção e o rigor das decisões administrativas que tenham de ser tomadas, ou que possam suscitar a dúvida do desempenho do exercício de funções públicas.

Assim, o Relatório sobre a execução do Plano de Prevenção de Riscos deve fazer referência à gestão de conflito de interesses.

A independência, isenção, respeito pela segregação de funções, objetividade e transparência de atuação de uma qualquer Parte Interessada pode ficar prejudicada quando aquela toma

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

uma decisão em situação de conflito de interesses, suscetível de ocorrer sempre que envolvam os seus interesses pessoais ou familiares, ou de terceiros com os quais se relacione.

A adequada gestão de conflitos de interesses deve encontrar sustentação em valores, princípios e normas éticas comuns de integridade pública. Os mecanismos de prevenção de conflitos de interesses adotados pela SIRESP, S.A. encontram-se previstos nos seguintes documentos:

• **Código de Ética** - disponível no sítio da internet da Empresa, aplica-se a titulares dos órgãos sociais, colaboradoras e colaboradores, clientes, fornecedores e demais parceiros com os quais a Empresa se relaciona. Menciona os princípios e valores fundamentais da Empresa, define as normas de conduta profissional, proíbe a decisão em situação de conflito de interesses, prevê o dever de confidencialidade e segurança da informação e proíbe as práticas de fraude, corrupção e suborno. Indica também o canal de comunicação a utilizar em casos de necessidade de reporte de violações do Código de Ética;

• **Política de gestão de riscos de fraude** – disponível no sítio da internet da Empresa, é aplicável a titulares dos órgãos sociais, colaboradoras e colaboradores, e ao relacionamento da SIRESP, S.A. com clientes, fornecedores e demais parceiros. Define o que se entende por conflito de interesses, em que situações podem ocorrer e refere as modalidades de reporte de situações de suspeita de fraude. No âmbito desta Política, os titulares dos órgãos sociais, bem como as colaboradoras e os colaboradores da Empresa, que tenham vínculo à função pública, ficam obrigados ao registo de interesses, mediante o preenchimento de um formulário que inclui a declaração i) das ofertas recebidas que possam ser consideradas como tentativa de influenciar as decisões da Empresa e/ou daquelas Partes Interessadas no exercício das suas funções e ii) das funções acumuladas, e se estas podem colidir com as funções exercidas e se podem colocar em causa a isenção e o rigor no desenvolvimento das funções na SIRESP S.A. A Política existe na Empresa desde 2020 e será revista periodicamente.

3.4 Metodologia

A identificação dos riscos associados aos processos operacionais e de suporte considerados como significativos pela gestão, que se encontram descritos em diversos documentos internos da Empresa desde 2008 e que têm sido sistematicamente revistos e atualizados, darão origem ao Manual de Procedimentos da SIRESP, S.A., em elaboração. Estes documentos encontram-se digitalizados e disponíveis a todos os colaboradores da Empresa, através de ficheiros partilhados.

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

No âmbito da identificação e avaliação dos potenciais riscos de fraude, corrupção e infrações conexas ao nível dos processos, e conforme recomendado pelo CPC, procedeu-se à classificação dos riscos segundo uma escala de risco baixo, médio ou alto.

O risco residual, definido como a parcela do risco total que não é mitigado pelos controlos existentes na organização, é determinado com base no impacto da materialização do risco e na respetiva probabilidade de ocorrência.

As classificações atribuídas tiveram por base as orientações do CPC que se apresentam de seguida:

a) Probabilidade de ocorrência

Alta - Probabilidade elevada de que o risco se concretize, uma vez que se refere a um processo complexo que requer coordenação e uma vigilância significativa ou a um processo dependente de atividades voláteis e imprevisíveis.

Média - Probabilidade média de que o risco se concretize, uma vez que o processo necessita de alguma vigilância e de coordenação, ou as atividades subjacentes poderão ser previsíveis.

Baixa - Probabilidade baixa de o risco se concretizar, uma vez que se refere a um processo rotineiro, previsível e automatizado, com baixa necessidade de supervisão.

b) Impacto

Alto - Quando pode ocorrer perda de reputação e de confiança dos *stakeholders* e ter um impacto grave nos *cash-flows*.

Médio - Evento de risco vai requerer atenção e intervenção significativas da gestão e perdas no *cash-flow* com impacto moderado.

Baixo - Necessidade mínima da intervenção da gestão no evento de risco, ou processo rotineiro com grande nível de automatização.

3.5 Monitorização, execução e atualização do Plano

É entendimento do Conselho de Administração da SIRESP, S.A. que, para o Plano ser efetivo, importa clarificar responsabilidades pela implementação de medidas nele previstas e supervisão da sua aplicação.

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

Do ponto de vista operacional, o Plano deve ser acompanhado, monitorizado e avaliado, nos respetivos domínios de competência pelas unidades orgânicas com o Conselho de Administração e, sempre que se afigure adequado, com o Fiscal Único.

A gestão da implementação do Plano e a respetiva supervisão ficará a cargo do Conselho de Administração da SIRESP, S.A..

Em conformidade com a recomendação de 1 de julho de 2009 do CPC, o Fiscal Único elabora anualmente um relatório de execução do Plano que, após aprovado pelo Conselho de Administração, é reportado ao CPC, por disponibilização da informação constante no sítio da internet da SIRESP, S.A., e também às entidades/órgãos de controlo, bem como ao Ministério das Finanças, incluindo a Unidade Técnica de Acompanhamento e Monitorização do Sector Público Empresarial, ao abrigo do disposto no n.º 2 do artigo 46.º do Decreto-Lei n.º 133/2013, de 3 de outubro.

O Plano deverá ser revisto e atualizado numa base anual. Serão realizadas ações de formação, de divulgação, reflexão e esclarecimento do Plano junto dos trabalhadores, contribuindo para o envolvimento destes numa cultura de prevenção de riscos.

4. Anexos – Matriz de Riscos e Controlos

4.1. Processo de Gestão Financeira

Subprocesso: Abertura e encerramento das contas bancárias						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Apropriação indevida de fundos da empresa	Movimentação indevida de conta bancária, em benefício próprio ou de terceiro.	A documentação de abertura de contas bancárias é assinada pelos administradores e pelo procurador (quando existente). Sempre que há pagamentos, é verificada a conformidade entre a ficha de assinaturas e o documento do banco com indicação dos movimentadores das contas.	Conselho de Administração Direção Financeira	Baixo	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

Subprocesso: Conferência e pagamento de documentos						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Apropriação indevida de fundos da empresa ou de meios de pagamento	Utilização indevida de fundos da empresa para pagamentos, em benefício próprio ou de terceiro. Pagamentos indevidos e/ou de montante diferente ao devido, em benefício próprio ou de terceiro. Pagamento de bens ou serviços não recebidos ou prestados à empresa, em benefício próprio ou de terceiro. Apropriação e utilização indevida de cartão do SIRESP, que permite efetuar pagamentos e levantamentos em caixas ATM.	As despesas são aprovadas de acordo com a delegação de competências em vigor. O acesso ao cofre está limitado a uma colaboradora da Área Financeira, havendo ainda uma delegação de competências numa outra colaboradora para situações de ausência ou impedimento da primeira. As despesas reembolsadas a administradores e a colaboradores são apresentadas e justificadas conforme previsto na Política de Pessoal, não sendo aceites documentos de despesa com os elementos essenciais de caracterização do documento de despesa alterados. No caso do reembolso de despesas por caixa, estas são registadas em folha de caixa na qual os colaboradores confirmam, por assinatura, o montante recebido. Aquando da reposição do saldo de caixa, o Diretor Financeiro confere o registo efetuado com os documentos de despesa em anexo. Análise/revisão mensal do balancete e das contas correntes de terceiros. Diariamente, são identificados os registos de todos os movimentos ocorridos em todas as contas bancárias da empresa e através do Controle.	Administradores Direção Financeira Superior hierárquico que valida e aprova as despesas e Direção Financeira e/ou Área de Recursos Humanos (consoante o tipo de despesas). Direção Financeira Direção Financeira Direção Financeira	Baixo	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

		Revisão mensal das reconciliações bancárias. Existe um cartão do SIRESP, que é utilizado apenas para a associação de identificadores de Via Verde. O cartão é de acesso restrito ao Diretor Financeiro e a uma colaboradora da Direção Financeira e são guardados em cofre com acesso restrito.	Direção Financeira Direção Financeira			

Subprocesso: Recebimentos						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Apropriação indevida de fundos da empresa	Desvio de fundos devidos à empresa, por depósito ou transferência para conta indevida, em benefício próprio ou de terceiro. Desvio de fundos recebidos em numerário	Revisão mensal das reconciliações bancárias. Análise das contas correntes de terceiros. Por princípio/politica, não são aceites quaisquer recebimentos por cheque. Todavia, caso exista algum recebimento por cheque, não são aceites cheques ao portador, mas apenas cheques emitidos à ordem da empresa e cruzados. O valor de cada recebimento é conferido com a transação que lhe deu origem.	Direção Financeira Direção Financeira Direção Financeira Direção Financeira	Baixo	Baixa	

4.2. Processo de Aquisição de bens e serviços

Processo: Aquisição de Bens e Serviços						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Apropriação indevida de bens e serviços para uso pessoal	Aquisição de bens e serviços não decorrente de necessidades reais da empresa em	Antes de cada procedimento, é elaborada uma nota interna ou e-mail a solicitar autorização para adquirir um bem ou serviço.	Área requisitante	Baixo	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

	benefício próprio ou de terceiro	A aquisição de bens ou serviços é sujeita a uma consulta prévia a pelo menos três fornecedores que estejam em condições de a prestar com qualidade e eficiência, em função da oferta que existe no mercado.	Área requisitante			
		As propostas são analisadas pelo Conselho de Administração, composto por três membros, onde é formalizado um relatório de análise comparativa das propostas.	CA			
		Formalização do processo de cabimentação da despesa e respetivo compromisso junto da Direção Financeira.	Direção Financeira			
		Elaboração do contrato de aquisição de bens ou serviços, ou revisão do contrato de aquisição de bens ou serviços nos casos em que este é elaborado pelo fornecedor.	Assessoria Jurídica			
		Os administradores e os colaboradores da empresa devem recusar quaisquer ofertas, para si ou para terceiros, que possam ser consideradas ou interpretadas como uma tentativa de influenciar as decisões da empresa ou do colaborador no exercício das suas funções.	CA e colaboradores			
		A não declaração, por um administrador ou colaborador, de um eventual interesse/ligação pessoal, é considerada uma violação à Política de Gestão do Risco de Fraude (PGRF), sendo aplicáveis os procedimentos disciplinares e/ou legais em vigor.	CA			
		A PGRF prevê mecanismos para reporte de qualquer				

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

		facto ou suspeita de situações irregulares, de fraude ou má conduta, por parte de qualquer colaborador, prestador de serviço ou terceira entidade, por carta fechada ou para o e-mail, conforme referido no Código de Ética da SIRESP S.A.				
Conluio entre colaboradores e fornecedores em benefício próprio ou de terceiro	Risco de estarem a ser favorecidos determinados fornecedores, de não existir independência face aos mesmos e de estarem a ser aprovadas propostas que não reúnem as melhores condições de qualidade e de preço.	A aquisição de bens ou serviços é sujeita a uma consulta prévia a pelo menos três fornecedores que estejam em condições de a prestar com qualidade e eficiência, em função da oferta que existe no mercado. As propostas são analisadas pelo Conselho de Administração, composto por três membros, onde é formalizado um relatório de análise comparativa das propostas. As adjudicações de aquisição bens e serviços são aprovadas pelo CA e tendo em atenção o relatório de análise comparativa das propostas quando a aquisição foi objeto de consulta por concurso. Todos os colaboradores, incluindo a Administração, são obrigados a declarar os seus interesses/ligações familiares com entidades com as quais a empresa se relacione, clientes, fornecedores e demais entidades externas.	Área requisitante CA CA CA CA e DAF	Baixo	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

Validação de serviço não prestado de acordo com o contratualizado ou não recebimento de bens encomendados, em benefício próprio ou de terceiro	Risco de o fornecedor não prestar o serviço de acordo com o contratualizado ou de não serem recebidos os bens efetivamente encomendados.	A conferência das faturas de bens e serviços é efetuada por colaborador diferente de quem efetuou a encomenda.	DAF	Médio	Baixa	
Apropriação indevida de material de economato, em benefício próprio ou de terceiro	Risco de os armários do economato e outros consumíveis (e.g. toners, tinteiros) poderem ser acedidos por terceiros, para apropriação indevida de material.	Existe um controlo implementado relativamente ao consumo de material de economato e outros consumíveis. O local onde o material de economato se encontra guardado é de acesso restrito.	DAF	Médio	Baixa	
Falta de acuidade na formalização dos contratos com fornecedores, em benefício próprio ou de terceiros	Risco de o contrato ser assinado contendo cláusulas penalizadoras para a empresa, em benefício próprio ou de terceiros.	Os contratos com fornecedores de bens e serviços, antes de serem assinados por dois administradores, são sujeitos a análise da ssessoria Jurídica	Assessoria Jurídica	Baixo	Baixa	

4.3. Processo de Gestão Documental

Processo: Gestão Documental						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Abuso de informação privilegiada	Utilização de informação privilegiada, em benefício próprio ou de terceiro.	A correspondência recebida na SIRESP S.A. e classificada no Sistema de Gestão Documental (Comunicações) só pode ser visualizada pelos colaboradores a quem aquela foi encaminhada/dirigida e por	DAF	Médio	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

		aqueles a quem estes encaminharem/derem conhecimento. Os administradores e colaboradores da empresa não podem utilizar e divulgar informação privilegiada a terceiros, conforme definido no Código de Ética.	CA e colaboradores			

4.4. Processo de Recursos Humanos

Processo: Recursos Humanos						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Conflito de interesses	Tomada de decisão ou análise técnica em situação de conflito de interesses, em benefício próprio ou de terceiro.	Existência de um Código de Ética na empresa, que é do conhecimento e vincula os administradores e colaboradores ao seu cumprimento. O Código de Ética prevê a realização periódica de sessões de formação/ sensibilização sobre o seu conteúdo. Existência de uma Política de Gestão do Risco de Fraude que vincula os administradores e colaboradores, com vínculo à função pública, à entrega de um formulário de registo de interesses.	CA CA e DAF CA e DAF	Médio	Baixa	
Atribuição, apropriação e ou uso indevidos de ativos	Atribuição, apropriação e ou uso indevido de bens da empresa (viaturas, telemóveis, computadores, entre outros) em benefício próprio ou de terceiro.	A atribuição de bens (viaturas, telemóveis, computadores, entre outros) a administrador ou colaborador é aprovada pelo CA, salvaguardando as obrigações legais aplicáveis, e em vigor na empresa em cada momento. Controlo dos limites de consumos definidos para os	CA CA e DAF	Médio	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

		administradores e colaboradores. Existência um Código de Ética na empresa, que é do conhecimento e vincula os administradores e colaboradores ao seu cumprimento. O Código de Ética prevê a realização periódica de sessões de formação/ sensibilização sobre o seu conteúdo. Aquando da saída de um administrador ou colaborador é preenchida uma *checklist* que evidencia a entrega de todos os bens que lhes foram confiados para uso no exercício das suas funções.	CA e DAF CA e DAF DAF			

Sub-Processo: Admissão e contratação						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Manipulação do processo de contratação de colaboradores	Falsa fundamentação da necessidade de contratação. Favorecimento de candidatos, em benefício próprio ou de terceiro.	A necessidade de admissão de colaboradores é formalmente fundamentada pelo CA. A necessidade de admissão de colaboradores é aprovada pelo CA, salvaguardando a legislação aplicável. Definição do processo de avaliação e seleção de candidatos. Processo documentado com evidências face aos requisitos definidos.	CA CA CA CA e DAF	Baixo	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

Sub-Processo: Processamento e controlo salarial						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Manipulação do processamento salarial	Manipulação da informação de modo a justificar o pagamento indevido de remunerações e/ou outros benefícios, em benefício próprio ou de terceiro. Aceitação de favor e/ou favorecimento ilícito em troca da concessão de vantagem indevida. Manipulação, não atualização ou atualização dolosa dos dados de colaboradores, em benefício próprio ou de terceiro	As remunerações e benefícios são aprovados pelo CA. Os dados a processar são validados pela DAF. Aprovação final pelo administrador com o pelouro dos Recursos Humanos.	CA e DAF	Baixo	Baixa	

Sub-Processo: Registo de férias						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Manipulação dos dias de férias e/ou de faltas	Atribuição de dias de férias em número superior ao que o administrador ou colaborador tem direito. Não registo ou anulação de registo de falta de administrador ou colaborador ou alteração de férias.	O plano de férias dos colaboradores e alterações são validados pelo superior hierárquico respetivo, ou, no caso de administradores, por outro administrador. O mapa de férias anual da empresa é aprovado pelo CA. Em caso de faltas, o colaborador terá de informar o seu superior hierárquico e os Recursos Humanos e, sempre que possível, apresentar o documento justificativo da mesma. É efetuado o levantamento de faltas para efeito de processamento salarial mensal. É feito o controlo de férias na aplicação Férias, para cada colaborador.	CA e DAF CA DAF DAF	Baixo	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

		As alterações de férias são comunicadas pelo colaborador ao superior hierárquico respetivo e aos Recursos Humanos, e validadas pelo superior hierárquico, sendo posteriormente registadas no suporte definido para efeito de controlo de férias: Aplicação Férias	DAF			

4.5. Processo de Contabilidade e Controlo Orçamental

Sub-Processo: Orçamento e Execução Orçamental						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Manipulação das demonstrações financeiras previsionais	Utilização dolosa de pressupostos inadequados na elaboração das demonstrações financeiras previsionais, em benefício próprio ou de terceiro. Manipulação das demonstrações financeiras previsionais (orçamento), em benefício próprio ou de terceiro. Análise incorreta e dolosa de desvios nos relatórios de execução orçamental trimestral, em benefício próprio ou de terceiro.	As demonstrações financeiras previsionais (orçamento) são aprovadas pelo CA e sujeitas a parecer de Auditoria enquanto órgão de fiscalização. Os relatórios de execução orçamental trimestral são analisados e aprovados pelo CA e sujeitos a parecer do órgão de fiscalização	CA e DAF CA e DAF	Baixo	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

Sub-Processo: Registos e prestação de contas						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Manipulação das demonstrações financeiras	Manipulação das demonstrações financeiras resultante da não contabilização ou incorreta contabilização das operações e transações da empresa, em benefício próprio ou de terceiro. Manipulação das demonstrações financeiras resultante de incorreta apresentação e/ou divulgação, em benefício próprio ou de terceiro.	Análise/revisão mensal do balancete e das contas correntes de terceiros. Revisão mensal das reconciliações bancárias. Revisão das demonstrações financeiras. Acompanhamento da preparação das demonstrações financeiras, incluindo a verificação da conformidade de apresentação com anos anteriores e do cumprimento com as normas contabilísticas aplicáveis, quer ao nível da apresentação quer das divulgações necessárias. Monitorização da preparação das demonstrações financeiras, pelo DAF. Aprovação das demonstrações financeiras pelo CA.	CA e DAF CA e DAF CA e DAF CA	Baixo	Baixa	

4.6. Processo de Segurança Informática e Física

Processo: Segurança Informática e Física						
Risco	**Descrição do Risco**	**Descrição do(s) Controlo(s)**	**Responsável**	**Imp.**	**Prob.**	**Risco**
Acesso a informação não autorizada	Acesso doloso a informação não autorizada, em benefício próprio ou de terceiro.	Estão definidos perfis de acesso ao sistema de gestão documental e às pastas de rede, em conformidade com as funções exercidas por cada colaborador. Os acessos são atribuídos e geridos pelo responsável pelo Sistema de Informação nos termos da política de	DTSI DTSI	Médio	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

		acessos, mediante autorização do CA.				
		O acesso a informação privilegiada é restringido aos administradores e aos colaboradores por eles indicados ou que a colocaram. A classificação de comunicação como privilegiada é efetuada pelos administradores ou pelos colaboradores que a colocam.	DTSI e CA			
		Existência de normas de utilização dos sistemas de informação.	DTSI e CA			
		Existência de software *anti-malware.*	DTSI			
Intrusão interna e externa	Alteração dolosa das regras de acesso à infraestrutura informática, em benefício próprio ou de terceiro. Alteração de dados e/ou destruição de dados.	Existência de normas de utilização dos sistemas de informação.		Médio	Baixa	
		A alteração das regras de acesso à infraestrutura informática é autorizada formalmente pelo administrador responsável pela área requisitante, com conhecimento do administrador responsável pela área de tecnologias de informação.	DTSI e CA DTSI			
		Periodicamente são efetuadas auditorias de alteração de acessos a pastas, VPN's e de verificação de utilizadores ativos e não ativos.	DTSI			
		Existência de *firewall* de perímetro externo e interno.				
		Existência de *software* antivírus.				
		Sistema de *Backup*				
	Risco de terceiros poderem entrar nas	O controlo de acesso ao edifício é efetuado por empresa de segurança 24h	DTSI e GSID			

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal

Acesso indevido às instalações e a documentação física protegida	instalações e terem acesso a documentação privilegiada, poderem furtar a mesma, bem como equipamentos e materiais	por dia e pelos registos eletrónicos de entrada e saída. As instalações da SIRESP só são acedidas por colaboradores ou prestadores de serviço com acesso registado e as portas só abrem com identificação biométrica ou por cartão com chip. Procede-se à gravação de imagens das áreas comuns.	Colaboradores DTSI	Média	Baixa	

SIRESP, Gestão de Redes Digitais de Segurança e Emergência, S.A.
Morada: Praça Duque de Saldanha, nº 1, 9º Piso – Frações E e F
1050-094 Lisboa, Portugal