PLANO DE GESTÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS 2021

INCM

ÍNDICE

1. INTRODUÇÃO

O Conselho de Prevenção da Corrupção (CPC) é uma entidade administrativa independente criada pela Lei n.º 54/2008, de 4 de setembro, que tem como fim desenvolver uma atividade de âmbito nacional no domínio da prevenção da corrupção e infrações conexas nomeadamente na recolha e análise de informação junto das entidades públicas, organismos, serviços e agentes da administração central, regional e local, bem como das entidades do setor público empresarial.

Foi neste enquadramento que o CPC emitiu, a 1 de julho de 2009, a recomendação para que as entidades elaborassem anualmente planos de gestão de riscos de corrupção e infrações conexas por forma a identificar, de forma transversal à organização:

a) Os riscos no domínio da prevenção da corrupção e infrações conexas;
b) As medidas adotadas que permitem a mitigação dos riscos identificados; e
c) Os responsáveis na organização pela elaboração, monitorização e controlo dos riscos.

Adicionalmente, a recomendação refere que as entidades devem promover a elaboração de relatórios de execução dos planos definidos.

Dando cumprimento ao disposto na Recomendação n.º 1/2009 do CPC, e reconhecendo a importância e o valor do instrumento de gestão no combate à corrupção e infrações conexas, a Imprensa Nacional-Casa da Moeda (INCM) elabora o presente Plano de Gestão de Riscos de Corrupção e Infrações Conexas de 2021. No sentido de assegurar a transparência do exercício de gestão de risco aqui descrito, e em cumprimento da Recomendação n.º 1/2010 do CPC, o presente plano encontra-se disponibilizado na internet em *https://incm.pt/portal/incm_gr.jsp*.

2. A IMPRENSA NACIONAL-CASA DA MOEDA, S. A. (INCM)

A INCM é uma sociedade anónima de capitais exclusivamente públicos, resultante da fusão, em 1972, da Imprensa Nacional com a Casa da Moeda. Pela longa história das empresas que a originaram, a INCM é herdeira dos mais antigos estabelecimentos industriais do País. A Casa da Moeda é talvez o mais antigo estabelecimento fabril do Estado português, com uma laboração contínua desde, pelo menos, o final do século XIII.

Pela forma como vem incorporando as novas tecnologias na sua

vasta gama de atividades, a INCM é uma empresa voltada para o futuro e apostada em vencer os desafios que a sua missão lhe coloca, num mundo em permanente mutação.

A empresa tem a seu cargo, por um lado, a produção de bens e serviços fundamentais ao funcionamento do Estado português, como os documentos de identificação e viagem, a cunhagem de moeda metálica e a edição de publicações oficiais, onde se destaca o *Diário da República,* e, por outro lado, um conjunto relevante de produtos e serviços mercantis, dentro das mesmas linhas de negócio, visando fornecer outros países com bens essenciais, proteger marcas, identificar pessoas e bens, entre outros.

A evolução das novas tecnologias faz das atividades da gráfica de segurança e da segurança digital áreas estratégicas de desenvolvimento da empresa, capacitando-as para fornecer os mais modernos e seguros documentos de identificação, em suporte físico e digital, respondendo às necessidades de um vasto leque de empresas e organizações.

A autentificação de artefactos de metais preciosos, tarefa em que a INCM tem já uma longa tradição, é feita hoje em modernos laboratórios, acreditados pelo Instituto Português da Acreditação.

A edição de obras essenciais da língua e cultura portuguesas é outra incumbência da INCM, levada a cabo através da sua editora Imprensa Nacional. O Estado garante assim a transmissão, entre gerações, do património bibliográfico da língua portuguesa e proporciona a edição de novas obras que o enriquecem continuamente.

Missão, Visão e Valores

A INCM, enquanto parte integrante do setor empresarial do Estado (SEE), tem como missão criar, produzir e fornecer bens e serviços que exigem elevados padrões de segurança, focados no cliente e em soluções inovadoras, assente nos seguintes valores:

- Cultura empresarial;
- Desenvolvimento sustentável;
- Responsabilidade para com os seus trabalhadores;
- Respeito pela igualdade de género e não discriminação;
- Satisfação do cliente;
- Serviço ao cidadão;

- Envolvimento e colaboração;
- Inovação em rede;
- Melhoria contínua;
- Excelência.

Tendo por base estes valores, a INCM tem como visão ser reconhecida, a nível nacional e internacional, como líder em produtos e serviços de segurança essenciais à sociedade e como promotora da língua e cultura portuguesas.

3. GOVERNAÇÃO NA INCM

De acordo com os princípios de bom governo das empresas do setor empresarial do Estado, referidos na Resolução do Conselho de Ministros n.º 49/2007, a INCM tem estruturas de administração e fiscalização ajustadas à sua dimensão e complexidade. O ambiente de controlo interno da INCM é sustentado pelo modelo de governança da sociedade consolidado na sua estrutura organizativa, que delimita a atribuição de autoridade e responsabilidade, ao nível estratégico, tático e operacional.

3.1. MODELO DE GOVERNO

A INCM é gerida de acordo com o modelo de governo latino reforçado, composto pela Assembleia Geral de Acionistas, Conselho de Administração, Conselho Fiscal e Revisor Oficial de Contas. Este arquétipo vai ao encontro das orientações para fortalecer as estruturas de controlo nos modelos de governo das empresas do Estado e assegura uma efetiva segregação entre as funções de administração executiva e de fiscalização.

O Conselho de Administração é o órgão responsável pela aprovação dos objetivos e políticas de gestão, elaboração e aprovação do plano estratégico e de negócio, relatório e contas anuais, relatório de sustentabilidade, relatórios financeiros e orçamentos, por estabelecer a organização interna da empresa e elaborar os regulamentos e as demais instruções convenientes para uma boa gestão.

As funções de fiscalização cabem ao Conselho Fiscal e ao Revisor Oficial de Contas. De entre as competências do Conselho Fiscal consta a emissão de parecer sobre todas as matérias relativas a controlo interno, gestão de riscos, reporte financeiro, auditoria externa e auditoria interna. Ao Revisor Oficial de Contas, para além das atribuições constantes da lei, compete emitir os pareceres previstos no sistema de controlo interno da administração financeira do Estado e do setor público empresarial.

A Direção de Auditoria Interna é responsável por delinear e realizar auditorias ou trabalhos de consultoria interna, avaliando de uma forma independente e sistemática as atividades e processos críticos, permitindo contribuir para uma melhoria do desempenho, controlo e governo da INCM, exercendo as suas funções de um modo independente e objetivo reportando funcionalmente ao Conselho Fiscal.

Ao nível tático destaca-se o Comité de Gestão de Riscos Corporativos. Órgão não executivo que tem como missão o apoio e aconselhamento do Conselho de Administração sobre todas as matérias relativas à gestão integrada de riscos corporativos, assegurando a supervisão e acompanhamento da gestão de riscos da INCM.

O Chief Risk Officer (CRO) é responsável pela implementação das atividades de gestão de risco corporativo em estreita colaboração com as diversas unidades orgânicas da INCM, assegurando uma constante identificação, análise e avaliação dos riscos da organização. É encarregue de assegurar que a informação de risco se encontra atualizada, consolidada, estruturada e devidamente comunicada para as partes interessadas. O CRO é também o coordenador do Comité de Gestão de Riscos Corporativos, competindo-lhe a supervisão das medidas decididas por este órgão.

3.2. ESTRUTURA ORGANIZACIONAL

Em termos organizacionais, a INCM está estruturada por unidades orgânicas que respondem ao Conselho de Administração[1].

A Comissão de Coordenação Estratégica (CCE) afeta responsáveis na organização pela estruturação e articulação da atividade das unidades orgânicas em torno dos seguintes eixos estratégicos:

- Internacionalização;
- Transição Digital;
- Eficiência e Indústria 4.0;
- Estratégia e Transformação Organizacional.

[1] O Conselho de Administração procedeu à revisão da estrutura orgânica da INCM, com efeitos a 1 de fevereiro de 2021 (DCA n.º 94/2021, de 11 de fevereiro). Esta atualização alinha a resposta da empresa com a estratégia traçada para o presente triénio, tendo ainda em conta o impacto profundo da pandemia e a aceleração da transformação digital das suas atividades.

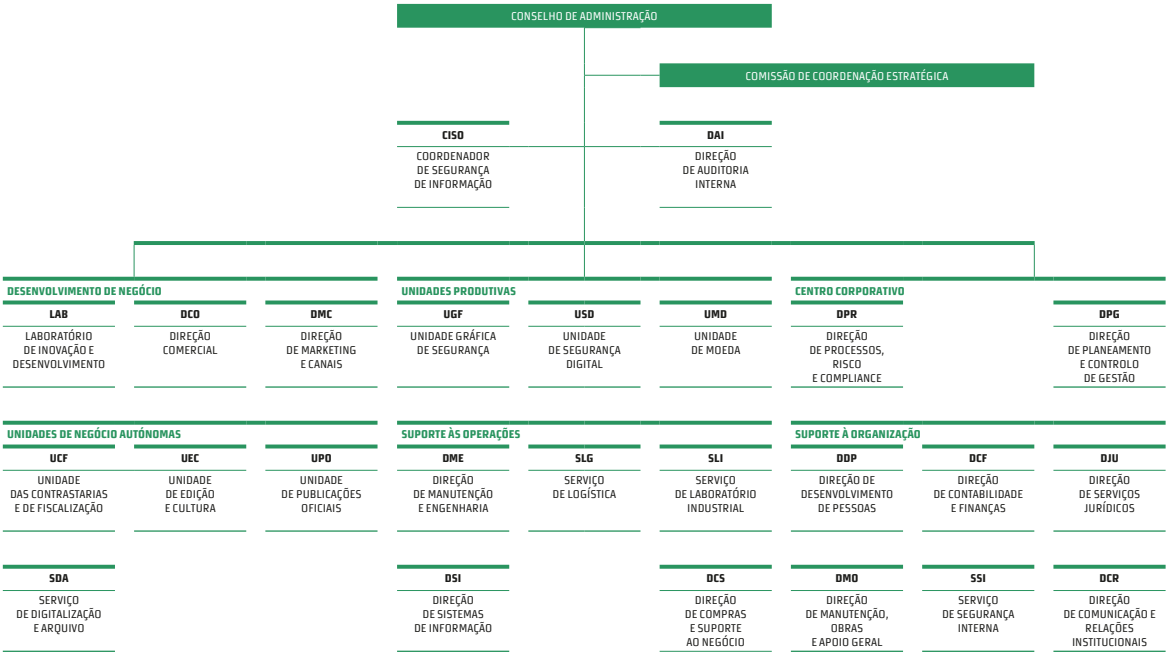

FIGURA 1
ORGANOGRAMA INCM

Estes responsáveis assumem também a presidência dos Comités relacionados com as respetivas áreas de coordenação.

Unidade Orgânica	Missão
DAI Direção de Auditoria Interna	Delinear e realizar auditorias ou trabalhos de consultoria internos, avaliando de uma forma independente e sistemática as atividades e processos críticos, permitindo contribuir para uma melhoria do desempenho, controlo e governo da INCM.
CISO Coordenador de Segurança de Informação	Garantir a segurança da informação nas práticas internas e externas da INCM e participar no desenvolvimento dos produtos e serviços de certificação eletrónica, garantindo a competitividade dos serviços da empresa e o cumprimento das boas práticas e certificações internacionais de segurança.

DESENVOLVIMENTO DE NEGÓCIO

Unidade Orgânica	Missão
LAB Laboratório de Inovação e Desenvolvimento	Desenvolver iniciativas de inovação e novos produtos comerciais, contribuindo para a manutenção de um portfólio de produtos inovador e rentável na INCM.
DCO Direção Comercial	Gerir a atividade comercial da empresa focada na gráfica e nas soluções digitais de segurança para clientes institucionais, contribuindo para o cumprimento dos objetivos de negócio e para a satisfação dos clientes.
DMC Direção de Marketing e Canais	Gerir a comercialização da moeda, de soluções empresariais e de produtos de retalho, incluindo os vários canais de relacionamento, contribuindo para o cumprimento dos objetivos de negócio e para a satisfação dos clientes.

CENTRO CORPORATIVO

Unidade Orgânica	Missão
DPR Direção de Processos, Risco e Compliance	Promover transversalmente práticas de gestão e operação alinhadas com referenciais e boas práticas reconhecidas internacionalmente numa lógica de sustentabilidade e melhoria contínua, garantindo o *compliance* e fomentando uma cultura de gestão e prevenção de riscos.
DPG Direção de Planeamento e Controlo de Gestão	Assegurar o processo de planeamento e os instrumentos de controlo de gestão da empresa, promovendo a disponibilização de informação de gestão relevante e a articulação de todas as unidades organizacionais numa perspetiva de criação de valor.

UNIDADES PRODUTIVAS

Unidade Orgânica	Missão
UGF Unidade Gráfica de Segurança	Desenvolver e fornecer produtos ou soluções gráficas com elevados níveis de segurança, contribuindo para a garantia da confiança nas relações entre o Estado, os cidadãos e as organizações.
USD Unidade de Segurança Digital	Conceber e fornecer soluções de identidade e segurança digital, em linha com a estratégia global da INCM.
UMD Unidade de Moeda	Assegurar a produção de moeda metálica para o Estado português, satisfazendo as necessidades de circulação monetária, produzir moeda para outros países, no âmbito da estratégia de internacionalização da INCM, e cunhar moeda para fins numismáticos e de colecionismo, promovendo a celebração de eventos, efemérides e personalidades.

UNIDADES DE NEGÓCIO AUTÓNOMAS

Unidade Orgânica	Missão
UCF Unidade das Contrastarias e de Fiscalização	Assegura o serviço público de garantir a espécie e o toque dos artigos com metais preciosos, o exercício das atividades enquadradas no âmbito do setor de ourivesaria, bem como a respetiva fiscalização e instrução dos processos contraordenacionais, contribuindo para a proteção do consumidor e a concorrência leal entre os agentes económicos.
UEC Unidade de Edição e Cultura	Assegurar a edição de livros (de forma supletiva), a gestão do património cultural e acervos históricos da INCM, bem como programar e garantir as atividades de responsabilidade cultural da empresa, tendo como princípio orientador a promoção da língua e cultura portuguesas.
UPO Unidade de Publicações Oficiais	Assegurar o serviço público de disponibilização do *Diário da República* e garantir a acessibilidade do Diário da República Eletrónico (DRE), gerindo os conteúdos e funcionalidades do sítio respetivo.
SDA Serviço de Digitalização e Arquivo	Assegurar a prestação de serviços de digitalização e arquivo de elevada segurança de documentos para clientes externos e internos da empresa, promovendo a preservação digital dos documentos e a disponibilização dos respetivos dados, potencialmente sujeitos a mecanismos de análise e valorização.

SUPORTE ÀS OPERAÇÕES

Unidade Orgânica	Missão
DSI Direção de Sistemas de Informação	Implementar e gerir todos os sistemas de informação e de infraestrutura tecnológica da INCM, apostando na qualidade, segurança e inovação tecnológica, aplicando as melhores práticas vigentes do mercado e contribuindo para o desenvolvimento de novos negócios.
DME Direção de Manutenção e Engenharia	Prestar serviços de manutenção industrial e engenharia às áreas fabris, laboratórios, infraestruturas técnicas de produção e rede elétrica da INCM, garantindo a sua operacionalidade.
DCS Direção de Compras e Suporte ao Negócio	Assegurar um processo eficiente de aquisição de todos os bens e serviços necessários para a INCM desenvolver a sua atividade e gerir as atividades de suporte ao negócio com os clientes de forma a cumprir as suas expectativas.
SLG Serviço de Logística	Assegurar a gestão integrada da cadeia logística da INCM, incluindo a receção de materiais, gestão de existências e expedição de produtos, contribuindo para a eficácia e eficiência das suas atividades.
SLI Serviço de Laboratório Industrial	Assegurar a realização de ensaios laboratoriais nas diferentes unidades de negócio e em clientes externos, bem como a verificação metrológica dos equipamentos de medição e ensaio da INCM, contribuindo para a qualidade dos respetivos produtos e processos.

SUPORTE À ORGANIZAÇÃO

Unidade Orgânica	Missão
DDP Direção de Desenvolvimento de Pessoas	Otimizar o desempenho e desenvolvimento das pessoas, garantindo as melhores condições de trabalho e de bem-estar, através de uma comunicação fluida e eficaz, promovendo iniciativas eficientes e sustentáveis e assegurando a concretização dos objetivos estratégicos da empresa.
DCF Direção de Contabilidade e Finanças	Gerir com rigor e disponibilizando com tempestividade os recursos financeiros, observando os normativos e a legislação contabilística e fiscal, constituindo um instrumento essencial de orientação para os objetivos da empresa.
DJU Direção de Serviços Jurídicos	Prestar apoio jurídico à atividade de todos os órgãos e serviços da INCM, defendendo e valorizando os interesses da empresa.
DMO Direção de Manutenção, Obras e Apoio Geral	Implementar e gerir todas as infraestruturas com caráter técnico de apoio à empresa, apostando na eficiência, sustentabilidade, qualidade e melhoria dos serviços internos, na segurança e saúde no trabalho, na projeção e execução dos projetos e obras referentes ao edificado da INCM, garantindo condições físicas e ambientais adequadas à atividade de cada trabalhador.
SSI Serviço de Segurança Interna	Assegurar os mecanismos e os serviços de segurança física nas instalações da INCM, garantindo a proteção das pessoas e bens.
DCR Direção de Comunicação e Relações Institucionais	Assegurar a comunicação institucional interna e externa, contribuindo para o posicionamento e crescimento da empresa no mercado e para uma cultura e clima organizacional transparentes e colaborativos.

Na sua estrutura organizacional, a INCM contempla ainda os Comités, órgãos não executivos, que desenvolvem uma atividade transversal a diversas áreas da empresa, onde existem elementos das diversas unidades orgânicas. Constitui-se, então, como órgão agregador das diferentes competências da INCM, no desenvolvimento de atividades específicas.

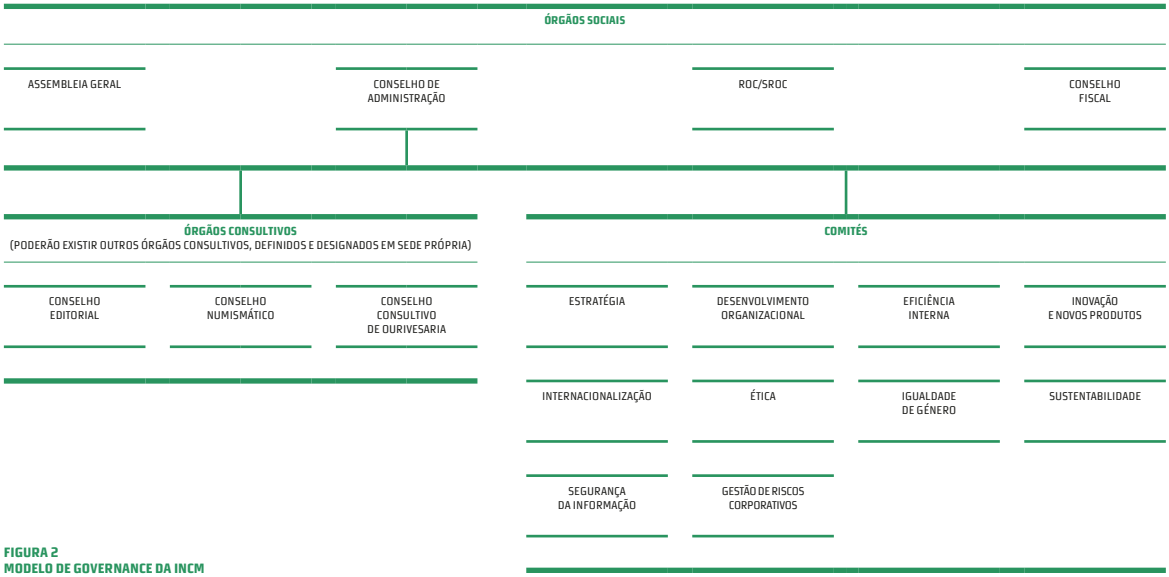

FIGURA 2
MODELO DE GOVERNANCE DA INCM

Comités para Acompanhamento da Execução do Plano de Investimento e de Objetivos Programáticos:

› **Comité de Estratégia**, que tem por objetivo impulsionar o desenvolvimento estratégico da INCM e a adaptação das várias atividades e áreas de responsabilidade, revendo o cumprimento dos objetivos constantes do plano estratégico e do contrato de gestão com o acionista;

› **Comité de Desenvolvimento Organizacional,** cuja missão é fomentar o desenvolvimento organizacional da INCM, acompanhando a evolução do respetivo modelo organizativo, articulando as políticas de desenvolvimento de recursos humanos e promovendo uma cultura alinhada com a estratégia e os valores da INCM;

› **Comité de Eficiência Interna**, que procura acompanhar a execução dos programas e projetos, com o intuito de aumentar a eficiência interna da INCM, articulando as diferentes áreas envolvidas e desenvolvendo uma cultura de eficiência em toda a organização;

› **Comité de Inovação e Novos Produtos**, cuja missão é promover o desenvolvimento da inovação na INCM, com o intuito de assegurar a integração contínua da investigação, do desenvolvimento e da inovação (ID&I) na organização, nos processos e nos produtos e

serviços da INCM, dotando a organização de capacidade de inovar a sua oferta e de responder às exigentes condições dos mercados, antecipando as necessidades dos seus clientes;

› **Comité de Internacionalização**, cujo intuito é promover o desenvolvimento sustentável do negócio da INCM nos mercados internacionais, através da consolidação de parcerias estratégicas, do reforço da competitividade e do alinhamento dos vários intervenientes internos, promovendo simultaneamente a capacitação da organização para a resposta aos desafios daí decorrentes.

Comités para acompanhamento das linhas orientadoras:

› **Comité de Ética**, cuja principal função é estabelecer os procedimentos relacionados com as questões de ética e de deontologia na INCM, e, simultaneamente com a articulação dos órgãos competentes nesta matéria, no âmbito do Código de Ética e de Conduta da INCM;

› **Comité de Igualdade de Género**, que fornece apoio e acompanhamento à implementação do Plano de Igualdade;

› **Comité de Sustentabilidade**, que visa a promoção da integração dos princípios da sustentabilidade no processo de gestão da empresa, alinhando a INCM com as melhores práticas nesta temática;

› **Comité para a Segurança da Informação**, cuja missão se foca no cumprimento dos requisitos da segurança da informação, de modo eficaz e consistente, em toda a INCM, de acordo com as boas práticas e normas aplicáveis, constituindo-se como órgão consultivo e supervisor do Sistema de Gestão de Segurança da Informação;

› **Comité para a Gestão de Riscos Corporativos**, que vem apoiar e orientar o CA em todas as matérias relativas à gestão de riscos corporativos, garantindo a supervisão neste domínio.

3.3. SISTEMA INTEGRADO DE GESTÃO

A INCM tem instituído um Sistema Integrado de Gestão (SIG) suportado em boas práticas de gestão que, maioritariamente, decorrem da implementação de normas nacionais e internacionais pelas quais a empresa se encontra certificada ou em vias de certificação.

O SIG pretende assegurar a integração e desenvolvimento dos processos da organização em três pilares estratégicos: Governança, Risco e Conformidade, tal como ilustrado no seu organograma funcional (Figura 3).

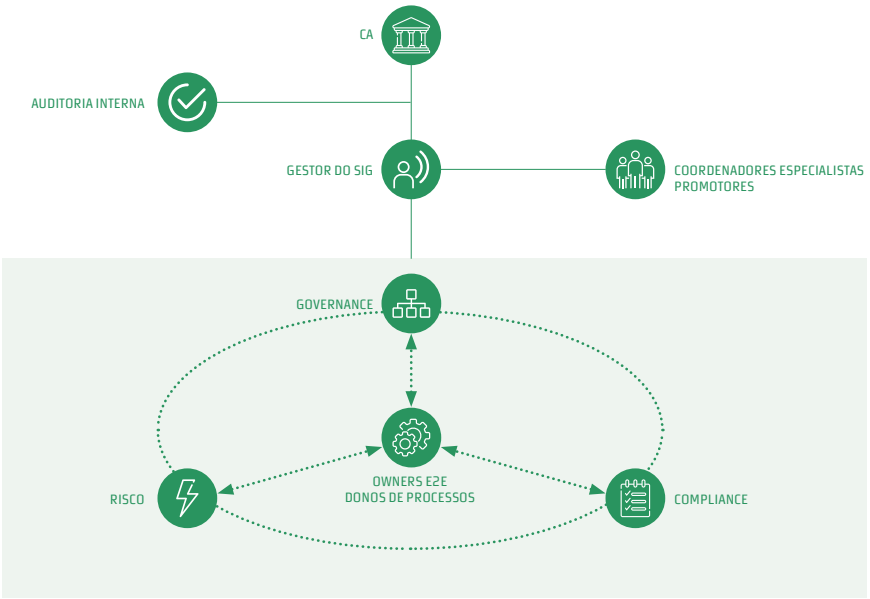

FIGURA 3
ORGANOGRAMA FUNCIONAL DO SISTEMA INTEGRADO DE GESTÃO

Sobre o pilar da Governança, o SIG tem o objetivo de garantir a execução de projetos e iniciativas de melhoria decorrentes de não conformidades com requisitos, gestão de risco, expectativas das partes interessadas, ou outras fontes de informação relevantes, definindo e implementando planos de ação conforme apropriado. Adicionalmente, deve analisar e avaliar o desempenho e eficácia do sistema através da identificação de objetivos e indicadores chaves de performance (KPI).

No âmbito do Risco, é necessário assegurar a execução de medidas de mitigação decorrentes da identificação, análise e avaliação dos riscos da organização, certificando que a informação de risco se encontra atualizada, consolidada e devidamente comunicada.

Sobre o pilar do *Compliance* é necessário que o sistema assegure uma atuação íntegra com os requisitos internos e externos da organização, identificando, analisando e atuando sobre não conformidades e ações corretivas identificadas.

O Programa «Mudar a Casa» tem como objetivo transformar a organização de forma a torná-la mais simples, mais eficiente, mais integrada e mais automatizada. Nesse sentido e com base numa análise crítica

à cadeia de valor da INCM, encontram-se identificados 13 processos *End-to-End* (E2E), que se entende cobrirem na íntegra toda a atividade e negócio da INCM e que aqui se dão conhecimento:

- Da Ideia ao Produto tem como propósito a inovação e desenvolvimento de negócio, partindo da conceção e desenvolvimento de ideias e de produtos novos, realização de testes e operacionalização dos mesmos;
- Da Oportunidade ao Negócio tem como finalidade a comercialização dos produtos e serviços oferecidos pela empresa, começando com a análise e prospeção de mercado, identificação de oportunidades de negócio e conclusão do negócio, gerindo os canais de venda que a INCM dispõe ao cliente;
- Do Planeamento à Entrega demonstra as várias fases produtivas desde o planeamento até a produção de produtos/serviços comercializados/oferecidos pela organização nas suas várias vertentes;
- Da Procura ao Pagamento visa o alinhamento organizacional na aquisição de bens e serviços a fornecedores externos desde o planeamento anual até ao pagamento de faturas;
- Da Encomenda à Faturação ilustra as atividades desde a receção e registo de encomendas até ao processamento dos recebimentos, tendo por objetivo realizar atividades administrativas do processo de venda, receber e planear as encomendas, garantir o transporte e descarga dos produtos, bem como faturar, controlar recebimentos e gerir as dívidas dos clientes (quando necessário);
- Governança, Risco e Conformidade tem como objetivo assegurar a eficiência, eficácia e melhoria contínua do SIG, controlar os riscos decorrentes do normal funcionamento da organização, garantir a conformidade da organização com as normas aplicáveis, e regulamentos, assim como a legislação vigorante, bem como delinear e realizar auditorias internas ou trabalhos de consultoria internos;
- Estratégia, Gestão e Orçamentação visa definir a estratégia de negócio e alocar os recursos necessários para que os objetivos sejam alcançados, comparando a performance financeira com o que foi planeado/orçamentado e redefinindo as estimativas, tendo em consideração as análises efetuadas, bem

como a viabilidade económica e necessidade de investimento de novos projetos;

- Do Registo ao Reporte Financeiro tem como objetivo recolher e processar toda a informação contabilística e financeira, com a finalidade de produzir tanto as demonstrações financeiras legais como os relatórios de gestão;

- Do Recrutamento à Saída/Reforma compreende os processos relacionados com a gestão administrativa dos recursos humanos, em todo o ciclo de vida do colaborador na INCM, desde a contratação à sua aposentação garantindo sempre o cumprimento dos requisitos legais aplicáveis;

- Da Aquisição ao Abate visa gerir todas as atividades relacionadas com o ciclo de vida dos ativos não fabris da organização como também a gestão de imobilizado e de obras;

- Segurança tem como objetivo assegurar uma visão transversal sobre toda a segurança de espaços físicos e lógicos da INCM, bem como garantir a prevenção e os procedimentos em caso de violação das suas políticas;

- Gestão de Recursos garante a gestão dos processos não core da organização, no entanto fundamentais para o seu correto funcionamento, nomeadamente a gestão do espaço físico de trabalho e de recursos administrativos;

- Gestão de Sistemas de Informação tem como propósito assegurar o suporte tecnológico dos processos, sejam eles transacionais ou analíticos, operacionais ou de suporte.

Um E2E trata-se assim de um macroprocesso desenhado numa lógica de cadeia de valor e/ou finalidade global no contexto da organização.

4. CONTROLOS PARA A PREVENÇÃO DE CORRUPÇÃO E INFRAÇÕES CONEXAS

Por forma a assegurar uma gestão adequada em matéria de prevenção de corrupção e infrações conexas a INCM tem implementado um conjunto de processos, políticas, práticas e ações que procuram mitigar os riscos existentes.

Destes destaca-se o Código de Ética e de Conduta, que define as regras de conduta que devem pautar o comportamento de todos os colaboradores no desempenho na sua atividade profissional. Nele destaca-se que «o cumprimento dos princípios de imparcialidade e independência são incompatíveis com a aceitação pelos colaboradores e colaboradoras da INCM, em benefício próprio ou de terceiros, de ofertas, prémios ou outros benefícios que possam ser considerados ou interpretados como uma tentativa de influenciar a empresa ou o(a) colaborador(a)». O Código aborda o dever de assegurar o sigilo profissional sobre as informações confidenciais obtidas no desempenho das suas funções ou em consequência desse desempenho. Em matéria de conflitos de interesses, e em resposta à recomendação do Conselho de Prevenção da Corrupção (CPC) de 8 de janeiro de 2020, e disposto no Código de Ética e de Conduta, os colaboradores e as colaboradoras da INCM:

- Sempre que, no exercício da sua atividade, sejam chamados a intervir em processos de decisão que envolvam, direta ou indiretamente, organizações com as quais colaborem ou tenham colaborado, ou ainda pessoas a que estejam ou tenham estado ligados por laços de parentesco ou afinidade, devem declarar-se impedidos e comunicar ao Comité de Ética e ou às chefias respetivas a existência dessas ligações;

- Com relações familiares ou equiparadas não deverão exercer a sua atividade profissional em relação hierárquica ou funcional direta;

- Devem abster-se de exercer quaisquer funções fora da empresa sempre que tais atividades ponham em causa o cumprimento dos seus deveres enquanto colaboradores(as) da INCM, ou em organizações cujos objetivos possam colidir ou interferir com os objetivos da INCM.

O Código de Ética e de Conduta é ainda divulgado no site da INCM[2], na intranet e disponibilizado a todos os colaboradores e colaboradoras, nos formatos impresso e ou digital, bem como em

[2] O Código de Ética e de Conduta da INCM pode ser consultado em: https://incm.pt/portal/incm_codetica.jsp

formato *e-learning*. A aceitação das regras emanadas no Código é parte integrante do contrato de trabalho e consequentemente a sua aceitação e cumprimento são obrigatórios para todos os colaboradores. O mesmo princípio é aplicado em todos os contratos estabelecidos com fornecedores, parceiros e clientes.

A INCM tem ainda definida uma Política de Gestão de Recursos Humanos. Nela, e para o efeito do presente Plano, destacam-se as regras estabelecidas para assegurar processos de recrutamento e seleção concorrenciais norteados pela aplicação de estratégias que têm em consideração a isenção, a transparência, a igualdade de oportunidades e o respeito pelas diferenças individuais.

É ainda definido como política que, após aprovação da contratação do colaborador, este deve assinar uma Declaração de Confidencialidade (*Non-Disclosure Agreement* ou NDA) e submeter, dependendo da função a desempenhar, registo criminal, que deve ser atualizado anualmente ou trianualmente.

Por forma a assegurar o princípio de segregação de funções nas tomadas de decisões, em particular no respeitante a decisões e aprovações, a INCM define um perfil de competências à função e ainda, por deliberação do Conselho de Administração, aprova o documento de delegação de competências e poderes.

A INCM tem ainda operacionalizado um Sistema de Gestão de Segurança da Informação, o qual se encontra certificado no âmbito do processo de produção do cartão tacógrafo pela ISO 27001:2013, e de acordo com a ISO 14298:2013 — Sistema de Gestão de Produção Gráfica de Segurança no que diz respeito à produção e personalização de passaportes, vistos Schengen, documentos de identificação, cartões de crédito, títulos de residência e cartas de condução, demonstrando a preocupação da organização em preservar a confidencialidade, integridade e disponibilidade da informação.

Nesse âmbito é consagrada a Política de Segurança da Informação, onde se destaca como regra o Princípio de Privilégio Mínimo de Acesso à Informação, que define que os colaboradores apenas devem ter acesso à informação estritamente necessária para o cumprimento das suas funções. A política descreve ainda os controlos de acesso físico e lógicos existentes por forma a assegurar uma correta segregação e utilização dos ativos da organização.

No respeitante ao processo de aquisição de bens e serviços, a INCM rege-se em conformidade com o Código dos Contratos Públicos, asseg-

urando assim um processo de aquisição concorrencial com estratégias definidas para assegurar a transparência, integridade e isenção do processo de identificação e seleção de fornecedores.

A INCM implementou ainda em maio de 2020 o procedimento para Identificação e Diligência de Clientes e Parceiros, cujo objetivo é a identificação e diligência de clientes e parceiros no estabelecimento de relações de negócio, centrado nos riscos relacionados com o branqueamento de capitais ou com o financiamento do terrorismo (BC/FT).

Anualmente é também publicado o Relatório de Execução do Plano de Gestão de Riscos de Corrupção e Infrações Conexas, que sumariza os controlos implementados por forma a melhorar o sistema de controlo interno da INCM e consequentemente assegurar um melhor combate à corrupção e infrações conexas.

Neste âmbito importa ainda realçar que a INCM aderiu à iniciativa do setor empresarial intitulada *Call to Action: Anti-Corruption and the Global Development Agenda* com o propósito de assumir um compromisso com a adoção generalizada de medidas anticorrupção eficazes, bem como a promoção de políticas que incentivem boas práticas neste domínio.

5. GESTÃO DE RISCO

A gestão de riscos corporativos é um processo de gestão que tem como objetivo identificar, analisar e mitigar os riscos que possam interferir com as operações e objetivos da organização. Focada na prevenção e proteção dos seus ativos, a INCM assume a gestão de riscos corporativos como parte integrante da gestão, com o propósito de promover uma cultura onde são privilegiadas medidas preventivas para assegurar o cumprimento dos objetivos.

Nesse sentido, a INCM estabelece uma Framework de Gestão de Riscos Corporativos que define os elementos que fornecem os fundamentos e disposições organizacionais para conceber, implementar, monitorizar, rever e melhorar continuamente a gestão do risco na INCM. A framework tem como objetivo:

- Promover a criação de valor da gestão de risco, assegurando que as tomadas de decisão consideram a informação de risco pertinente e os princípios da gestão de risco se encontram alinhados com a missão e estratégia da INCM;

- Promover uma cultura de gestão de risco onde são privilegiadas medidas preventivas para assegurar o cumprimento de objetivos;
- Assegurar a consciencialização dos intervenientes através da identificação das funções e responsabilidades na estrutura de gestão de riscos corporativos e respetiva formação e sensibilização;
- Promover a partilha e o reúso da informação de risco nos diferentes contextos da INCM através da definição de referenciais transversais à organização;
- Assegurar a conformidade do processo de gestão de risco com requisitos externos (normativos, legais, etc.) e internos.
- Os principais objetivos para a gestão de riscos corporativos são estabelecidos em concordância com os objetivos estratégicos da INCM, através da definição das categorias de risco que se desejam ver abordadas, sendo uma das categorias a da prevenção e combate à corrupção e infrações conexas.

Processo de Gestão de Risco

O processo de gestão de risco implementado na INCM é baseado nas normas ISO 31000:2018, e ISO/IEC 27001:2013 e estabelece um conjunto de atividades (representadas na Figura 4) para a eficiente gestão de riscos na organização.

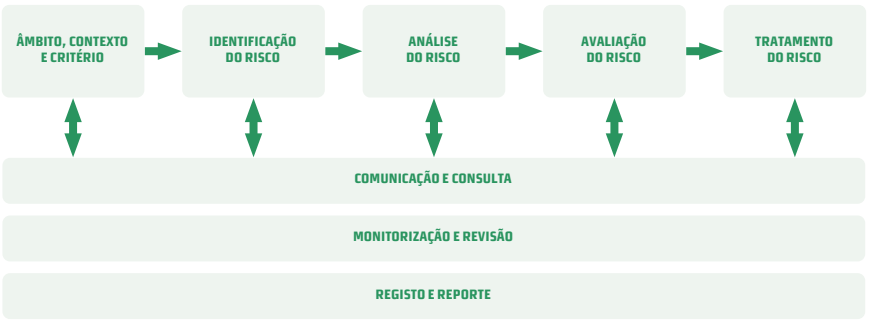

FIGURA 4
PROCESSO DE GESTÃO DE RISCO CORPORATIVO

O estabelecimento do referencial consiste na definição do âmbito onde a gestão de risco será implementada. A atividade identifica o referencial a utilizar para a identificação do risco e é, por-

tanto, essencial para as restantes atividades do processo. Para o presente Plano de Gestão de Riscos de Corrupção e Infrações Conexas foi estabelecida uma identificação de riscos orientada aos processos E2E identificados no SIG.

A identificação do risco consiste na identificação da causa e da consequência do evento que caracteriza o risco. Adicionalmente, a identificação de risco contempla a identificação dos controlos existentes e do dono do risco. A identificação do risco é da responsabilidade dos donos de processo.

Adicionalmente, os riscos identificados são categorizados de acordo com a sua descrição. Para o presente Plano foram consideradas as seguintes categorias de risco:

- Risco de abuso de direitos, relacionado com o risco de efetuar operações sem a devida autorização, o que pode indiciar um crime de tráfico de influência, conflito de interesses, abuso de poder ou de participação económica em negócio. Nesta tipologia foram incluídos riscos das categorias de abuso de direitos, idoneidade do cliente, incumprimento de procedimentos internos e operações não autorizadas;

- Risco de divulgação de informação, que pode indicar um crime de violação de segredo por funcionário. Nesta tipologia foram incluídos riscos de divulgação de informação;

- Risco de falha humana, que pode, caso a falha seja intencional, indiciar um crime de recebimento indevido de vantagem. Nesta tipologia foram incluídos riscos de falha humana;

- Risco de indisponibilidade de informação para a correta execução do processo, o que pode indiciar um crime de concussão. Nesta tipologia foram incluídos riscos de indisponibilidade de informação;

- Risco de integridade de informação comprometida relacionado com informação errada ou manipulada de forma intencional, ou sem autorização, o que pode indiciar um crime de recebimento indevido de vantagem ou participação económica em negócio. Nesta tipologia foram incluídos riscos das categorias de indução em erro, perda de informação de segurança e acesso não autorizado a ativos de segurança;

- Risco de recuperação de produtos ou matérias-primas para

destruição relacionado com a utilização abusiva de produtos ou matérias-primas destinados à destruição, o que pode indiciar um crime de recebimento indevido de vantagem, ou peculato. Nesta categoria foram incluídos riscos de recuperação de produtos ou matérias-primas de segurança para destruição;

› Risco de extravio de bens relacionado com o extravio de ativos da organização, o que pode indicar um risco de peculato ou peculato de uso. Nesta tipologia foram incluídos riscos das categorias de extravio de ativos, extravio de produtos ou matérias-primas de segurança.

Os riscos de corrupção e infrações conexas encontram-se descritos no anexo II.

A análise do risco consiste em medir os riscos anteriormente identificados com recurso às métricas de probabilidade, impacto e nível do risco. Para permitir a comparação da informação de risco é necessário que as métricas possuam escalas comparáveis. No entanto e reconhecendo a existência de diversos contextos da gestão do risco é expectável que as métricas possuam diferentes dimensões consoante o contexto. A estimativa das métricas definidas é da responsabilidade dos donos do risco identificados na atividade anterior. O anexo I apresenta os critérios de análise. O anexo III identifica a avaliação dos riscos de corrupção e infrações conexas.

A avaliação do risco consiste no processo de comparação dos resultados da análise do risco para determinar se o risco é aceitável ou tolerável consoante o nível do risco estimado. A decisão de tratamento deve ser baseada no nível do risco definido. A avaliação do risco consiste na identificação dos controlos para os riscos não aceitáveis. Um controlo pode tratar-se de um processo, política, dispositivo, prática ou outra ação que modifique o risco.

O tratamento do risco consiste no planeamento e implementação dos controlos identificados na atividade anterior. A implementação do controlo deve ser verificada periodicamente pelos donos do risco. Se, após tratamento, o risco ainda apresentar um nível de risco alto então deve-se identificar e implementar novo controlo.

A monitorização e revisão da gestão de riscos corporativos envolve a verificação, periódica ou idealmente contínua, da informação de risco aquando de mudanças de contexto interno ou externo.

Para garantir que as partes interessadas entendem e conseguem utilizar a informação de risco, é essencial que as atividades de risco envolvam a comunicação e consulta constante com essas partes. Neste contexto, o registo e reporte é assegurado através da produção de relatórios de riscos que incluem a informação possível e necessária, estruturada e apresentada de acordo com as preocupações e necessidades do destinatário.

ANEXO I
CRITÉRIOS DE ANÁLISE DE RISCO

PONTUAÇÃO	DESCRIÇÃO	PROBABILIDADE		FREQUÊNCIA
5	Esperado	É esperado que o evento ocorra	80-90%	O evento ocorreu ou é previsível que possa ocorrer uma vez nos próximos 6 meses
4	Muito provável	O evento pode ocorrer na maioria das circunstâncias	60-79%	O evento ocorreu ou é previsível que possa ocorrer uma vez nos próximos 12 meses
3	Provável	O evento irá provavelmente ocorrer	40-59%	O evento ocorreu ou é previsível que possa ocorrer uma vez nos próximos 18 meses
2	Não provável	O evento não é provável, mas pode ocorrer	20-39%	O evento ocorreu ou é previsível que possa ocorrer uma vez nos próximos 24 meses
1	Raro	É estimado que o evento ocorre apenas em circunstâncias excecionais	1-19%	O evento ocorreu ou é previsível que possa ocorrer uma vez nos próximos 48 meses

TABELA 1. PROBABILIDADE DO RISCO

PONTUAÇÃO	DESCRIÇÃO	SIGNIFICADO
5	Muito Alta	Controlo de prevenção redundante avaliado e continuamente monitorizado
4	Alta	Controlo de prevenção redundante com eficácia avaliada e verificada
3	Moderada	Controlo de prevenção redundante não avaliado ou monitorizado
2	Baixa	Controlo de prevenção não redundante dependendo de ação humana ou sujeito a falhas
1	Muito Baixa	Controlo de prevenção inexistente

TABELA 2. EFICÁCIA DO CONTROLO DE PREVENÇÃO

PROBABILIDADE DE PERDA DERIVADA

		PROBABILIDADE DO EVENTO				
		Raro	Não Provável	Provável	Muito Provável	Esperado
Eficácia do controlo de prevenção	Muito Baixa	Muito Baixa	Baixa	Moderada	Alta	Muito Alta
	Baixa	Muito Baixa	Muito Baixa	Baixa	Moderada	Alta
	Moderada	Muito Baixa	Muito Baixa	Muito Baixa	Baixa	Moderada
	Alta	Muito Baixa	Muito Baixa	Muito Baixa	Muito Baixa	Baixa
	Muito Alta	Muito Baixa	Muito Baixa	Muito Baixa	Muito Baixa	Muito Baixa

TABELA 3. PROBABILIDADE DE PERDA DERIVADA

MATRIZ DE IMPACTO NEGATIVO

	1 Insignificante	2 Baixo
ESTRATÉGICO	› Atraso ou desvio no plano de ações › Sem impacto nas metas estabelecidas	› Impede o cumprimento de uma ou mais metas intercalares estabelecidas › Sem impacto no cumprimento dos indicadores
OPERACIONAL	› Impacto insignificante nos processos de negócio › Impacto pode ser mitigado com operações de rotina	› Impacto baixo nos processo de negócio › Pode originar atrasos recuperáveis › Impacto pode ser mitigado ao nível operacional
FINANCEIRO	› Impacto financeiro insignificante (<250m€) › <1% impacto no custo do projeto	› Impacto financeiro baixo (250m€ - 500m€) › 2-5% impacto no custo do projeto
REPUTACIONAL	› Incidente com publicidade negativa limitada. Rapidamente esquecido. › Sem dano na reputação/marca	› Incidente com publicidade negativa a nível local/regional › Dano baixo limitado (curto prazo) na reputação/marca
SEGURANÇA DE INFORMAÇÃO*	› Ativos de segurança de informação de valor muito baixo comprometidos no que diz respeito à confidencialidade, integridade, ou disponibilidade	› Ativos de segurança de informação de valor baixo comprometidos no que diz respeito à confidencialidade, integridade, ou disponibilidade
REGULAMENTAR	› Perigo de incorrer em incumprimento legal, contratual ou normativo	› Ato isolado em incumprimento legal ou normativo › Incumprimento contratual detetado por uma das partes
SEGURANÇA NO TRABALHO	› Lesões insignificantes › Perdas materiais insignificantes	› Lesões que requerem primeiros socorros › Perdas materiais baixas recuperáveis a curto prazo (< 24horas)
AMBIENTAL	› Impacto ambiental insignificante	› Impacto ambiental baixo reparável

*Sempre que seja identificado um risco com impacto nos ativos de segurança de informação deve ser identificado em que pilar da segurança da informação (confidencialidade, integridade ou disponibilidade) este foi afetado.

TABELA 4. MATRIZ DE IMPACTO NEGATIVO

3 Moderado	4 Elevado	5 Severo
› Impede o cumprimento de um ou mais indicadores estabelecidos › Sem impacto no cumprimento dos objetivos	› Impede o cumprimento de um ou mais objetivos estabelecidos	› Impede o cumprimento de um ou mais objetivos estratégicos da organização
› Impacto moderado nos processos de negócio › Performance do negócio afetada impedimento o cumprimento de metas estratégicas	› Impacto elevado nos processos de negócio › Performance do negócio afetada com consequências negativas elevadas (atrasos no serviço, perdas financeiras, insatisfação cliente, quebras regulamentares, etc.)	› Impacto severo nos processos de negócio › Indisponibilidade de serviços e/ou pessoas criticas ao negócio
› Impacto financeiro moderado (500m€ - 750m€) › 5-10% impacto no custo do projeto	› Impacto financeiro elevado (750m€ - 1M€) › >10% impacto no custo do projeto	› Impacto financeiro severo (>1M€) › >30% impacto no custo do projeto
› Incidente com publicidade negativa a nível local/regional › Pressão para a INCM mitigar impacto › Dano moderado para reputação/ marca	› Incidente com publicidade negativa a nível nacional › Pressão intensa para INCM mitigar impacto › Dano elevado para reputação/marca	› Incidente com publicidade negativa a nível internacional › Mitigação de impacto requer mudanças estratégicas › Dano severo para reputação/marca
› Ativos de segurança de informação de valor moderado comprometidos no que diz respeito à confidencialidade, integridade, ou disponibilidade	› Ativos de segurança de informação de valor alto comprometidos no que diz respeito à confidencialidade, integridade, ou disponibilidade	› Ativos de segurança de informação de valor crítico comprometidos no que diz respeito à confidencialidade, integridade, ou disponibilidade
› Atividade ou rotina em incumprimento legal ou normativo › Incumprimento contratual com ameaça de quebra contratual ou penalizações	› Incumprimento legal resultante em investigação por parte das autoridades › Incumprimento contratual com penalizações › Incumprimento normativo sujeito a não conformidade maior	› Incumprimento legal resultante em graves penalizações › Incumprimento contratual com quebra de contrato › Incumprimento normativo sujeito a perda de certificação
› Lesões ou doenças que requerem intervenção médica (cortes fundos, fraturas, queimaduras, etc.) › Perdas materiais moderadas com recuperação a longo prazo (>24 horas)	› Lesões sérias implicando ausência prolongada. Baixa superior a 30 dias › Perdas materiais elevadas com recuperação parcial a longo prazo (>24 horas). Requer renovação ou substituição de materiais	› Lesões severas (perdas de membros, audição, visão, etc.) ou morte › Perdas materiais severas irrecuperáveis. Requer substituição de equipamento
› Impacto ambiental moderado com necessidade de ações de mitigação	› Impacto ambiental elevado com danos parciais irreversíveis	› Impacto ambiental severo com danos irreversíveis

NÍVEL DE RISCO

		IMPACTO MÁXIMO				
Insignificante		Baixo	Moderado	Elevado	Severo	
Probabilidade de perda derivada	Muito Alta	Baixo	Baixo	Alto	Muito Alto	Muito Alto
	Alta	Muito Baixo	Baixo	Moderado	Alto	Muito Alto
	Moderada	Muito Baixo	Baixo	Moderado	Moderado	Alto
	Baixa	Muito Baixo	Muito Baixo	Baixo	Moderado	Moderado
	Muito Baixa	Muito Baixo	Muito Baixo	Muito Baixo	Baixo	Moderado

TABELA 5. NÍVEL DE RISCO

NÍVEL DO RISCO (Probabilidade x Impacto)

Muito Alto	Ação imediata deve ser tomada de forma a mitigar o risco
Alto	Devem ser alocados esforços para mitigar o risco logo que possível
Moderado	Risco deve ser mitigado. Eficácia dos controlos deve ser monitorizada
Baixo	Risco pode ser aceite/rejeitado. Controlo do risco deve ser efetuado com base numa análise custo/benefício
Muito Baixo	Risco pode ser aceite/rejeitado pois não representa uma ameaça para a organização. Deve ser monitorizado de forma a garantir que não se altera

TABELA 6. MEDIDAS DE TRATAMENTO RECOMENDADAS

ANEXO II IDENTIFICAÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

PROCESSO E2E – DA AQUISIÇÃO AO ABATE

Categoria do Risco	Evento	Causa	Consequência
Reputação e Imagem - Incumprimento de Procedimentos Internos	Beneficiar uns clientes em relação a outros	Pressão por parte do cliente (por exemplo cliente interno)	Prazos acordados, falta de imparcialidade na forma de atuar
Limite de Autoridade - Abuso de Direitos	Aquisição de bens/ serviços não decorrente de necessidades reais	Ação deliberada para proveito próprio	Corrupção e Infrações Conexas
Segurança da Informação - Divulgação de Informação Confidencial	Divulgação externa de informação confidencial	Erro humano ou ação deliberada para proveito próprio	Quebra de confidencialidade de informação com dano para imagem, reputação da INCM e/ou informação crítica para o negócio divulgada
Limite de Autoridade - Abuso de Direitos	Manipulação de ensaios laboratoriais para seleção de fornecedor	Acão deliberada para proveito próprio	Processo concorrencial comprometido
Limite de Autoridade - Abuso de Direitos	Faturação indevida de manutenção e obras	Sobreavaliação das medições dos trabalhos Indução em erro da avaliação final da obra/ manutenção Cobrança de trabalhos a mais	Derrapagem ou aumento de custos planeados
Limite de Autoridade - Indução em Erro	Inexistência, ou existência deficiente, de estimativas de custo para a realização das obras/manutenção	Acão deliberada para proveito próprio	Derrapagem ou aumento de custos planeados
Segurança da Informação - Perda de Informação de Segurança	Indisponibilidade da informação para recuperação de avaria	Inexistência de backups ou backup corrompido	Tempo de resolução de avaria demorado Incumprimento de normas
Segurança da Informação - Operação Não Autorizada	Alteração indevida dos parâmetros das máquinas produtivas	Necessidade operacional de conceder acesso remoto limitado a fornecedores	Dano nos produtos de segurança e/ou nas máquinas produtivas
Qualidade do Produto/ Serviço - Falha Humana	Resultados incorretos	Utilização de equipamento inadequado ao ensaio laboratorial	Produto não conforme Reclamação
Qualidade do Produto/ Serviço - Falha Humana	Amostras danificadas	Manuseamento inadequado dos artigos, amostras a ensaiar	Incapacidade de realizar serviço Incumprimento de SLA
Eficácia e Eficiência - Indisponibilidade de Informação	Ineficiência de processo de gestão de cablagem elétrica	Ausência de placas sinaléticas nos quadros elétricos	Indisponibilidade de produção Incumprimento de boas práticas de segurança

PROCESSO E2E – DA AQUISIÇÃO AO ABATE

Categoria do Risco	Evento	Causa	Consequência
Eficácia e Eficiência - Indisponibilidade de Informação	Ineficiência de processo de gestão de cablagem elétrica	Ausência de etiquetagem da cablagem elétrica	Indisponibilidade de produção Incumprimento de boas práticas de segurança

PROCESSO E2E – DA ENCOMENDA À FATURAÇÃO

Categoria do Risco	Evento	Causa	Consequência
Perda e/ou Obsolescência - Extravio de Ativos	Extravio de produtos/ valores	Roubo por cliente ou funcionário	Perda do produto/valores

PROCESSO E2E – DA OPORTUNIDADE AO NEGÓCIO

Categoria do Risco	Evento	Causa	Consequência
Segurança da Informação - Perda de Informação de Segurança	Violação ou destruição de dados via ficheiros informáticos	Clientes que enviam informação sensível (ex. dados pessoais) através de ficheiros não protegidos via *email* que, por sua vez, circulam da mesma forma internamente entre DCO e UGF|PER	Divulgação ou destruição de informação confidencial e dados de produção
Segurança da Informação - Divulgação de Informação Confidencial	Divulgação de informação confidencial de dados comerciais	Erro humano ou ação deliberada para proveito próprio	Quebra de confidencialidade de informação com dano para imagem, reputação da INCM e/ou informação crítica para o negócio divulgada
Reputação e Imagem - Incumprimento de Procedimentos Internos	Produção de espécimes sem o conhecimento e autorização prévia do cliente	Inexistência/ incumprimento de procedimentos internos relativos à produção e distribuição de espécimes	Circulação de produtos sem controlo por parte do dono do produto
Reputação e Imagem - Idoneidade do Cliente	Fornecimento de produtos a cliente não autorizado	Fornecimento de produtos a clientes não autorizados a ter acesso a esses produtos	Utilização abusiva de produtos de segurança

PROCESSO E2E – DA OPORTUNIDADE AO NEGÓCIO

Categoria do Risco	Evento	Causa	Consequência
Qualidade do Produto/ Serviço - Falha Humana	Pedido de documentos para postos não autorizados (aplicável a situações com tabelas de recebedor e emissor codificados associadas a produto)	Engano no registo dos pedidos por parte do cliente	Entrega de documentos em balcões do cliente trocados
Reputação e Imagem - Idoneidade do Cliente	Fornecimento de produtos a cliente não autorizado	Pedido de encomenda de cartões por representantes de entidade não autorizada	Utilização abusiva de produtos de segurança
Cadeia de Fornecimento - Indisponibilidade de Informação	Atraso na produção de peças para cunhagem	Atraso na entrega de materiais pelos autores	Atraso na produção e na venda de moedas

PROCESSOS E2E - DA PROCURA AO PAGAMENTO

Categoria do Risco	Evento	Causa	Consequência
Segurança da Informação - Divulgação de Informação Confidencial	Fuga de informação confidencial por fornecedores ou empresas subcontratadas	Não cumprimento dos requisitos de segurança por parte dos fornecedores ou empresas subcontratadas	Informação confidencial comprometida
Limite de Autoridade - Indução em Erro	Processo de aquisição com informação incompleta (escolha de fornecedor, solicitação de cotação, análise de propostas, etc.)	Ação deliberada para proveito próprio	Corrupção e Infrações Conexas
Limite de Autoridade - Abuso de Direitos	Formalização do processo de compra após aquisição	Ação deliberada para proveito próprio	Corrupção e Infrações Conexas
Limite de Autoridade - Abuso de Direitos	Seleção de fornecedor não tendo como critério as melhores condições	Ação deliberada para proveito próprio	Corrupção e Infrações Conexas
Cadeia de Fornecimento - Indisponibilidade de Informação	Insatisfação das áreas requisitantes	Atraso na entrega dos bens/serviços Fraca qualidade dos materiais	Produto não conforme com requisitos

PROCESSO E2E – DO PLANEAMENTO À ENTREGA

Categoria do Risco	Evento	Causa	Consequência
Reputação e Imagem - Incumprimento de Procedimentos Internos	Produção ou testes realizados na produção sem evidências da devida aprovação por alguém mandatado para tal	Incumprimento dos procedimentos internos estabelecidos e/ou incumprimento do Código de Ética e de Conduta	Fabrico de produtos não autorizados Utilização/ocupação indevida das máquinas produtivas para a realização de testes não autorizados e ausência de rastreabilidade dos materiais de segurança utilizados
Qualidade do Produto/ Serviço - Falha Humana	Peças não conforme com as especificações do cliente	Utilização de punção incorreto (erro humano)	Má qualidade do serviço e indeminização financeira
Eficácia e Eficiência - Indisponibilidade de Informação	Falta de especificações técnicas de produtos	Atraso	Incapacidade de produzir ou produtos finais com especificações erradas
Segurança da Informação - Extravio de Produtos ou Matérias-Primas de Segurança	Extravio de unidades de produto acabado na expedição	Erro humano ou ação deliberada para proveito próprio	Corrupção e Infrações Conexas
Segurança da Informação - Divulgação de Informação Confidencial	Divulgação externa e abusiva de informação do *Mint Directors Working Group*	Erro humano ou ação deliberada para proveito próprio	Quebra de confidencialidade de informação
Eficácia e Eficiência - Falha Humana	Erros na conferência de material rececionado	Falha humana na contagem de material	Registo errado de quantidade em SAP
Perda e/ou Obsolescência - Extravio de Ativos	Roubo ou extravio de peças depositadas na UCF	Vulnerabilidades do processo de guarda e controlo	Incumprimento legal Incidente com publicidade negativa a nível nacional
Qualidade do Produto/ Serviço - Falha Humana	Validade do certificado criptográfico do passaporte inválida	Erro na operação de rotação de certificados	Incumprimento contratual com possível indemnização Possível incidente com publicidade negativa a nível nacional dado que passaportes inválidos são colocados em causa durante controlo de fronteiras
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Acesso não autorizado a quadros elétricos	Chaves acessíveis	Indisponibilidade de alimentação elétrica
Reputação e Imagem - Idoneidade do Cliente	Atribuição de licença indevida	Acão deliberada para proveito próprio Erro humano	Incumprimento legal

PROCESSO E2E – DO PLANEAMENTO À ENTREGA

Categoria do Risco	Evento	Causa	Consequência
Eficácia e Eficiência - Falha Humana	Atrasos (< 24 h) na publicação de atos relevantes	Atraso no envio/extensão do documento	Dano na reputação
Perda e/ou Obsolescência - Extravio de Ativos	Desaparecimento de inventários	Roubo ou extravio	Incapacidade de produzir de acordo com as necessidades
Eficácia e Eficiência - Indisponibilidade de Informação	Falta de ordens de produção	Atraso motivado por falta de informação	Informação indisponível, com riscos de produção desadequada às necessidades
Segurança da Informação - Recuperação de Produtos ou Matérias-Primas de Segurança para Destruição	Falha no processo de destruição e de destino de tintas de segurança a inutilizar (ex. restos de tinta ou tintas obsoletas)	Erro humano na execução	Utilização indevida de tintas de segurança por pessoas não autorizadas e/ou eliminação indevida de resíduos perigosos com impacto ambiental
Eficácia e Eficiência - Falha Humana	Juntar, soldar e furar incorretamente as várias camadas constituintes do cartão	Posicionamento incorreto do *chip (contactless)* na operação de junção de folhas antes da laminagem	Fabrico de produto não conforme
Eficácia e Eficiência - Falha Humana	Seleção de *chip (contact)* incorreto para aplicar em cartão	Aspeto físico muito semelhante entre os módulos-chip	Fabrico de produto não conforme
Eficácia e Eficiência - Falha Humana	Iniciar a preparação e afinação da máquina sem ter em conta as especificações da ordem de produção	Erro humano na execução	Fabrico de produto não conforme
Eficácia e Eficiência - Falha Humana	Gravação incorreta da matriz de impressão (chapa ou película), detetada nas etapas a jusante	Erro humano na execução	Fabrico de produto não conforme
Eficácia e Eficiência - Falha Humana	Requisitar internamente e liberar pedido de compra de matéria-prima com caraterísticas erradas	Erro humano na execução	Fabrico de produto não conforme
Segurança da Informação - Divulgação de Informação Confidencial	Divulgação de elementos confidenciais de marcas	Ação deliberada para proveito próprio	Segurança da marcação comprometida
Perda e/ou Obsolescência - Extravio de Ativos	Extravio de peças preciosas	Ação deliberada para proveito próprio Ausência de Controlos Físicos	Indemnização financeira Dano reputacional

PROCESSO E2E – DO PLANEAMENTO À ENTREGA

Categoria do Risco	Evento	Causa	Consequência
Eficácia e Eficiência - Falha Humana	Orçamentar produto com erro de quantidade de materiais ou fora das especificações do cliente	Erro humano na execução	Trabalho desnecessário e perdas de tempo na execução de novo orçamento
Qualidade do Produto/ Serviço - Falha Humana	Peças danificadas	Erro da técnica ou ferramenta de marcação	Má qualidade do serviço Indeminização financeira
Segurança da Informação - Recuperação de Produtos ou Matérias--Primas de Segurança para Destruição	Recuperação de ferros de punção arrasados	Ação deliberada para proveito próprio	Marcação de peças indevida com marcas oficiais
Segurança da Informação - Extravio de Produtos ou Matérias--Primas de Segurança	Extravio de punção	Ação deliberada para proveito próprio	Marcação de peças indevida com marcas oficiais
Segurança da Informação - Extravio de Produtos ou Matérias--Primas de Segurança	Roubo de punção em serviço de marcação ao domicílio	Transporte de punções durante serviço	Marcação de peças indevida com marcas oficiais
Tecnologia da Informação - Falha Humana	Utilização de chaves criptográficas incorretas	Engano do colaborador	Paragem na produção/ produção de produtos com defeito
Eficácia e Eficiência - Falha Humana	Passaportes furados que impedem leitura na máquina de destruição de PEP's e CC's	Falha nas lojas/SEF/IRN	Falta de produtividade que leva a leitura manual dos artigos
Cadeia de Fornecimento – Indisponibilidade de Informação	Envio de produtos para locais onde não é possível efetuar entregas seguras	Falha de informação aquando da elaboração de contratos	Incapacidade de efetuar entrega segura
Eficácia e Eficiência - Falha Humana	Erro na leitura dos códigos de barras das paletes de caixas de certificados de inspeção	Sequenciação inadequada das caixas e etiquetas de código de barras mal formatadas	Maior tempo de processamento das encomendas
Eficácia e Eficiência - Falha Humana	Erro no suprimento de material à produção	Erro de operação	Devolução de material Novo fornecimento
Reputação e Imagem - Incumprimento de Procedimentos Internos	Venda indevida de equipamento produtivo	Procedimento de venda não considerar requisitos de segurança	Utilização abusiva de equipamentos de produção
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Acesso indevido a máquinas produtivas *legacy*	Máquinas sem controlo de acessos ou sem possibilidade de alterar *password*	Dano nos produtos de segurança e/ou nas máquinas produtivas

PROCESSO E2E – DO PLANEAMENTO À ENTREGA

Categoria do Risco	Evento	Causa	Consequência
Segurança da Informação - Operação Não Autorizada	Utilização indevida de materiais de segurança, por pessoas não autorizadas	Chapas deixadas no interior da máquina, quando não estão em utilização	Produção indevida por pessoas não autorizadas
Segurança da Informação - Perda de Informação de Segurança	Perda (temporária ou permanente) de fase de fabrico ao longo do processo produtivo	Transporte e movimentações desnecessárias	Atraso no prazo de entrega do produto final
Cadeia de Fornecimento - Indisponibilidade de Informação	Guias de remessa com informação errada ou incompleta	Falta de dados por parte do fornecedor	Material em espera
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Indisponibilidade de alimentação elétrica	Danos ou corte de cabos elétricos	Indisponibilidade ou limitação de serviços

PROCESSO E2E – DO RECRUTAMENTO À SAÍDA/REFORMA

Categoria do Risco	Evento	Causa	Consequência
Limite de Autoridade - Indução em Erro	Colaborador a termo integrado nos quadros indevidamente	Desconhecimento do fim de prazo de contrato a termo	Aumento de custos com pessoal
Limite de Autoridade - Abuso de Direitos	Favorecimento de candidato em processo de recrutamento	Divulgação de informação confidencial a candidato sobre avaliação do candidato	Corrupção e Infrações Conexas. Colaborador sobrevalorizado
Segurança da Informação - Divulgação de Informação Confidencial	Divulgação de dados pessoais de colaboradores	Acesso não autorizado a informação em papel ou digital	Confidencialidade da informação comprometida
Limite de Autoridade - Abuso de Direitos	Manipulação de informação ou utilização em fraude de serviços sociais	Ação deliberada para proveito próprio	Corrupção e Infrações conexas
Segurança da Informação - Divulgação de Informação Confidencial	Divulgação de dados pessoais de colaboradores	Ação deliberada para proveito próprio	Confidencialidade da informação comprometida
Eficácia e Eficiência - Falha Humana	Informação salarial incorreta	Implementação de regras salariais feitas manualmente	Pagamento indevido (em falta ou excesso)

PROCESSO E2E – DO RECRUTAMENTO À SAÍDA/REFORMA

Limite de Autoridade - Abuso de Direitos	Manipulação da informação salarial	Corrupção e Infrações conexas	Perda irrecuperável de informação (relativa a entidades externas e internas)
Limite de Autoridade - Abuso de Direitos	Discriminação no desenvolvimento de carreira e condições de trabalho	Comportamento baseado em fator de discriminação	Violação do princípio da igualdade/assédio

PROCESSOS E2E – GESTÃO DE RECURSOS

Categoria do Risco	Evento	Causa	Consequência
Segurança da Informação - Divulgação de Informação Confidencial	Divulgação de informação confidencial do Arquivo Intermédio	Acesso não autorizado ao Arquivo Intermédio	Informação confidencial comprometida
Segurança da Informação - Perda de Informação de Segurança	Extravio de informação do Arquivo Intermédio	Ação deliberada para proveito próprio	Informação confidencial comprometida
Eficácia e Eficiência - Falha Humana	Acumulação de resíduos perigosos nas zonas de acesso a áreas de segurança	Dificuldade e morosidade na transposição de áreas de segurança para colocação dos resíduos em contentor	Libertação de odores Dificuldade de circulação em áreas de acesso Rotura de sacos de resíduos com o consequente espalhar do conteúdo no chão

PROCESSO E2E – GESTÃO DE SISTEMAS DE INFORMAÇÃO

Categoria do Risco	Evento	Causa	Consequência
Segurança da Informação - Perda de Informação de Segurança	Sistemas não monitorizados pelo novo SIEM	O levantamento de ativos para associar o agente do sistema SIEM poderá não estar completo	Existirem ativos não monitorizados, pelo que não é possível recolher eventos sobre os mesmos
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Quebra da estrutura de vidro na sala do servidor	Ato voluntário	Danos na infraestrutura Acesso indevido a zona restrita
Tecnologia da Informação - Falha Humana	Passagem a produção de código defeituoso	Engano do colaborador	Existência de algum erro no código que pode levar a uma paragem na produção

PROCESSO E2E – GESTÃO DE SISTEMAS DE INFORMAÇÃO

Categoria do Risco	Evento	Causa	Consequência
Segurança da Informação - Perda de Informação de Segurança	Degradação do *DataCenter*	Falha ou degradação de equipamento de climatização	Perda de informação

PROCESSO E2E – GESTÃO DE SISTEMAS DE INFORMAÇÃO

Categoria do Risco	Evento	Causa	Consequência
Eficácia e Eficiência - Falha Humana	Atraso na entrada de projetos em produção	Falta de tempo, engano no código que leva a uma maior perda de tempo	Atraso na produção Má reputação
Segurança da Informação - Operação Não Autorizada	Instalação de programas não autorizados pela equipa SC	Incumprimentos das regras internas estabelecidas	Segurança lógica comprometida
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Equipa de SC utilizar privilégios e aplicações de administração para acessos não autorizados	Acesso não autorizado	Acesso indevido a informação confidencial Acesso indevido a equipamentos
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Equipa de SC aceder fisicamente a equipamentos com informação confidencial	Comportamento doloso premeditado	Acesso indevido a informação confidencial Acesso indevido a equipamentos
Segurança da Informação - Operação Não Autorizada	Pedido de *password* por colaborador não autorizado	Ação deliberada para proveito próprio	Acesso não autorizado a posto de trabalho
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Extravio de portáteis fora da organização	Portáteis autorizados a sair da organização	Confidencialidade e disponibilidade da informação comprometida

PROCESSO E2E – SEGURANÇA

Categoria do Risco	Evento	Causa	Consequência
Segurança da Informação - Divulgação de Informação Confidencial	Incorreta personalização de documento reclamados	Ação deliberada ou erro humano Possibilidade de reimpressão sem controlos de autorização ou registo por forma a dar resposta a reclamações de produtos não conformes ou não entregues	Quebras de confidencialidade e integridade dos produtos Incorreto planeamento do produto e consequentemente incorreta gestão de *stocks* de matéria-prima e refugo
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Destruição de imagens do sistema interno de CCTV	Acesso não autorizado a sistemas de CCTV ou a base de dados das gravações de imagens	Segurança comprometida
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Acesso indevido ao *DataCenter*	Acesso ao *DataCenter* sem autorização prévia	Acesso indevido a informação confidencial Acesso indevido a equipamentos
Segurança da Informação - Acesso Não Autorizado a Ativos de Segurança	Acesso não autorizado a ativos de segurança por pessoal externo ao serviço	Necessidade de acesso a zonas de segurança para intervenções nos espaços (exemplo: execução de obras ou outras intervenções na infraestrutura)	Divulgação de informação confidencial Desvio de produto, materiais ou imagens

ANEXO III
AVALIAÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

PROCESSOS E2E – DA AQUISIÇÃO AO ABATE

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Beneficiar uns clientes em relação a outros	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Aquisição de bens/serviços não decorrente de necessidades reais	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Divulgação externa de informação confidencial	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Manipulação de ensaios laboratoriais para seleção de fornecedor	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Perda e extravio das amostras	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Faturação indevida de manutenção e obras	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Inexistência, ou existência deficiente, de estimativas de custo para a realização das obras/ manutenção	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Informação errónea/insuficiente	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar
Indisponibilidade da informação para recuperação de avaria	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Alteração indevida dos parâmetros das máquinas produtivas	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Resultados incorretos	1 - Muito Baixa	2 - Pequeno	1 - **Muito Baixo**	Aceitar
Amostras danificadas	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Ineficiência de processo de gestão de cablagem elétrica (Ausência de placas sinaléticas nos quadros elétricos)	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar
Ineficiência de processo de gestão de cablagem elétrica (Ausência de etiquetagem da cablagem elétrica)	4 - Alta	3 - Moderado	3 - **Moderado**	Mitigar

PROCESSO E2E - DA ENCOMENDA À FATURAÇÃO

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Extravio de produtos/valores	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar

PROCESSO E2E - DA OPORTUNIDADE AO NEGÓCIO

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Violação ou destruição de dados via ficheiros informáticos	1 - Muito Baixa	4 - Significativo	2 - Baixo	Mitigar
Divulgação de informação confidencial de dados comerciais	1 - Muito Baixa	4 - Significativo	2 - Baixo	Aceitar
Produção de espécimes sem o conhecimento e autorização prévia do cliente	3 - Moderada	3 - Moderado	3 - Moderado	Mitigar
Fornecimento de produtos a cliente não autorizado	2 - Baixa	4 - Significativo	3 - Moderado	Mitigar
Pedido de documentos para postos não autorizados (aplicável a situações com tabelas de recebedor e emissor codificados associadas a produto)	1 - Muito Baixa	4 - Significativo	2 - Baixo	Aceitar
Fornecimento de produtos a cliente não autorizado	1 - Muito Baixa	4 - Significativo	2 - Baixo	Aceitar
Fuga de informação confidencial por fornecedores ou empresas subcontratadas	1 - Muito Baixa	5 - Severo	3 - Moderado	Mitigar
Atraso na produção de peças para cunhagem	2 - Baixa	4 - Significativo	3 - Moderado	Mitigar

PROCESSO E2E - DA PROCURA AO PAGAMENTO

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Processo de aquisição com informação incompleta (escolha de fornecedor, solicitação de cotação, análise de propostas, etc.)	1 - Muito Baixa	4 - Significativo	2 - Baixo	Aceitar
Formalização do processo de compra após aquisição	1 - Muito Baixa	3 - Moderado	1 - Muito Baixo	Aceitar
Pagamento de bens/serviços indevida	1 - Muito Baixa	5 - Severo	3 - Moderado	Mitigar
Seleção de fornecedor não tendo como critério as melhores condições	1 - Muito Baixa	4 - Significativo	2 - Baixo	Aceitar
Insatisfação das áreas requisitantes	2 - Baixa	3 - Moderado	2 - Baixo	Aceitar

PROCESSO E2E - DO PLANEAMENTO À ENTREGA

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Acesso indevido a redes externas	5 - Muito Alta	1 - Mínimo	2 - **Baixo**	Mitigar
Produção ou testes realizados na produção sem evidências da devida aprovação por alguém mandatado para tal	3 - Moderada	4 - Significativo	3 - **Moderado**	Mitigar
Peças não conforme com as especificações do cliente	3 - Moderada	4 - Significativo	3 - **Moderado**	Mitigar
Moedas (correntes e de acabamento especial) produzidas com defeito	1 - Muito Baixa	5 - Severo	3 - **Moderado**	Mitigar
Falta de especificações técnicas de produtos	1 - Muito Baixa	5 - Severo	3 - **Moderado**	Mitigar
Extravio de unidades de produto acabado na expedição	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Divulgação externa e abusiva de informação do *Mint Directors Working Group*	2 - Baixa	5 - Severo	3 - **Moderado**	Mitigar
Erros na conferência de material rececionado	3 - Moderada	1 - Mínimo	1 - **Muito Baixo**	Aceitar
Roubo ou extravio de peças depositadas na UCF	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Validade do certificado criptográfico do passaporte inválida	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Acesso não autorizado a quadros elétricos	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar
Atribuição de licença indevida	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar
Produção involuntária de erros nos atos	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Publicação com erro de edição	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar
Atrasos (< 24 h) na publicação de atos relevantes	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Desaparecimento de inventários	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Defeitos não detetados ao longo do processo produtivo	3 - Moderada	4 - Significativo	3 - **Moderado**	Mitigar
Falta de ordens de produção	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Erro na definição de especificações de produtos	1 - Muito Baixa	5 - Severo	3 - **Moderado**	Mitigar

PROCESSO E2E - DO PLANEAMENTO À ENTREGA

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Falha no processo de destruição e de destino de tintas de segurança a inutilizar (ex. restos de tinta ou tintas obsoletas)	2 - Baixa	2 - Pequeno	1 - **Muito Baixo**	Aceitar
Juntar, soldar e furar incorretamente as várias camadas constituintes do cartão	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Seleção de *chip* (*contact*) incorreto para aplicar em cartão	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Iniciar a preparação e afinação da máquina sem ter em conta as especificações da ordem de produção	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Gravação incorreta da matriz de impressão (chapa ou película), detetada nas etapas a jusante	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Requisitar internamente e liberar pedido de compra de matéria-prima com caraterísticas erradas	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Divulgação de elementos confidenciais de marcas	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Extravio de peças preciosas	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Orçamentar produto com erro de quantidade de materiais ou fora das especificações do cliente	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Peças danificadas	3 - Moderada	4 - Significativo	3 - **Moderado**	Mitigar
Recuperação de ferros de punção arrasados	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Extravio de punção	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Roubo de punção em serviço de marcação ao domicílio	2 - Baixa	4 - Significativo	3 - **Moderado**	Evitar
Utilização de chaves criptográficas incorretas	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Passaportes furados que impedem leitura na máquina de destruição de PEP's e CC's	3 - Moderada	2 - Pequeno	2 - **Baixo**	Aceitar
Envio de produtos para locais onde não é possível efetuar entregas seguras	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Erro na leitura dos códigos de barras das paletes de caixas de certificados de inspeção	2 - Baixa	2 - Pequeno	1 - **Muito Baixo**	Aceitar

PROCESSO E2E - DO PLANEAMENTO À ENTREGA

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Utilização de certificados expirados	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Erro no suprimento de material à produção	3 - Moderada	2 - Pequeno	2 - **Baixo**	Aceitar
Venda indevida de equipamento produtivo	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Acesso indevido a máquinas produtivas *legacy*	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Utilização indevida de materiais de segurança, por pessoas não autorizadas	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Roubo ou extravio do produto acabado durante o transporte nacional	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Dificuldade na rastreabilidade das chapas produzidas/utilizadas/ destruídas	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar
Perda (temporária ou permanente) de fase de fabrico ao longo do processo produtivo	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Guias de remessa com informação errada ou incompleta	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar
Indisponibilidade de alimentação elétrica	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar

PROCESSO E2E - DO RECRUTAMENTO À SAÍDA/REFORMA

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Colaborador a termo integrado nos quadros indevidamente	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Favorecimento de candidato em processo de recrutamento	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Divulgação de dados pessoais de colaboradores	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Manipulação de informação ou utilização em fraude de serviços sociais	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Divulgação de dados pessoais de colaboradores	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Informação salarial incorreta	2 - Baixa	3 - Moderado	2 - **Baixo**	Mitigar

PROCESSO E2E - DO RECRUTAMENTO À SAÍDA/REFORMA

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Manipulação da informação salarial	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Discriminação no desenvolvimento de carreira e condições de trabalho	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar

PROCESSO E2E – GESTÃO DE RECURSOS

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Divulgação de informação confidencial do Arquivo Intermédio	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Extravio de informação do Arquivo Intermédio	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Acumulação de resíduos perigosos nas zonas de acesso a áreas de segurança	3 - Moderada	2 - Pequeno	2 - **Baixo**	Aceitar

PROCESSO E2E – GESTÃO DE SISTEMAS DE INFORMAÇÃO

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Sistemas não monitorizados pelo novo SIEM	1 - Muito Baixa	2 - Pequeno	1 - **Muito Baixo**	Aceitar
Ataque informático a sistema com sucesso	1 - Muito Baixa	5 - Severo	3 - **Moderado**	Mitigar
Quebra da estrutura de vidro na sala do servidor	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Passagem a produção de código defeituoso	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Degradação do *DataCenter*	1 - Muito Baixa	5 - Severo	3 - **Moderado**	Mitigar
Atraso na entrada de projetos em produção	3 - Moderada	3 - Moderado	3 - **Moderado**	Mitigar
Instalação de programas não autorizados pela equipa SC	3 - Moderada	3 - Moderado	3 - **Moderado**	Transferir
Equipa de SC utilizar privilégios e aplicações de administração para acessos não autorizados	3 - Moderada	4 - Significativo	3 - **Moderado**	Mitigar
Equipa de SC aceder fisicamente a equipamentos com informação confidencial	3 - Moderada	4 - Significativo	3 - **Moderado**	Mitigar

PROCESSO E2E – GESTÃO DE SISTEMAS DE INFORMAÇÃO

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Pedido de *password* por colaborador não autorizado	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Mitigar
Extravio de portáteis fora da organização	2 - Baixa	3 - Moderado	2 - **Baixo**	Aceitar

PROCESSOS E2E - SEGURANÇA

Evento	Probabilidade da Perda Derivada	Nível de Impacto	Nível de Risco	Estratégia de Tratamento
Indisponibilidade de equipamentos nas instalações de suporte ao controlo de segurança física	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Incorreta personalização de documento reclamados	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar
Ataque informático	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Mitigar
Indisponibilidade do SADI — Sistema de Deteção Automática de Incêndios ou SEAI — Sistema de Extinção Automática de Incêndios	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Ataque terrorista	1 - Muito Baixa	5 - Severo	3 - **Moderado**	Mitigar
Destruição de imagens do sistema interno de CCTV	1 - Muito Baixa	3 - Moderado	1 - **Muito Baixo**	Aceitar
Acesso indevido ao *DataCenter*	1 - Muito Baixa	5 - Severo	3 - **Moderado**	Mitigar
Dificuldade na identificação de pessoal autorizado	3 - Moderada	3 - Moderado	3 - **Moderado**	Mitigar
Acesso não autorizado a ativos de segurança por pessoal externo ao serviço	1 - Muito Baixa	4 - Significativo	2 - **Baixo**	Aceitar
Incapacidade de manutenção do sistema de CCTV	2 - Baixa	4 - Significativo	3 - **Moderado**	Mitigar