U.PORTO

FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

MESTRADO EM CIÊNCIA DA INFORMAÇÃO

CONCEÇÃO DE UM SERVIÇO INTEGRADO DE AVALIAÇÃO DA GESTÃO E PROTEÇÃO DE DADOS

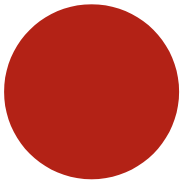
José António Casanova Monteiro

M

2020

UNIDADES ORGÂNICAS ENVOLVIDAS

FACULDADE DE ENGENHARIA
FACULDADE DE LETRAS



José António Casanova Monteiro

CONCEÇÃO DE UM SERVIÇO INTEGRADO DE AVALIAÇÃO DA GESTÃO E PROTEÇÃO DE DADOS

Dissertação realizada no âmbito do Mestrado em Ciência da Informação, orientada pelo Professor Doutor Gabriel David

Faculdade de Engenharia e Faculdade de Letras

Universidade do Porto

Setembro de 2020

CONCEÇÃO DE UM SERVIÇO INTEGRADO DE AVALIAÇÃO DA GESTÃO E PROTEÇÃO DE DADOS

José António Casanova Monteiro

Dissertação realizada no âmbito do Mestrado em Ciência da Informação, orientada pelo Professor Doutor Gabriel David

Membros do Júri

Presidente: Professora Doutora Carla Teixeira Lopes

Faculdade de Engenharia - Universidade do Porto

Arguente: Professor Doutor Filipe Sá Soares

Escola de Engenharia - Universidade do Minho

Orientador: Professor Doutor Gabriel David

Faculdade de Engenharia - Universidade do Porto

“Uma hipótese nunca é verdadeira ou falsa, mas sim,
mais ou menos útil” – Mara Selvini

Agradecimentos

Na elaboração deste trabalho foram vários os que contribuíram para que fosse possível atingir o fim desta dissertação.

Agradeço ao meu orientador, Professor Gabriel David por todo o suporte, orientação e conhecimento.

À minha família, mãe, irmã e sobrinho, por todo o apoio e pela compreensão de tantos momentos ausente.

À minha Angelinha, pela força sem a qual seria impossível.

Aos meus amigos, pelos momentos de descontração tão importantes para voltar ao foco necessário.

A todos os meus colegas sem os quais muito conhecimento seria perdido.

A todos, um muito obrigado do fundo do coração.

Resumo

O Regulamento Geral de Proteção de Dados (RGPD) recentemente publicado, lançou novos desafios aos sistemas de informação e às empresas produtoras e utilizadoras desses mesmos sistemas de informação. A proteção dos titulares de dados é um direito fundamental das pessoas singulares e agora com um regime jurídico a nível europeu devidamente ajustado.

A presente dissertação estuda os desafios que o RGPD veio colocar aos sistemas de informação de gestão comuns nas organizações e propõe algumas respostas. O método é análise do caso do sistema Sistrade® MIS | ERP nos diversos módulos que o constituem: Administrativa & Financeira, Gestão Comercial & Orçamentação, Gestão da Produção, Gestão de Stocks & Compras, e Soluções de Gestão WEB. Inicialmente o estudo é realizado através da identificação de processos em cada um dos módulos e do mapeamento dos tratamentos de dados efetuados. Analisa-se em seguida o risco de cada um desses tratamentos para a proteção de dados pessoais, obtendo-se uma avaliação do impacto global dos diversos módulos do sistema.

Posteriormente, e partindo das fragilidades identificadas no sistema, são efetuadas algumas sugestões por forma a mitigar os riscos de violação de dados. É ainda especificado um processo de auditoria onde se levantam algumas questões em relação aos tratamentos efetuados, sendo ainda sugeridos alguns modelos de relatórios que poderão ajudar à conformidade das implementações do próprio sistema.

Em síntese, esta dissertação permitiu uma análise da proteção de dados ao Sistrade® MIS | ERP, efetuando algumas indicações para o cumprimento das novas exigências do RGPD.

Palavras-chave: Regulamento Geral da Proteção de Dados, ERP, Segurança da Informação

Abstract

The recently published General Data Protection Regulation (GDPR) launched new challenges for information systems, for either software houses and users companies using those same information systems. The protection of data owners is a fundamental right of individuals and now with a legal frame at European level duly adjusted.

This dissertation studies the challenges that the GDPR raised on the management information systems commonly operating in the organizations and proposes some answers. The method is the case analysis of the Sistrade® MIS | ERP in its various modules: Administrative & Financial, Commercial & Budget Management, Production Management, Stock & Purchasing Management, and WEB Management Solutions. Initially, the assessment is carried out by identifying processes in each of the modules and mapping the data processings performed. Follows an assessment of the risk each of those data processings poses to the protection of personal data, conducing to a global impact assessment of the several modules in the system.

Subsequently, and working from the weaknesses identified in the system, some suggestions are made in order to mitigate the risks of data breaches. An audit process is also specified in which some questions are raised in relation to the data processings carried out, and some report models are suggested that may help to the compliance of the system's own implementations.

In summary, this dissertation allowed an analysis of data protection in Sistrade® MIS | ERP, and giving some hints for the fulfillment of the new requirements of the GDPR.

Keywords: General Data Protection Regulation (GDPR), ERP, information security

Sumário

Lista de figuras

Lista de tabelas

Lista de abreviaturas e siglas

CRM	*Customer Relationship Management*
ERP	*Enterprise Resource Planning*
GDPR	*General Data Protection Regulation*
KPI	*Key Performance Indicator*
MIS	*Management Information System*
MRP	*Material Requirement Planning*
OEE	*Overall Equipment Effectiveness*
PLM	*Product Lifecycle Management*
RGPD	Regulamento Geral de Proteção de Dados
SCADA	*Supervisory Control and Data Acquisition*

1. Introdução

1.1. Contextualização

A entrada em vigor do Regulamento Geral de Proteção de Dados, em Maio de 2018, coloca desafios importantes às empresas e aos seus sistemas de informação. Diversos serviços e aplicações utilizados no mundo empresarial interagem de forma intensiva com dados pessoais. A crescente digitalização e integração dos fluxos de dados pessoais nas cadeias de valor industrial colocam também importantes desafios às organizações. Operando em áreas industriais e comerciais com fluxos de dados crescentes e mais complexos, as organizações têm que cumprir o referido regulamento.

A identificação, mapeamento e análise destes fluxos de dados e a conceção de soluções que possam torná-los conformes com o RGPD são tarefas que muitas vezes requerem competências que as empresas não dispõem internamente e, no entanto, serão obrigadas a realizar por forma a evitar avultadas coimas.

Torna-se assim pertinente a conceção de um serviço integrado de avaliação da gestão e proteção de dados pessoais no âmbito empresarial que possa ser implementado nas organizações, permitindo assim aferir a sua conformidade com o respetivo regulamento (*GDPR Compliance*).

1.2. Instituição de acolhimento

A SISTRADE - Software Consulting, S.A. é uma empresa portuguesa especializada no desenvolvimento de software e na prestação de serviços de consultoria para diferentes sectores de atividade, nomeadamente para a indústria e para os serviços, encontrando-se presente em 26 mercados internacionais. Esta atividade tem por objetivo fornecer soluções informáticas às organizações, com base nas mais recentes tecnologias, para que estas possam tirar partido de soluções de gestão inovadoras, permitindo-lhes não só uma boa gestão interna, mas também uma cada vez maior ligação a parceiros através do comércio eletrónico e de ferramentas de colaboração *online*.

Sistrade® MIS | ERP

A SISTRADE desenvolveu uma solução empresarial orientada para a gestão de processos denominada Sistrade® MIS (*Management Information System*) | ERP (*Enterprise Resource Planning*). Esta solução tecnológica oferece às empresas de média e grande dimensão diversas funcionalidades, tais como: CRM (*Customer Relationship Management*), gestão

comercial, orçamentação, gestão de encomendas, compras, stocks, gestão da produção, contabilidade, entre outras.

No módulo CRM *Customer Care Relationship Management* permite registar informações sobre os contactos dos clientes, desde informação financeira, interlocutores, ou projetos e encomendas em curso. Este módulo influencia o desempenho da área comercial e tem impacto nas restantes funções da empresa.

Por sua vez, o módulo de Gestão Comercial permite, apoiado num sistema de *workflow* de processos, efetuar orçamentos, registar encomendas e faturas, gerir expedição e analisar as diferentes entidades.

A Gestão Financeira permite ações e procedimentos administrativos, abrangendo planeamento, análise e controlo das atividades financeiras, com o objetivo de maximizar o resultado da área operacional. O módulo de Contabilidade integra com os restantes módulos automatizando o registo da maior parte das operações. O módulo de Gestão de Recursos Humanos permite gerir facilmente todas as pessoas da organização. O módulo Imobilizado controla o ciclo de vida dos bens da empresa.

O iProcurement agiliza a compra e aproxima os fornecedores à cadeia de valor da empresa, sendo possível gerir preços de diversos fornecedores, lançar ordens de compra, gerir stocks, verificar conta corrente de artigos, etc.

A vertente de Gestão de Produção e Controlo Industrial visa simplificar e tornar mais eficiente o processo de produção. Permite modelar, automatizar e otimizar as áreas de planeamento da produção, gestão de ordens de fabrico, custeio e recolha de dados industriais.

Graças à mobilidade da tecnologia Sistrade® MIS | ERP todas estas informações estão disponíveis em qualquer parte do mundo com ligação à internet, permitindo resposta aos clientes em tempo útil e assim conseguir a fidelização dos mesmos.

1.3. Objetivos e resultados esperados

O objetivo desta dissertação é conceber um serviço que auxilie as entidades utilizadoras do Sistrade® MIS | ERP a avaliar a sua gestão e proteção de dados, ajudando a garantir o cumprimento do Regulamento Geral de Proteção de Dados.

Por forma a garantir tal objetivo, será necessário efetuar uma avaliação do sistema Sistrade® MIS | ERP no que diz respeito à proteção de dados e à utilização de dados pessoais. Inicialmente será necessário identificar os processos decorrentes das atividades de produção e de suporte à própria atividade.

Após identificados esses processos, os mesmos serão mapeados e classificados em relação ao tratamento de dados pessoais efetuado. Nas atividades com tratamento de dados pessoais deverá ser assegurada uma avaliação da utilização desses dados pessoais, bem como do impacto sobre a proteção de dados.

Identificado o estado atual do sistema Sistrade® MIS | ERP, serão especificados os requisitos da plataforma informática de suporte ao serviço integrado de avaliação da gestão e proteção de dados. A especificação dos requisitos será efetuada de forma faseada iniciando por algumas medidas de correção do sistema atual para mitigação dos riscos de violação promovendo a privacidade *by design*. De seguida, serão especificados os requisitos para o processo de auditoria a disponibilizar na plataforma. Por final, serão gerados modelos dos relatórios a apresentar como resultado da auditoria.

Estes objetivos devem materializar-se na conceção de um serviço integrado de avaliação da gestão e proteção de dados, incluindo a respectiva documentação e especificação da plataforma informática de suporte. Os objetivos podem ser revistos da seguinte árvore de objetivos:

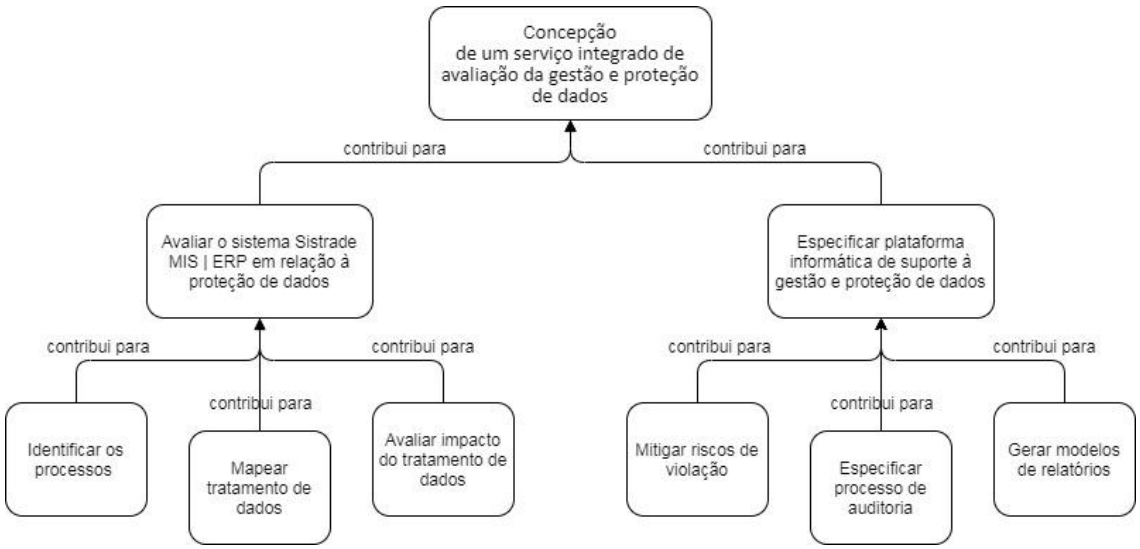


Figura 1 – Árvore de objetivos

1.4. Estrutura da dissertação

A presente dissertação está dividida em seis capítulos, acrescendo no término do documento as respetivas referências bibliográficas e anexos relevantes para todo o trabalho realizado, incluindo imagens que ilustram a realidade atual, o que se pretende alcançar na plataforma, bem como a apresentação de um inquérito efetuado a alguns clientes desta solução.

O primeiro capítulo destina-se à introdução, onde são apresentados os fundamentos e a

motivação para esta dissertação, procurando-se expor de forma argumentativa a problemática existente. Neste capítulo é também apresentada a instituição de acolhimento, bem como a plataforma e os módulos integrantes. Por final, os objetivos e os resultados esperados desta abordagem, bem como a estrutura da própria dissertação.

No segundo capítulo encontramos a fundamentação teórica para a problemática da proteção de dados. Este capítulo está dividido em dez partes. A primeira parte pretende demonstrar a importância e o crescimento dos dados na sociedade da informação. A segunda e terceira partes visam explicar alguns conceitos decorrentes da proteção de dados, nomeadamente dados pessoais e tratamento de dados. A quarta parte propõe-se a distinguir proteção de dados e privacidade, conceitos que muitas vezes se cruzam e são confundidos, nomeadamente em ambientes *cloud*. A quinta parte aborda o Regulamento Geral de Proteção de Dados decretado pela União Europeia, e onde se definem os princípios do tratamento de dados pessoais e algumas obrigações que as empresas deverão cumprir. A sexta parte mostra como o Regulamento Geral de Proteção de Dados está a ser visto pelas empresas, dando continuidade na sétima parte com algumas normas de ajuda ao cumprimento do referido regulamento. A oitava parte define o risco e como deve ser efetuada a gestão do mesmo, sendo abordada na nona parte a avaliação dos riscos relacionados com o tratamento de dados pessoais. Por final, na décima e última parte são revistas algumas estatísticas em segurança da informação.

No terceiro capítulo pode ser encontrada a abordagem metodológica que foi aplicada na presente dissertação, especificando-se os métodos que foram utilizados no processo de investigação e que permitiram recolher os dados que tornaram possível o desenvolvimento de um trabalho rigoroso e preciso.

No quarto capítulo é efetuada uma análise do sistema Sistrade® MIS | ERP com o objetivo de mapear as atividades onde são utilizados os dados pessoais, identificar o fluxo informacional e a forma como são utilizados, verificando a existência de risco de violações do Regulamento Geral de Proteção de Dados.

No quinto capítulo, e mediante a análise efetuada no capítulo anterior, foi efetuada a confrontação com o Regulamento Geral de Proteção de Dados verificando o seu cumprimento e eventuais violações do mesmo, acrescendo algumas sugestões de melhoria por forma a mitigar riscos de violação. É também especificado um processo de auditoria que irá ajudar as organizações a cumprir com o regulamento, gerando modelos de relatórios atestando o cumprimento do mesmo.

O sexto capítulo destina-se a expor as conclusões retiradas após todo o percurso que levou

aos resultados obtidos. Pretende-se, neste capítulo, apresentar as aprendizagens alcançadas durante toda a jornada que esta dissertação permitiu realizar junto de uma equipa multidisciplinar, incluindo o valor da integração neste projeto.

Na última parte da dissertação encontram-se as referências bibliográficas que suportam todo o trabalho realizado, bem como os anexos, onde se poderão consultar documentos considerados fundamentais para o desenvolvimento de toda a dissertação. Assim, aqui poderão ser encontrados o mapeamento do tratamento de dados, o inquérito efetuado, os resultados desse mesmo inquérito e alguns modelos de documentos que são sugeridos para o cumprimento do RGPD.

Neste contexto coloca-se a questão se o Sistrade® MIS | ERP cumpre o RGPD, e se as organizações que o utilizam estão salvaguardadas em relação à proteção dos dados pessoais que utilizam.

2. Revisão de literatura

2.1. Sociedade da informação

A nossa sociedade é verdadeiramente uma sociedade da informação, a nossa era uma era da informação (Mason, 1986).

O conceito de sociedade da informação é no entanto altamente abstrato (Karvalics, 2007), tendo sido identificadas algumas definições diferentes:

- Uma sociedade que se organiza em torno do conhecimento no interesse do controlo social e da gestão da inovação e mudança…(Bell, 1980);
- Um novo tipo de sociedade, onde a posse de informação (e não a riqueza material) é a força motriz por trás da sua transformação e desenvolvimento […] (e onde) a criatividade intelectual humana floresce (Masuda, 1980);
- A sociedade da informação é uma realidade económica e não simplesmente uma abstração mental… A lenta propagação/disseminação de informação termina […] novas atividades, operações e produtos gradualmente surgem (Naisbitt, 1985);
- Uma sociedade em que […] a informação é usada como um recurso económico, a comunidade aproveita/explora e, por trás de tudo, se desenvolve uma indústria que produz a informação necessária… (Moore, 1998);
- Uma estrutura social baseada na criação, distribuição, acesso e uso gratuitos de informação e conhecimento […] a globalização de vários campos da vida. ((Hungarian) National Strategy of Informatics, 1995);
- Um novo tipo de sociedade em que a humanidade tem a oportunidade de liderar um novo modo de vida, ter um padrão de vida mais alto, realizar um trabalho melhor e desempenhar um papel melhor na sociedade, graças ao uso global das tecnologias da informação e das telecomunicações. (Murányi).

A sociedade da informação é sustentada em dados e impulsionada pela crescente utilização de tecnologias da informação e comunicação.

Esse crescimento foi e continuará a ser acelerado, e segundo estimativas irá haver um crescimento de 33 ZB de 2018 para 175 ZB em 2025 (Reinsel, Gantz, & Rydning, 2018).

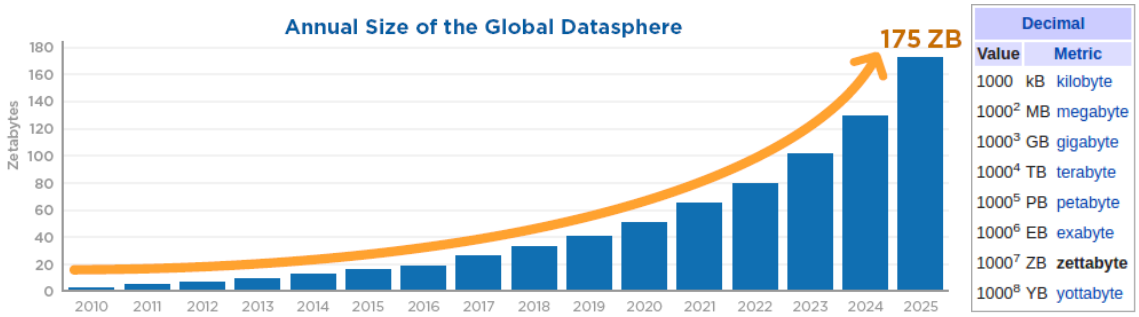


Figura 2 – Perspectiva de crescimento da esfera global de dados

Fonte: Reinsel, Gantz, & Rydning, 2018

A maior parte desses dados será armazenada em servidores externos, à medida que soluções *cloud* ganham dimensão.

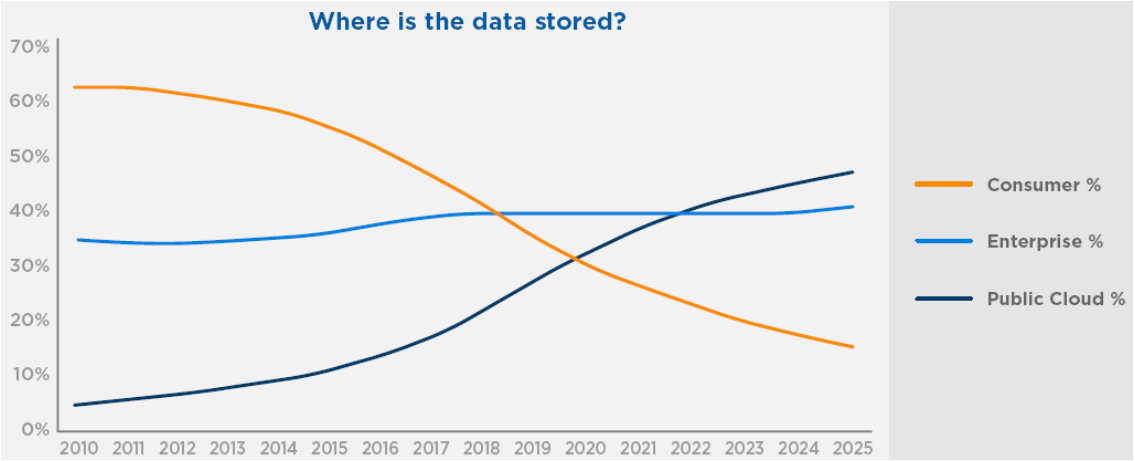


Figura 3 – Perspectiva do local de armazenamento dos dados

Fonte: Reinsel, Gantz, & Rydning, 2018

Segundo o mesmo estudo, os dados ajudam a alcançar novos mercados, servir melhor os clientes existentes, otimizar operações e a criar valor através de dados brutos e analisados.

O tratamento desses dados ameaça a dignidade humana (Mason, 1986), pois cada vez somos mais expostos a que os dados pessoais sejam apresentados de uma forma pública, mesmo contra a vontade dos titulares dos dados, constituindo assim uma ameaça ao direito à privacidade.

2.2. Dados pessoais

O Regulamento Geral de Proteção de Dados definiu dados pessoais como "*informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome,*

um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (Parlamento Europeu, 2016).

Conforme esta definição tanto informação direta como indireta são consideradas dados pessoais, devendo ter o mesmo nível de proteção.

Alguns exemplos de identificadores são:

- Nome;
- Apelido;
- Nº identificação fiscal;
- Foto;
- Endereço de residência;
- Endereço pessoal de correio eletrónico;
- Nº de cartão de identificação;
- Número de telefone;
- Dados de localização;
- Endereço IP;
- Dados genéticos do hospital ou médico.

Para além destes, podem ser considerados identificadores indiretos dados que, cruzados com outros, permitam identificar pessoas. Por exemplo, os dados de localização de um telemóvel, conjugados com o conhecimento do utilizador do telemóvel transformam os dados de localização em identificador pessoal indireto. O mesmo se diga de outros atributos de perfis financeiros, culturais ou sociais distintivos.

Os dados pessoais são todos os dados que sejam associáveis através de identificadores diretos ou indiretos a uma pessoa singular. Isto inclui dados sócio-económicos, de saúde, de perfil cultural ou social, entre outros.

Exemplos de dados não considerados pessoais:

- Número de registo de empresa;
- Endereço de correio eletrónico empresarial;
- Dados anonimizados ou pseudonimizados, isto é, completamente desligados das pessoas ou ainda ligados, mas através de um pseudónimo devidamente protegido.

Os dados pessoais podem assumir várias categorias (Nascimento, 2019):

- Internas:
    - Conhecimento e Crenças: dados sobre as crenças religiosas, filosóficas e

pensamentos;

  - Autenticação: dados sobre forma de autenticar, seja através de senha de acesso, PIN e impressão digital;
  - Preferência: interesses pessoais relacionados com cores, música e gostos;

- Externas:
  - Identificação: informação que identifica uma pessoa singular, nomeadamente nome, foto, dados biométricos ou identificador único;
  - Etnia: descrição da raça, origem e idiomas falados;
  - Sexual: preferências pessoais e sexuais;
  - Comportamento: descrição de atividades relativas a uma pessoa;
  - Demografia: informação sobre escalões de rendimento, faixas etárias e traços físicos;
  - Médica e Saúde: historial clínico, nomeadamente tipo de sangue, DNA, resultados de testes, deficiências e prescrições;
  - Características Físicas: aparência tal como altura, peso, idade, cor do cabelo, pele, tatuagens e género.
- Históricas:
  - História de vida: historial da pessoa que pode ter influenciado a vida da mesma.
- Financeiras:
  - Conta: dados de contas financeiras, por exemplo, número de cartão de crédito e número de conta bancária;
  - Propriedade: coisas que a pessoa possui;
  - Transações: compras ou despesas relacionadas com vendas, créditos, receitas, empréstimos, transações, impostos e hábitos de compras;
  - Crédito: informação sobre dinheiro para credibilidade, capacidade e posição de crédito.
- Sociais:
  - Profissional: carreira académica ou profissional nomeadamente salário,

avaliações, entrevistas e historial de trabalho;

- Criminal: condenações e acusações criminais;
- Vida Pública: reputação, religião, filiações políticas e sindicais;
- Família: estrutura familiar, irmãos, primos, casamento e divórcios;
- Redes Sociais: relações sociais referentes a amigos, conhecidos, associações e grupos;
- Comunicação: mensagem por duas pessoas através de email e voz.

- Rastreamento:
  - Computador: informação referente a dispositivo de utilização pessoal relacionada com o endereço IP e endereço MAC;
  - Contacto: correio eletrónico e número de telefone;
  - Localização: localização por coordenadas GPS e país.

Esses dados são um dos ativos mais importantes que uma empresa possui. Com o surgimento da economia de dados, as empresas encontram um enorme valor na recolha, partilha e utilização de dados.

2.3. Tratamento de dados

Tratamento de dados é definido como "*uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;*" (Parlamento Europeu, 2016).

Existem diversos problemas éticos no tratamento de dados, podendo ser sumarizados pelo acrónimo PAPA (Mason, 1986):

- **Privacidade (*Privacy*)**: Que informação sobre si próprio ou sobre as associações que uma pessoa deve revelar a outras pessoas, em que condições e com que salvaguardas? Que aspetos as pessoas podem guardar para si mesmas e não serem forçadas a revelar aos outros?
- **Exatidão (*Accuracy*)**: Quem é responsável pela autenticidade, exatidão e precisão

da informação? Da mesma forma, quem deve ser responsabilizado por erros na informação e como a parte lesada deve ser compensada?

- **Propriedade (*Property*)**: Quem é o dono da informação? Quais são os preços justos e corretos para a sua troca? Quem possui os canais, especialmente as vias aéreas, através dos quais as informações são transmitidas? Como o acesso a esse recurso escasso deve ser alocado?
- **Acessibilidade (*Accessibility*)**: Que informação uma pessoa ou organização tem o direito ou privilégio de obter, em que condições e com que garantias?

Assim, devemos garantir que a tecnologia da informação e a informação que ela manipula sejam usadas para aumentar a dignidade da humanidade. Para atingir esses objetivos, devemos formular um novo contrato social, que garanta a todos o direito de realizar seu próprio potencial humano (Mason, 1986).

2.4. Proteção vs. privacidade de dados

Privacidade é a capacidade de um indivíduo controlar o acesso ao seu espaço pessoal. Este espaço tem dimensões físicas, como o próprio corpo, a habitação ou o local de trabalho (em níveis diferentes), dimensões mentais, como as convicções, perfil psicológico, história pessoal, o que faz ou diz em ambiente restrito, e dimensões sociais, como a religião, partido, relacionamentos, redes em que participa, etc. O controlo do acesso a este espaço pode implicar mecanismos físicos (muros, portas, recolha de amostras fisiológicas) e de acesso a informação (escutas, câmaras, registos em papel ou digitais). Com a progressiva digitalização da Sociedade, os mecanismos de acesso a informação em suporte digital, que controlam a privacidade de dados, tornaram-se um aspeto fundamental da privacidade.

Nesta definição, estamos a deixar propositadamente de lado a questão do controlo de acesso a dados de organizações, que incluímos na questão mais geral da segurança de dados, entendida como a capacidade de garantir que as várias operações sobre os dados (consulta, criação, alteração e eliminação) só são realizadas por quem esteja autorizado a tal pelos respetivos titulares ou pela legislação. A privacidade pressupõe, portanto, a segurança, mas é um conceito que requer a capacidade de identificar pessoas singulares e se refere aos dados pessoais.

As preocupações práticas sobre privacidade de dados geralmente giram em torno de:

- Se ou como os dados são partilhados com terceiros;
- Como os dados são recolhidos ou armazenados legalmente;

- Restrições regulatórias, como por exemplo o RGPD.

Uma perspetiva abrangente sobre a privacidade de dados tem em conta todo o ciclo de vida dos dados, incluindo como os dados são recolhidos, partilhados e utilizados.

Os dados pessoais podem estar encriptados, com acesso restrito e em conformidade com os mecanismos de proteção de dados e, no entanto, falharem na privacidade por estar em falta o consentimento devido do respetivo titular.

A privacidade de dados não pode existir sem proteção dos mesmos.

A crescente utilização do armazenamento de dados via *cloud* traz novas preocupações em relação à privacidade e proteção dos dados. Todo o ciclo de vida dos dados geridos na *cloud* tem os seus problemas (Chen, 2012):

- **Geração** – geralmente utilizadores e organizações detêm e gerem a informação. Migrando os dados para a *cloud* é necessário repensar a manutenção dessa propriedade da informação;
- **Transferência** – no seio da empresa a transmissão de dados não necessita ser cifrada, mas para a efetuar fora dos limites da empresa tanto a confidencialidade como a integridade devem ser asseguradas;
- **Utilização** – geralmente os dados utilizados por aplicações baseadas na *cloud* não estão encriptados e o controlo de acessos é mais difícil;
- **Partilha** – a partilha de dados é cada vez mais comum, assim os proprietários dos dados podem autorizar o acesso a terceiros que por sua vez podem partilhar a outros sem autorização dos proprietários;
- **Armazenamento** – disponibilidade dos serviços de *cloud* atuais e futuros, e os serviços de *backup* providenciados pelo serviço da *cloud*;
- **Arquivo** – a duração do suporte de armazenamento terá de ser consistente com os requisitos de arquivo;
- **Destruição** – os dados que já não são necessários e são destruídos, devido às características do suporte de armazenamento, podem ser restaurados e resultar em divulgação de informações sensíveis.

Em maio de 2018, a Comissão Europeia decretou o Regulamento Geral de Proteção de Dados para proteger os dados pessoais dos cidadãos da União Europeia.

2.5. Regulamento geral de proteção de dados

O Regulamento Geral de Proteção de Dados (RGPD) visa estabelecer regras em relação ao tratamento de dados pessoais e à sua circulação, defendendo os direitos e liberdades das pessoas singulares.

Assim, foram definidos os seguintes princípios relativos ao tratamento de dados pessoais:

- Licitude, lealdade e transparência do tratamento de dados em relação ao titular dos dados;
- Limitação das finalidades, isto é, os dados só poderão ser tratados para a finalidade que foram recolhidos;
- Minimização dos dados recolhidos em função dos efeitos para que são recolhidos;
- Exatidão dos dados a serem tratados;
- Limitação da conservação pelo período necessário;
- Integridade e confidencialidade no seu tratamento, garantindo a segurança contra perda ou tratamento ilícito;
- Responsabilidade pelo tratamento de dados, comprovando o cumprimentos de regras e direitos.

Ao abrigo do RGPD, o tratamento só é lícito quando:

- O titular der o seu consentimento para a finalidade específica;
- For necessário para a execução de um contrato do qual o titular dos dados faz parte;
- For necessário para o cumprimento de uma obrigação jurídica;
- For necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa;
- For necessário para o exercício de funções do interesse público;
- For necessário para efeitos de interesses legítimos.

O titular dos dados tem os seguintes direitos:

- Pedidos de informação de forma transparente;
- Acesso à informação e ao processamento dos seus dados;

- Retificação sem demora dos seus dados pessoais;
- Apagamento sem demora dos seus dados pessoais;
- Limitação do tratamento dos dados pessoais;
- Portabilidade dos dados pessoais;
- Oposição e restrição sempre que identificado o seu perfil;
- Reclamação às autoridades de controlo;
- Indemnização por violação dos direitos de privacidade.

Assim, as empresas deverão cumprir algumas obrigações, nomeadamente:

- Adotar políticas de privacidade e de segurança da informação, por forma a clarificar o tratamento e finalidades da recolha de dados;
- Realizar avaliação de impacto sobre a proteção de dados relativo às atividades de elevado risco;
- Obter consentimento dos titulares para as finalidades de tratamento em causa por via de mecanismo "*opt-in*";
- Tratar os dados recolhidos para as finalidades determinadas, explícitas e legítimas;
- Efetuar registos do tratamento de dados efetuado;
- Informação aos titulares dos dados;
- Garantir os direitos de acesso, retificação, esquecimento e oposição;
- Manter os dados pessoais apenas pelo tempo necessário;
- Contemplar os princípios de "*privacy by design*" e "*privacy by default*";
- Contemplar boas práticas e medidas de segurança adequadas, nomeadamente a nível de autenticação, deveres de utilização e cuidados a ter por parte dos utilizadores;
- Contrato escritos com os subcontratantes assegurando a defesa dos direitos dos titulares dos dados;
- Participar violações de dados e incidentes de segurança à autoridade de controlo (no prazo de 72 horas) e ao titular dos dados (caso o risco seja elevado);
- Assegurar a conformidade através de auditorias.

2.6. RGPD nas empresas

Embora as pequenas, médias e microempresas desempenhem um papel decisivo na economia digital europeia, elas foram identificadas como um dos elos mais fracos da segurança da informação (Papanikas, Ntouskas, & Polemi, 2012).

As pequenas e médias empresas desconhecem o Regulamento Geral de Proteção de Dados, pelo que necessitam rapidamente da elaboração de um plano de abordagem e de implementação de processos organizacionais e/ou tecnológicos para assegurarem a conformidade com as novas exigências da Proteção de Dados Pessoais. É de todo aconselhável que este trabalho seja realizado em conjunto com as Associações dos diversos sectores da indústria, comércio e serviços (Freitas & Mira, 2018).

As empresas devem garantir que os contratos com fornecedores e prestadores de serviços contenham termos específicos de proteção de dados estabelecidos no Regulamento. Devem implementar sistemas e processos capazes de responder a solicitações de indivíduos que exercem seus direitos ao abrigo do RGPD, incluindo direitos de aceder, corrigir, transferir, excluir ou restringir o processamento de dados pessoais.

Parte do planeamento de qualquer organização inevitavelmente deve incluir uma avaliação dos riscos e a priorização dos seus investimentos em conformidade. Com base nessa avaliação, o atendimento aos requisitos da declaração de privacidade do RGPD deve quase sempre subir ao topo da lista (Hintze, 2019).

Padrões de segurança como ISO 27001 (Sistema de Gestão da Segurança da Informação) e ISO 27002 (Guia de boas prática para controlos de segurança da informação) ajudarão as organizações a garantir a existência de programas eficazes de segurança da informação (Tankard & Pathways, 2016).

O uso da ISO 27001 ajudará a garantir o princípio consagrado no RGPD de que medidas tecnológicas e organizacionais apropriadas estejam em vigor para proteger a informação. Ajudará as organizações a definir responsabilidades, como quem é responsável por determinados ativos de informação e quem pode autorizar o acesso aos dados. A ISO 27001 fornece credenciamento independente para sistemas de gestão de segurança da informação, enquanto a ISO 27002 é um código de prática que não é credenciado por terceiros, fornece recomendações de práticas recomendadas sobre controlo de segurança da informação para uso dos responsáveis por iniciar, implementar ou manter sistemas de gestão de segurança da informação.

2.7. Segurança da informação

A norma em vigor para Sistema de Gestão da Segurança da Informação é a ISO 27001. Esta norma responde às necessidades dos negócios no estabelecimento de uma política abrangente de Sistemas de Gestão da Segurança da Informação, que permite não apenas a harmonização dos processos organizacionais relacionados aos Sistemas de Informação, mas também à certificação, estabelecendo assim um ponto de referência comum para a empresa certificada no mercado global (Y. Barlette and V. V. Fomin, 2008).

A aplicação da norma é um processo de três etapas (Jd & Freeman, 2007):

- Uma organização deve preparar, desenvolver e implementar seu Sistema de Gestão da Segurança da Informação e integrá-lo ao processo comercial diário. Isso envolve a formação da equipa e o estabelecimento de um programa contínuo de manutenção do Sistema de Gestão da Segurança da Informação.
- Um dos organismos de certificação credenciados deve realizar uma auditoria do SGSI. Quando o certificado é concedido, ele dura três anos antes da recertificação ser necessária.
- O organismo de certificação visitará regularmente o site do SGSI (a cada 6 a 9 meses) para realizar uma auditoria de vigilância.

Os tópicos abordados em uma auditoria ISO 27001 incluem (Jd & Freeman, 2007):

- Política de segurança;
- Segurança organizacional;
- Classificação e controlo de ativos;
- Segurança de pessoal;
- Segurança física e ambiental;
- Gestão de comunicações e operações;
- Controlo de acesso;
- Desenvolvimento e manutenção de sistemas;
- Gestão de continuidade de negócios;
- Conformidade.

Alguns desafios na gestão da informação (Ashenden, 2008) passam pela procura por maior

conectividade e a necessidade de flexibilidade no uso de novas tecnologias. Cada vez mais, as organizações precisam compartilhar informação com clientes, partes interessadas e atravessar a cadeia de valor. Isso deve ser gerido de forma a garantir que o risco para a informação permaneça num nível aceitável.

A vertente humana tem que ser considerada pois os *hackers* passam mais tempo considerando os desafios humanos do que os profissionais de Segurança da Informação (Adams & Sasse, 1999). A gestão da segurança da informação é mais do que apenas bloqueios e chaves e deve estar relacionado ao agrupamento e comportamento sociais (Dhillon & Backhouse, 2001).

2.8. Gestão do risco

O risco é visto como "*operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais,…*" (Parlamento Europeu, 2016).

O processo de gestão do risco identifica e analisa os riscos, definindo passos para reduzir o risco a num nível aceitável. Este processo, segundo a norma ISO 27005 é composto pelas seguintes fases (International Organization for Standardization, 2018):

- Definição do contexto – serve para definir o âmbito da gestão de risco, bem como os critérios sobre os quais se vai avaliar o risco;
- Análise de risco – identificar riscos, estimar o valor e avaliar os riscos;
- Tratamento do risco – forma de lidar com o risco, quer seja pela redução, eliminação ou manutenção dos riscos existentes. É definido um plano de implementação;
- Aceitação do risco – decisão de aceitar ou não o plano de tratamento do risco;
- Comunicação do risco – troca de informação com os *stakeholders* relativa aos riscos existentes e às tomadas de decisão;
- Monitorização e análise crítica de riscos – acompanhamento e revisão dos riscos.

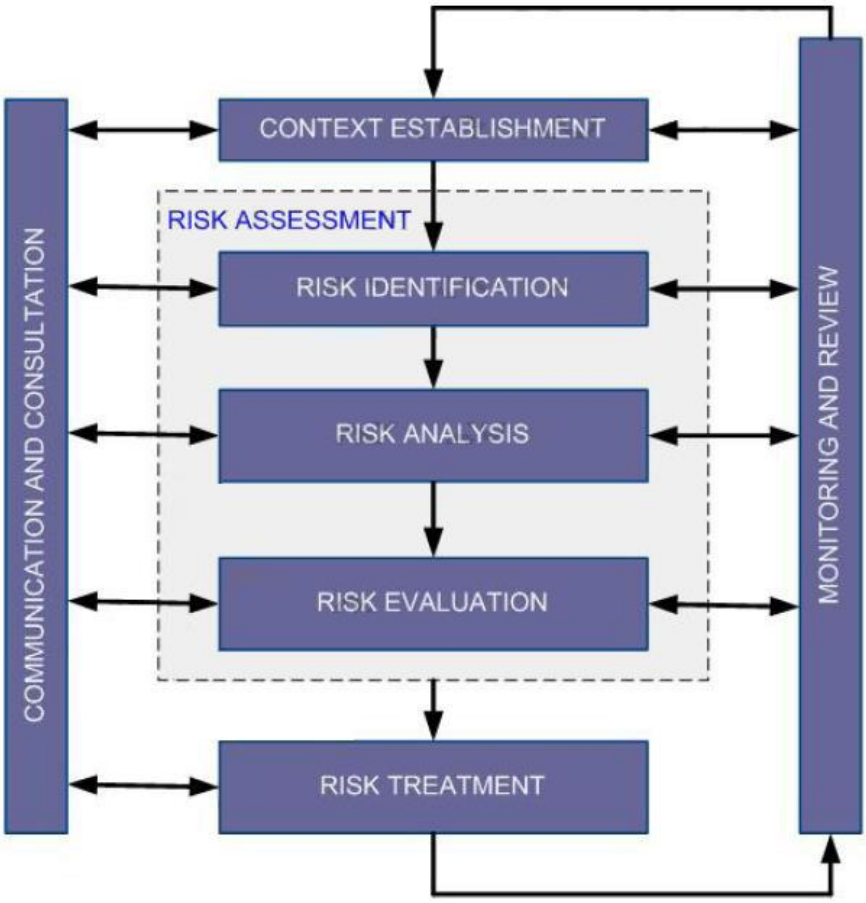


Figura 4 – Fases da Gestão do Risco segundo a ISO 27005

Fonte: International Organization for Standardization, 2018

A gestão do risco deve ser um processo em contínuo relacionado com as atividades da organização, devendo ser definidos responsáveis pelos riscos.

Uma matriz de riscos permite gerir os riscos de forma visual, identificando quais são os riscos que devem receber mais atenção. Por se tratar de uma forma de priorização de riscos, ela pode ser aplicada na avaliação de riscos.

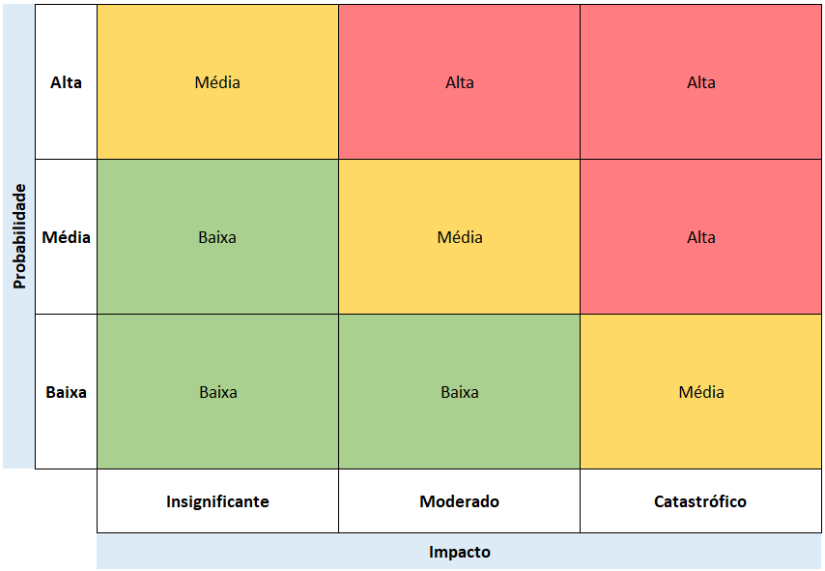


Figura 5 - Matriz de riscos

2.9. Riscos na proteção de dados

Existem tratamentos de dados que são sujeitos a risco (Mendes, 2018):

- Processamento automatizado de dados onde é traçado um perfil dos indivíduos (*profiling*);
- Processamento automatizado de dados com consequências legais;
- Processamento de dados utilizados para observar, monitorar ou controlar indivíduos;
- Processamento de dados sensíveis, tais como relativos à origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual;
- Processamento de dados em grande escala;
- Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos;
- Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.);
- Processamento de dados através de uso de novas tecnologias;
- Transferência de dados para fora da União Europeia;
- Processamento de dados que possa impedir indivíduos de exercer direitos;
- Processamento de novos tipos de dados pessoais;

- Novos tipos de processamento de dados.

Os riscos relacionados com o tratamento de dados pessoais são (Mendes, 2018):

- Recolha de dados não justificada;
- Recolha de dados excessiva;
- Acesso não autorizado aos dados;
- Destruição ou alteração acidental/ilegal de dados;
- Divulgação não autorizada de dados;
- Roubo de dados;
- Uso/armazenamento de dados desatualizados;
- Utilização dos dados para além do que é expectável;
- Utilização dos dados para além do que é socialmente aceitável;
- Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar.

2.10. Estatísticas da segurança da informação

As instituições estão a ser pressionadas sobre a proteção de dados dos seus clientes e do seu negócio. São aqui apresentadas algumas estatísticas sobre a proteção de dados (Vijayan, 2019):

- Violações de dados e ataques cibernéticos:
    - 4,1 biliões de registos de dados comprometidos em mais de 3.800 violações de dados nos primeiros seis meses de 2019;
    - 70 milhões de registos de dados roubados em 2018 devido a *clouds* do AWS S3 mal configurados;
    - $8,19 milhões: custo total médio de uma violação de dados para empresas americanas;
    - 34% das violações de dados em 2018 causada por ator interno;
    - 45% das organizações de saúde atacadas com o principal intuito de destruir dados;
- Dados Sensíveis:
    - 53% das organizações deixam 1.000 ou mais arquivos com dados

confidenciais abertos a todos os funcionários;

  - 534.465 arquivos que contêm dados confidenciais numa empresa média;
  - 1 em cada 2,2 empresas possuem aplicações móveis que acedem dados de alto risco em 2018;
  - $40 é o preço máximo para conjunto de dados pessoais na *dark web*;
  - $1.000 a $1.200 é o preço para credenciais de conta bancária com saldo de $20.000 ou mais;

- Regulamentos de dados e o segurança na *cloud*:
  - 66% dos especialistas citaram a segurança dos dados como o maior desafio ao migrar para a *cloud*;
  - 27% das organizações dizem que 95% dos seus processos de trabalho serão executadas na *cloud* em cinco anos;
  - 44% das organizações acham que garantir a segurança de dados é complexo;
  - 31% das organizações encriptam histórico de dados;
  - 59% dos especialistas em segurança de dados acham que as suas organizações estão a cumprir todos os requisitos do RGPD;
  - 42% dos responsáveis de segurança dizem que a segurança é o maior desafio à conformidade com o RGPD;
  - 10% de empresas americanas trabalham ativamente para cumprir 50 ou mais leis de privacidade;
  - 47% das organizações atualizaram as políticas de cookies de sites mais de uma vez no ano passado;
  - $55 biliões de custo inicial para as empresas da Califórnia cumprirem o California Consumer Privacy Act;

- Consciência e resposta do consumidor:
  - 78% de entrevistados que se preocupam com a segurança e a privacidade de seus dados financeiros;
  - 45% dos utilizadores tiveram as informações pessoais comprometidas pelo menos uma vez nos últimos cinco anos;

- 34% dos utilizadores dos EUA dizem que seus dados pessoais são muito vulneráveis a comprometer;
- 45% dos utilizadores dos EUA evitam abrir e-mails de pessoas que não conhecem;
- 49% dos utilizadores online europeus conhecem as regras locais de proteção de dados e privacidade;
- 64% dos utilizadores dos EUA considerariam uma empresa responsável pela perda de dados pessoais;

3. Abordagem metodológica

Na presente dissertação pretende-se, como já foi referido, contribuir para o desenvolvimento de um serviço integrado de avaliação da gestão e proteção de dados. Por forma a esta contribuição ser realizada de forma eficiente, será inicialmente executado um trabalho de revisão de literatura com o objetivo não só de perceber conceitos essenciais da área de estudo, mas também saber o que já foi feito noutras aplicações para esta área em específico, assim como perceber quais são as necessidades informacionais e os limites relativos ao cumprimento do Regulamento Geral de Proteção de Dados, bem como algumas normas relativas a segurança da informação.

Posteriormente será efetuada a análise do sistema Sistrade® MIS | ERP com o objetivo de mapear as atividades onde são utilizados os dados pessoais, identificar o fluxo informacional e a forma como são utilizados, verificando a existência de violações do referido regulamento. Para conseguir entender o sistema Sistrade® MIS | ERP, vai-se estudar o sistema, consultando os manuais de utilização, bem como realizar testes de utilização dos vários módulos, procurando detetar atividades que envolvem a utilização de dados pessoais. Numa fase posterior foram analisadas algumas necessidades de clientes e implementações específicas do sistema nesses clientes, através de um inquérito efetuado a diversos utilizadores do sistema.

Após analisado o sistema bem como as implementações efetuadas em alguns clientes modelo, será confrontado com o Regulamento Geral de Proteção de dados verificando o seu cumprimento e eventuais violações ao mesmo, efetuando sugestões de melhoria por forma a garantir o cumprimento do regulamento.

Plano de trabalho

O plano de trabalho elaborado encontra-se separado em três fases distintas. A primeira fase é relativa ao projeto da dissertação, onde se encontra a preparação da dissertação nomeadamente a revisão de literatura. A segunda fase refere-se à análise do sistema Sistrade® MIS | ERP, com o objetivo de conhecer o sistema e avaliar o tratamento de dados efetuado pelo mesmo. Já a terceira fase é dedicada à especificação da plataforma informática por forma a mitigar os riscos de violação, especificar o processo de auditoria e gerar modelos de relatórios.

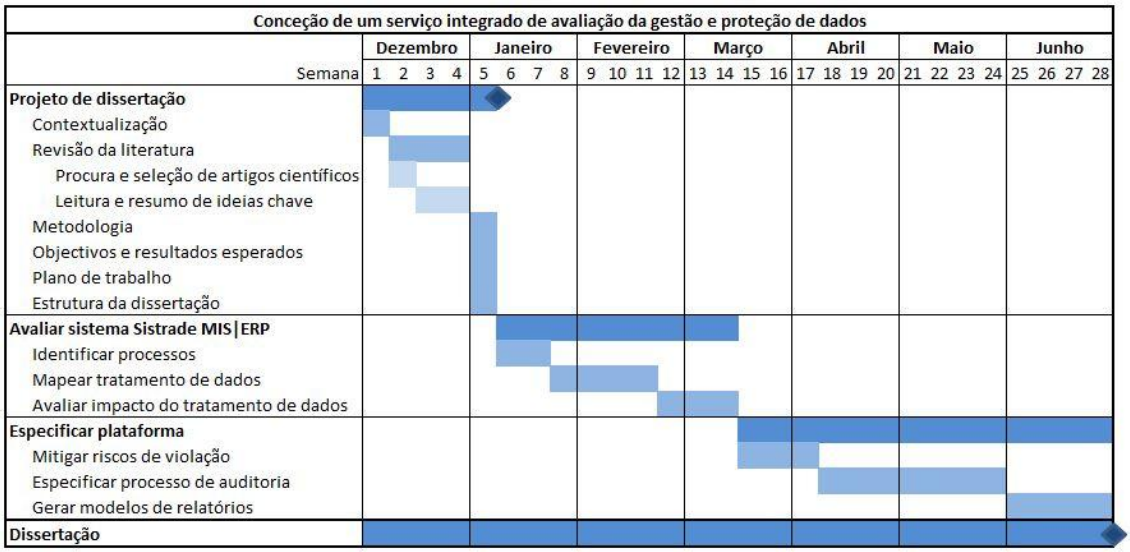


Figura 6 – Plano de trabalho

4. Avaliação do Sistrade® MIS | ERP

4.1. Identificação de processos e mapeamento dos tratamentos de dados

O Sistrade® MIS | ERP é constituído por 5 módulos, denominados por Administrativa & Financeira, Gestão Comercial & Orçamentação, Gestão da Produção, Gestão de Stocks & Compras, e Soluções de Gestão WEB.

Figura 7 – Módulos Sistrade® MIS | ERP

Fonte: Sistrade

As soluções apresentadas podem ser implementadas na sua totalidade como um ERP integrado, ou então poderão ser devidamente parametrizadas individualmente segundo as necessidades específicas de cada empresa. De referir que atualmente a solução está implementada para um total superior a 3.000 utilizadores, em mais de 20 países em 4 continentes. É uma solução baseada em SQL Server, utilizável em diversos dispositivos (PC, tablet e/ou telemóvel) e que pode ser parametrizada em infraestruturas no local ou na nuvem.

Após efetuada a identificação de processos previstos no Sistrade® MIS | ERP foi possível iniciar o mapeamento dos dados pessoais tratados. Assim, e com recurso ao modelo de formulário apresentado no anexo A, efetuou-se o mapeamento dos dados pessoais nos diferentes módulos e funcionalidades. Após efetuado o mapeamento do tratamento de dados, foi possível verificar a tramitação da informação e dos diversos dados pessoais ilustrado para os diferentes processos no anexo B.

O Regulamento Geral de Proteção de Dados veio legislar sobre a privacidade e proteção dos

dados pessoais, sendo que os sistemas de informação devem respeitar dois conceitos: a privacidade desde a conceção, isto é, no desenvolvimento de novo projeto ou processo devem ser determinadas e implementadas medidas de privacidade e procedimentos técnicos adequados de forma a garantir que o tratamento está em conformidade com o RGPD e proteger os direitos dos titulares dos dados em causa; e a privacidade por omissão, que visa assegurar que são colocados em prática mecanismos para garantir que, por defeito, apenas serão recolhidos, utilizados e conservados para cada tarefa, os dados pessoais necessários para a respetiva finalidade. Foi analisada para cada módulo e funcionalidade deste sistema, a aplicação destes dois conceitos.

4.1.1. Administrativa & Financeira

O módulo dedicado à área Administrativa e Financeira prevê um conjunto de ações e procedimentos relativos à atividade da empresa nas funções de contabilidade, tesouraria, imobilizado e de recursos humanos, com vista à maximização dos resultados económicos e financeiros.

Em relação à contabilidade, o Sistrade® MIS | ERP prevê a contabilidade geral e analítica, contando com a integração dos movimentos gerados pelos restantes módulos, automação por forma a melhorar a eficiência dos sistemas bem como prevenir erros, e a definição de lançamentos típicos da empresa. Permite ainda gerar orçamento para posterior análise do desvio entre o real e a estimativa. A gestão das contas do plano de IVA, centro de custos, fluxos de caixa e de funções ajudam a gestão financeira da organização. A gestão de períodos contabilísticos é efetuada através da abertura e fechos de anos fiscais, sendo possível efetuar a gestão do IVA e apuramento dos resultados. Toda a gestão é efetuada de acordo com os requisitos do país de implementação, nomeadamente a gestão dos impostos. Existe ainda uma panóplia de relatórios e análises disponibilizados por forma a melhorar o controlo da contabilidade da empresa, nomeadamente extrato de contas, declaração periódica do IVA, extratos de fluxo de caixa e centros de custo, mapas diários, diversos balancetes (razão, analítico, IVA, centro de custos, saldos), diário de resumos mensais, mapas de resultados líquidos, etc.

Quanto à função de tesouraria, o sistema permite efetuar a gestão de contas correntes, vendedores e agentes, e controlo de pagamentos e recebimentos. A gestão de contas correntes permite integração direta com contas bancárias, registo de liquidações e reconciliação com clientes e fornecedores, gerir os pagamentos quer pendentes a clientes que efetuados por fornecedores (nomeadamente transferir créditos e débitos entre clientes e fornecedores), emissão de confirmações de liquidações, entre outras funções. Em relação aos vendedores e

agentes, é possível efetuar uma gestão das comissões e gerir o pagamento das respectivas verbas por períodos temporais desejados. Através das funcionalidades de controlo de pagamentos e recebimentos é possível definir movimentos típicos através da programação de lançamentos automáticos, gerir pagamentos recebidos de diferentes formas (cheques, numerário, transferência bancária), com toda a gestão dos fluxos bancários. A função de tesouraria permite também acesso a uma série de relatórios e análises, nomeadamente avisos prévios de pagamentos e cobranças, folhas de pagamentos a fornecedores, impressão de recibos, carteira de clientes e fornecedores, controlo dos saldos bancários e dos cheques emitidos, etc.

A gestão de imobilizado visa gerir todo o património de uma empresa, tendo a capacidade de controlar os bens em todo o seu ciclo de vida. Assim, algumas das funcionalidades disponibilizadas são: integração direta com contabilidade, revalorizações de bens, fichas individuais de ativos, alienações, abates, reparações, etc. Alguns dos relatórios e análises que se encontram disponíveis são listas de ativos, balancetes de depreciações, mapa de revalorizações e mapa de abates.

Mapeando o tratamento de dados efetuado relativamente às funcionalidades de contabilidade, tesouraria e imobilizado, o sistema apenas faz referência a dados pessoais por forma a registar quem faz as diversas transações. Essas transações são registadas identificando o número e nome do colaborador que as efetuou. Esses dados pessoais são depois associados aos registos e poderão ser visualizados e exportados em diversos documentos, bem como mapas e relatórios relativos à atividade Administrativa & Financeira.

A gestão de recursos humanos é vital para o funcionamento das empresas. No Sistrade® MIS | ERP a gestão de recursos humanos tem como base o cadastro do colaborador, a gestão de horários e de faltas, o processamento de salários, a gestão de ações de formação e a gestão de segurança, higiene e saúde no trabalho. O cadastro de colaboradores é efetuado através da folha individual do funcionário, estando dividido em diversas secções que vão desde os dados pessoais, dados profissionais, informações relacionadas com o IRS e Segurança Social, remunerações e retenção fixa, assim como o histórico do colaborador. É possível anexar documentos relativos aos colaboradores, nomeadamente documentos de identificação, carta de condução, certificado de habilitações, etc. A gestão de horários permite efetuar a gestão das férias dos colaboradores, a definição de períodos de trabalho com os seus horários e turnos associados, a marcação de faltas e o controlo de horas extra, inclusive o tratamento de picagens com integração com relógio de ponto. Em relação à gestão de faltas, algumas das funcionalidades são a marcação das faltas quer individuais quer em grupo, permitindo acesso a calendário para visualização das ausências mensais. O processamento de salários dos

colaboradores é de vital importância num módulo de Recursos Humanos, assim tarefas como atribuição de abonos e descontos (individuais ou em grupo), controlo de possíveis adiantamentos, e o controlo dos pagamentos efetuados de diversas formas como por exemplo transferência bancária, numerário, cheque e cartões refeição. A formação é um imperativo legal que a entidade patronal deverá dar aos seus colaboradores, pelo que existe um módulo de gestão de ações de formação, com o controlo das inscrições e presenças, bem como as respetivas avaliações. Em relação à Segurança, Higiene e Saúde no Trabalho, o sistema permite o registo de consultas e exames dos colaboradores, assim como acidentes de trabalho e doenças profissionais, permite promover ações de saúde e efetuar programas de prevenção, registar fatores de riscos de diversas origens (físicos, químicos, biológicos, etc.), controlar a entrega de EPI's (Equipamentos de Proteção Individual) aos colaboradores, e registar auditorias e inspeções por entidades internas ou externas. Como nas restantes funções, a gestão de recursos humanos disponibiliza diversos relatórios, tanto internos (recibos de vencimentos, mapa de vencimentos, mapa de pagamentos, mapa de faltas, etc.) como relatórios legais (declaração mensal de remunerações, modelo 10, relatório único, folha de férias, etc.).

Em relação a estas funcionalidades de recursos humanos, o sistema efetua o tratamento de dados através do cadastro do colaborador onde se pode verificar inúmeros dados pessoais.

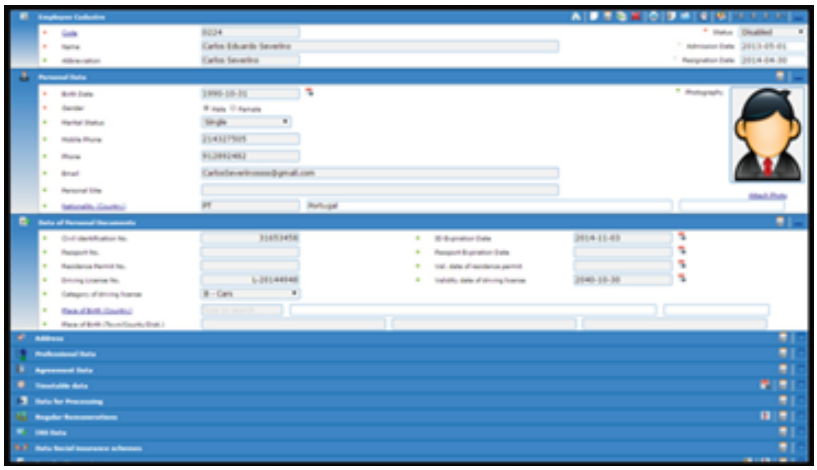


Figura 8 – RH: Cadastro de colaborador

Fonte: Sistrade

Na admissão do colaborador são solicitados dados pessoais e profissionais com a finalidade de serem registados no seu cadastro. Alguns dos campos solicitados são: nome, morada, nº cartão identificação, nº contribuinte, nº segurança social, data de nascimento, sexo, nacionalidade, nº telemóvel, etc. Os campos disponíveis são selecionados durante a parametrização da solução. O cadastro do colaborador é posteriormente atualizado conforme

os processamentos efetuados como remunerações e retenções associadas a IRS e Segurança Social, assim como possíveis adiantamentos e penhoras de vencimento. O acesso a estes dados pessoais na funcionalidade de Recursos Humanos é suposto ser efetuado apenas pelos colaboradores do Departamento de Recursos Humanos. Todos os registos podem ser visualizados em diversos documentos, mapas e relatórios, podendo ser exportados em diversos formatos.

4.1.2. Gestão Comercial & Orçamentação

O módulo de Gestão Comercial & Orçamentação engloba algumas funcionalidades como CRM, orçamentação, gestão de propostas, encomendas, expedição e faturação.

Um CRM visa melhorar a relação com o cliente potencializando as vendas da empresa utilizando para algumas funcionalidades conforme a figura 9. O calendário permite efetuar uma gestão de interações e de eventos e tarefas como reuniões ou visitas comerciais. Existem contas para definir objetivos mediante diversos parâmetros (período temporal, comercial, cliente, produto ou gama de produtos, etc.). O serviço pós-venda permite gerir as reclamações do cliente e assegurar o tratamento das mesmas. O CRM permite ainda retirar uma série de informações e relatórios do sistema, nomeadamente: contas (com moradas e contactos), histórico de contactos, oportunidades de vendas, evolução da faturação real / prevista, reclamações, etc.

Figura 9 – Customer Relationship Management (CRM)

Fonte: Sistrade

No que diz respeito ao CRM, e sendo um sistema de informação que automatiza as funções de contacto com o cliente, é um sistema sensível em relação a dados pessoais. O sistema identifica clientes e outros *stakeholders* como sendo um Terceiro, podendo este ter vários tipos de entidade. O sistema associa ao Terceiro uma Gestão de Dados Pessoais, quando na verdade apenas se tratam de dados empresariais. A intenção dos campos previstos prevê apenas a sua utilização para dados empresariais, no entanto facilmente os utilizadores podem adaptar os campos para uma utilização pessoal.

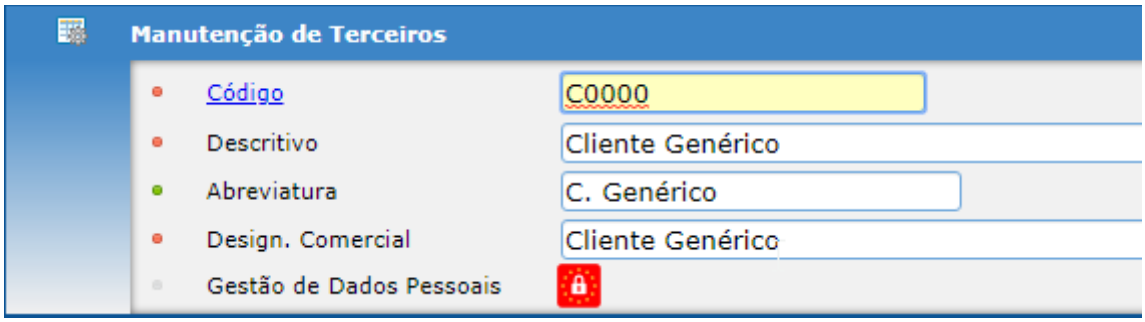


Figura 10 – CRM: Manutenção de Terceiros

Fonte: Sistrade

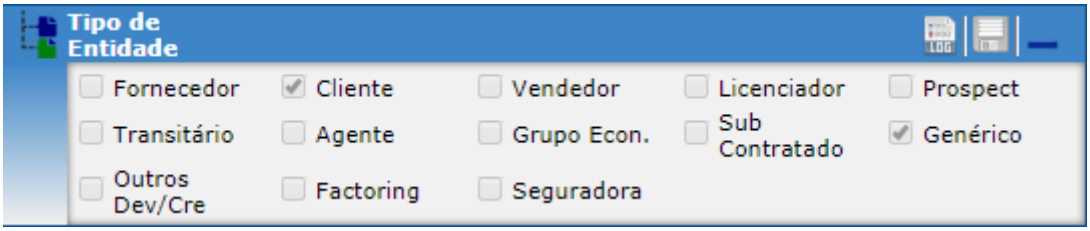


Figura 11 – CRM: Tipos de entidades

Fonte: Sistrade

As informações registadas no CRM estão subdivididas em vários sectores, sendo que no sector de Morada estão alguns campos que poderão facilmente ser incorretamente preenchidos com dados pessoais, como por exemplo telefone e e-mail.

Figura 12 – CRM: Subdivisão da informação de Terceiros

Fonte: Sistrade

A funcionalidade de orçamentação permite gerir um pedido de orçamento até à sua aprovação por parte do cliente. Assim, mediante um pedido de orçamento, é possível calcular os custos do serviço solicitado, avaliando o custo das matérias-primas, o custo de recursos/máquinas, o tempo de execução do serviço desde a preparação até à sua finalização, incluindo ainda a possibilidade de contemplar custos de subcontratação de certos serviços. Após calculado o custo do serviço é possível aplicar margens financeiras, como margens de lucro, custos administrativos, etc. Definido o preço de venda é possível simular diferentes quantidades para o mesmo serviço, e enviar o orçamento por correio eletrónico diretamente do ERP para o cliente, até ter a aprovação do orçamento por parte do cliente.

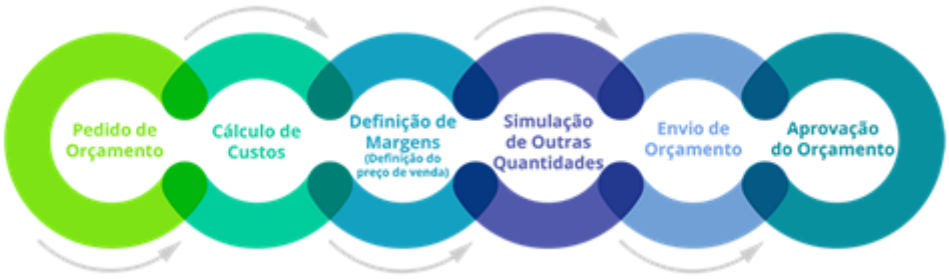


Figura 13 – Fluxo do pedido de orçamento

Fonte: Sistrade

A gestão de propostas permite gerir os orçamentos agrupando-os e tratando-os como um só.

A gestão de encomendas permite gerir o estado das encomendas. As encomendas podem ser classificadas como: pendente, confirmada, aprovada para produção, etc. É possível e mediante a ficha de cliente, controlar o limite de crédito associado ao mesmo. As encomendas podem estar associadas a vários serviços diferentes, pelo que é possível atribuir vários tipos de descontos, e planos de entregas faseados por data e destino.

Nestes processos de orçamentação, gestão de propostas e encomendas os dados pessoais localizados foram apenas relativos à criação pelo utilizador, e ao seguimento dado por outros utilizadores para aprovação dos documentos em causa. Essas aprovações podem ser técnicas para garantir a validade do orçamento, ou então financeira para garantir a aprovação por parte do responsável. Após essas validações feitas, o orçamento pode seguir para o cliente. Acompanhando a proposta na funcionalidade de gestão de proposta, e sendo o orçamento aprovado é efetuado o registo da encomenda. Para cada validação é registado o utilizador responsável pela mesma. Esses dados pessoais (numero de empregado e nome) são depois associados aos registos e poderão ser visualizados e exportados em diversos documentos, bem como mapas e relatórios relativos à atividade de Gestão Comercial & Orçamentação.

A expedição é o processo que trata da transferência do produto. Nesta funcionalidade o sistema permite criar guias de remessa e guias de transporte que suportam o transporte do produto quer para fornecedores quer para o cliente final, para isso emite a saída de material do armazém. Na criação destes documentos o sistema permite a comunicação à Autoridade Tributária conforme obrigatoriedade legal imposta pelo Decreto-Lei nº 198/2012.

A faturação é essencial para o cliente num sistema ERP. O Sistrade® MIS | ERP permite além da emissão de faturas, criar notas de débito e crédito, bem como faturas pró-forma. Para tal, permite recorrer à faturação em bloco, agregando várias faturas do mesmo cliente. A emissão das faturas poderá ser efetuada recorrendo a faturação eletrónica via EDI (*Electronic Data Interchange*) mantendo a validade legal do documento.

Relativamente aos processos de expedição e faturação, os únicos dados pessoais que surgem são o número e nome do colaborador que criou os respectivos documentos, bem como a mesma informação para quem deu seguimento a esses documentos internamente. Todas essas informações podem ser extraídas do sistema, bem como visualizadas através de documentos, mapas e relatórios.

4.1.3. Gestão da Produção

O módulo de Gestão da Produção permite às empresas incorporar conceitos da Indústria 4.0 e automatizar as linhas de produção. Algumas das funcionalidades do sistema são o *Product*

Lifecycle Management (PLM), Ordens de Fabrico, *Supervisory Control and Data Acquisition* (SCADA), *Kaizen Dashboard*, *Andon Board*, *Overall Equipment Effectiveness* (OEE) e *Scheduling*.

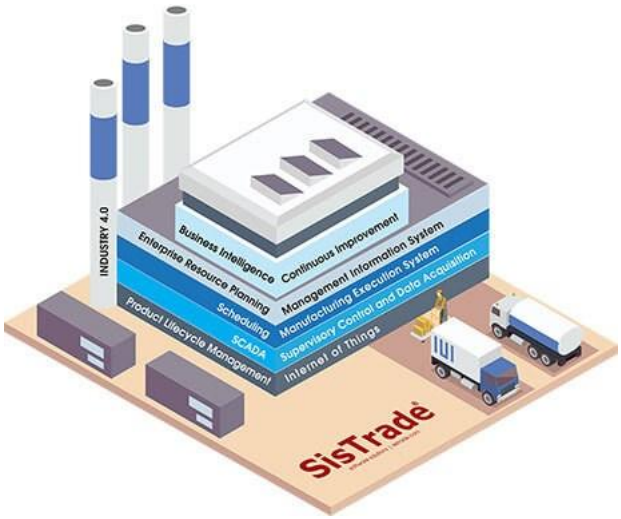


Figura 14 – Indústria 4.0 na Gestão de Produção

Fonte: Sistrade

O *Product Lifecycle Management* (PLM) é um processo que visa a gestão de todo o ciclo de vida de um produto, desde a sua conceção, passando pela fabricação até ao final de vida do produto. O sistema através de fichas técnicas do produto, árvore de produtos, controlo de versões, gestão de números de série, teste e ensaios, entre outras funcionalidades, permite um PLM eficiente.

Neste processos de *Product Lifecycle Management* (PLM) apenas se encontram dados pessoais referindo os colaboradores associados às transações dos produtos. Esses dados pessoais identificam os colaboradores pelo número de empregado e nome, e podem ser visualizados e exportados posteriormente associados a documentos, mapas e relatórios referentes ao *Product Lifecycle Management* (PLM).

A partir das Ordens de Fabrico é possível criar instruções de trabalho para o chão de fábrica com informação daquilo que se deve fabricar. Estas Ordens de Fabrico podem ser emitidas manualmente ou geradas através das encomendas efetuadas pelos clientes. Aqui temos algumas funcionalidades como gestão de séries e versões, *workflow* de aprovação das Ordens de Fabrico, anexo de documentos de apoio ao processo produtivo, parâmetros de máquinas utilizadas, associação com a ficha técnica do produto, definição de lotes de produção, etc. Umas das ferramentas utilizadas é a consola de recolha de dados no chão de fábrica.

Relativamente às Ordens de Fabrico, os dados pessoais utilizados visam a identificação pelo

número de empregado, nome e foto, dos diversos colaboradores nas diferentes fases da ordem de fabrico, desde o colaborador que criou a ordem de fabrico, passando por todas as fases até à sua conclusão. A consola de recolha de dados no chão de fábrica permite visualizar como decorre a ordem de fabrico, sendo possível visualizar quem são os operadores encarregues das mesmas. Os dados pessoais utilizados podem posteriormente ser visualizados e exportados em diversos documentos, bem como mapas e relatórios relativos às Ordens de Fabrico.

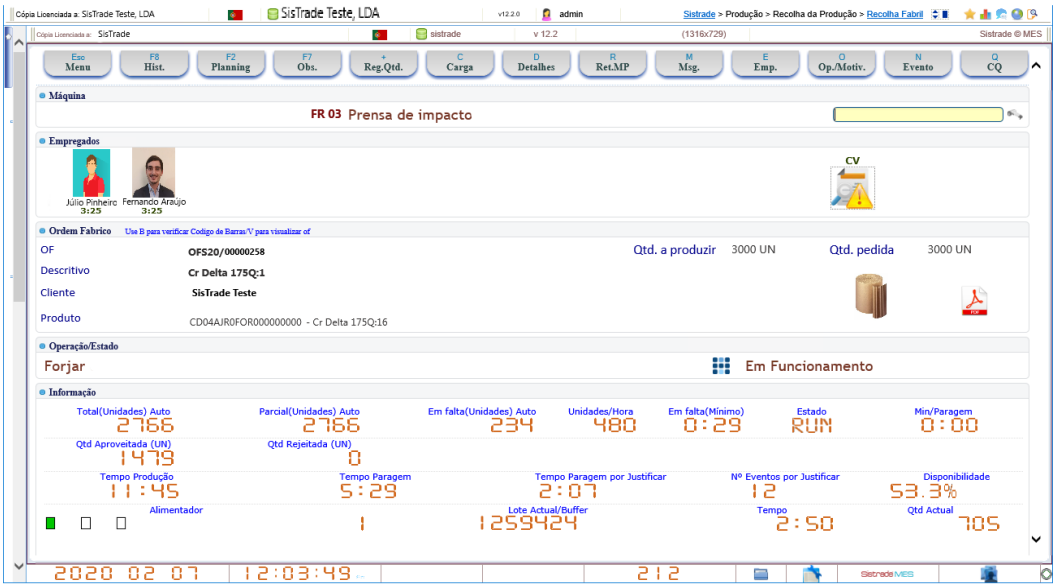


Figura 15 – Gestão de Produção: Consola de recolha de dados no chão de fábrica

Fonte: Sistrade

O *Supervisory Control and Data Acquisition* (SCADA) permite a monitorização do processo produtivo em tempo real. Utiliza a recolha de dados por diversas formas, desde introdução manual pelos trabalhadores, sensores de máquinas ou *Programmable Logic Controllers* (PLC's), apresentando uma planta da fábrica com todas as máquinas e o atual estado das mesmas. O sistema permite a supervisão de diversas fábricas remotamente, identificação dos colaboradores que operam as máquinas, ordens de produção em execução, velocidades por máquina, tempos e motivos de paragens, análises de rentabilidade e taxas de ocupação, etc. Com estes sistemas de recolha automática de dados, o sistema permite um aumento de fiabilidade dos dados, minimizando o erro humano, com um melhor controlo da velocidade das máquinas. Alguns dos dados medidos podem ser a velocidade, grossura, contador, gás, peso, temperatura, etc.

O *Supervisory Control and Data Acquisition* (SCADA) é uma funcionalidade parametrizável que tem a capacidade de apresentar uma planta da fábrica, com identificação das máquinas, dos colaboradores e respectivas ordens de fabrico em tempo real. Assim, e conforme a

parametrização da planta que for efetuada, permite ter os dados dos colaboradores afetos às máquinas e às ordens de fabrico. Aqui os dados pessoais dos colaboradores utilizados são o número de empregado e o nome, conseguindo ainda identificar a localização do colaborador conforme a máquina que estiver associado. Os dados poderão ser visualizados e exportados em diversos documentos, mapas e relatórios.

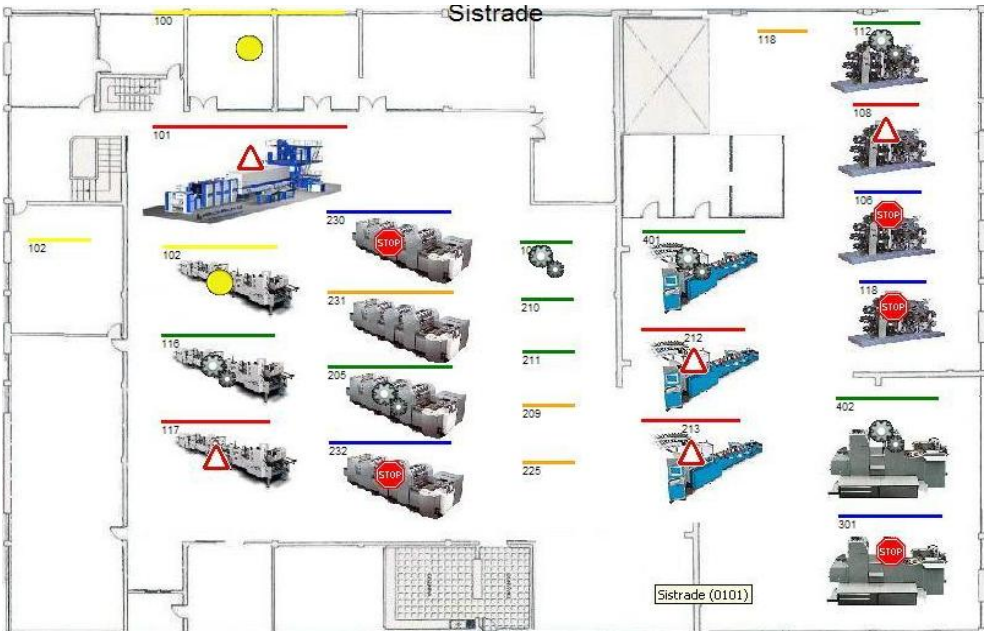


Figura 16 – Gestão de Produção: *Supervisory Control and Data Acquisition* (SCADA)

Fonte: Sistrade

Através do *Kaizen Dashboard* é possível implementar a metodologia *Kaizen* com um *dashboard* interativo dispensando os usuais quadros, canetas e papéis. Nestes *dashboards* podem ser visualizados diversos dados agrupados de diferentes formas, como por exemplo, por máquina, por tempo, por turno, por colaborador, por ordem de fabrico, etc. A apresentação de dados depende da necessidade do negócio, sendo que por muitas vezes são utilizados ecrãs tácteis para suporte às reuniões *Kaizen*.

Também o *Kaizen Dashboard* é uma ferramenta parametrizável que tem por função apresentar um *dashboard* com as informações pretendidas. Assim, uma das possíveis visualizações trata-se da apresentação de dados por colaborador, havendo ai uma utilização de dados pessoais identificando os colaboradores pelo nome e foto. A sua localização de implementação é diversa, desde salas de reuniões, chão de fábrica e até receções das empresas. Todos os mapas são passíveis de serem visualizados e exportados.

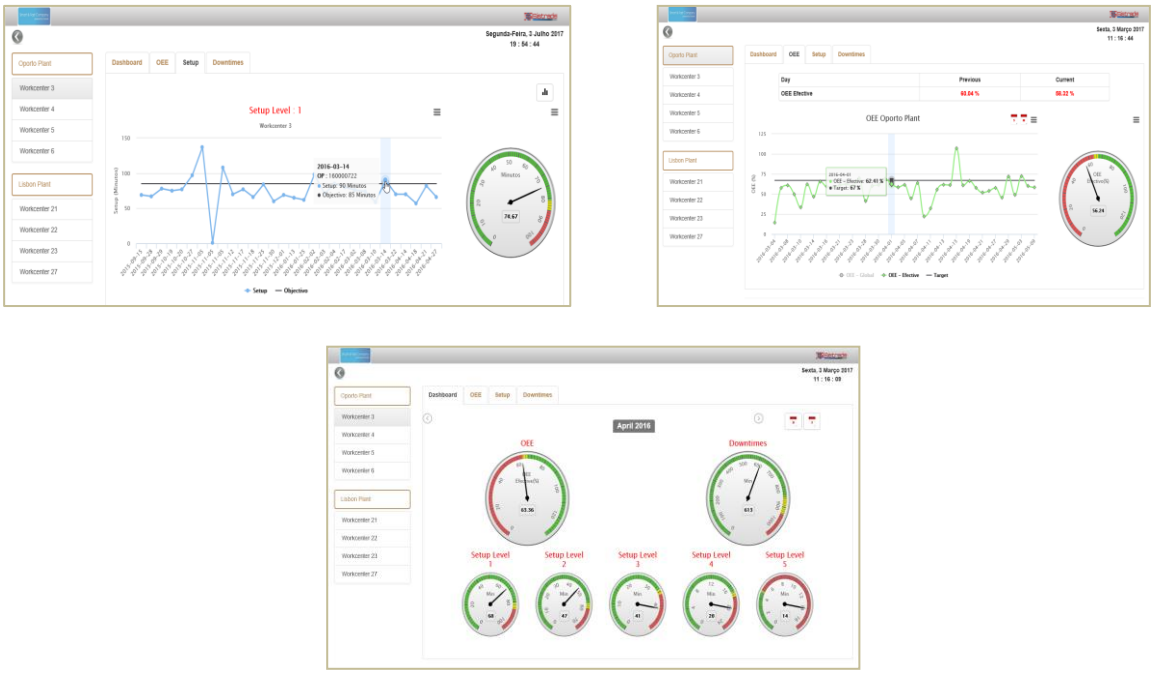


Figura 17 – Gestão de Produção: *Kaizen Dashboard*

Fonte: Sistrade

O *Andon Board* é um quadro visual que demonstra o estado das linhas de produção e no qual podem ser parametrizados alertas na ocorrência de certos eventos. Normalmente o *Andon Board* apresenta algumas informações como KPI's, atrasos e tempos de paragens, ordens de produção atual e seguinte, comparativo entre produtividade real e prevista, entre outras informações.

O *Andon Board* também consegue ser parametrizável, contendo muitas vezes alguns dados a nível pessoal. A identificação dos colaboradores por número de empregado, nome e foto associados aos dados de produção é uma constante, sendo a maior parte das vezes implementado no chão de fábrica, mas também em escritórios e mesmo em receções das empresas. Todos os mapas apresentados além de visualizados em tempo real, podem ser visualizados e extraídos posteriormente.

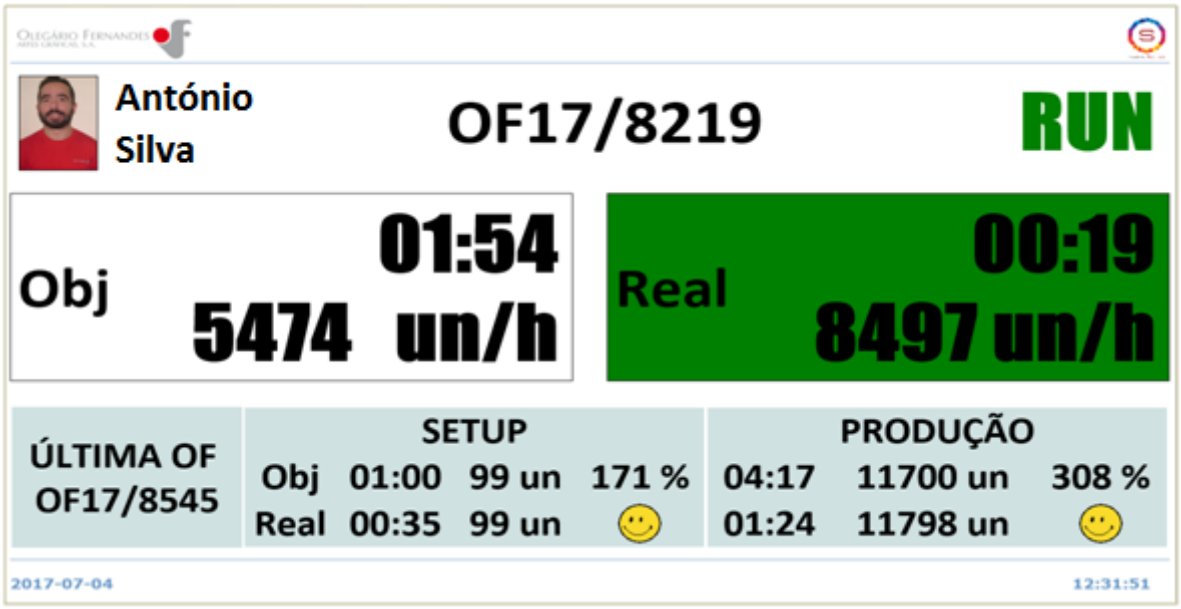


Figura 18 – Gestão de Produção: *Andon Board*

Fonte: Sistrade

O *Overall Equipment Effectiveness* (OEE) é um rácio que mede o quanto uma unidade produtiva se comporta em relação à sua capacidade teórica através da análise de 3 fatores: disponibilidade, desempenho e qualidade. O Sistrade® MIS | ERP permite calcular em tempo real o OEE com intuito de otimizar a produtividade e contribuindo para a melhoria contínua da fábrica. Alguns dos relatórios disponíveis são: análise de performance atual, análise de tempos de paragem, rácios de disponibilidade, eficiência e qualidade, rácio OEE, performance por turno, máquina e colaborador.

O *Schedulling* permite organizar toda a produção da unidade fabril. Dadas as ordens de fabrico em lista de espera e as tarefas que cada ordem de fabrico terá que executar, é possível programar todo o trabalho num gráfico de *Gantt*. A programação respeita a sequência lógica e necessária para realização das ordens de fabrico, e apresenta várias opções conforme os critérios selecionados.

O *Schedulling* tem como resultado um gráfico de *Gantt* onde é possível verificar as ordens de fabrico planeadas para produção, sendo que algumas das vistas possíveis permitem verificar os colaboradores afetos a cada ordem de fabrico. Os colaboradores são identificados pelo número de empregado, nome e foto, podendo os dados serem visualizados e exportados em diversos documentos, mapas e relatórios.

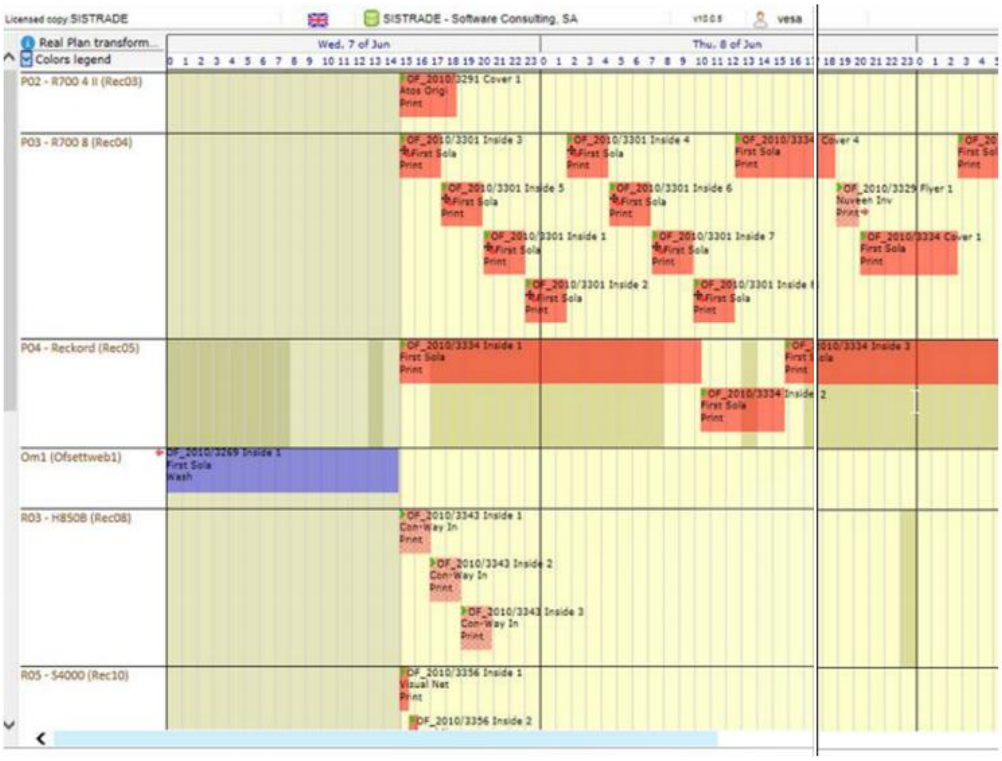


Figura 19 – Gestão de Produção: *Schedulling*

Fonte: Sistrade

4.1.4. Gestão de Stocks & Compras

Em qualquer ERP, o módulo de gestão de stocks e compras é essencial, pois o seu desempenho tem reflexo direto no resultado da empresa. A decisão de comprar, que materiais comprar, a que fornecedor e qual a quantidade necessária são cruciais na gestão do negócio. Assim, o Sistrade® MIS | ERP neste módulo trabalha com o aprovisionamento, gestão de fornecedores e stocks.

O aprovisionamento tem por função efetuar o planeamento de necessidades de material (MRP – *Material Requirements Planning*) que, com base num algoritmo, permite analisar as necessidades de material para suprir as ordens de fabrico e sugerir as compras a efetuar. Efetuada a sugestão das compras a realizar, é necessário validar as compras que efetivamente vão ocorrer, entrando em ação a gestão de compras que irá assegurar a melhor combinação entre os preços dos diferentes fornecedores e os prazos de entrega do material.

O processo de aprovisionamento, tendo por funcionalidade a identificação das matérias primas necessárias, regista como dados pessoais apenas a identificação de quem deu início a essa transação, bem como a aprovação da mesma. Esses dados podem ser visualizados e exportados em diversos documentos, mapas e relatórios.

A gestão de fornecedores permite gerir toda a cadeia de abastecimento, gerindo catálogos de fornecedores e os seus contratos de fornecimento. É possível fazer a interligação de fornecedores com os materiais ou serviços fornecidos.

A gestão de fornecedores, lidando com toda a cadeia de abastecimento, ligando os fornecedores aos materiais, regista dados pessoais dos colaboradores que intervieram no processo de compra, identificando-os pelo número de colaborador e pelo nome. Mais uma vez, esses dados além de visualizados podem ser exportados no formato de vários documentos, mapas e relatórios.

A gestão de stocks permite monitorar em tempo real todo o inventário da empresa. Ações como saídas de materiais para produção, vendas de produto acabado, devoluções, etc. são alguns dos movimentos possíveis previsto nas movimentações de stock. O sistema permite a gestão multi armazém e com recurso a localizações dos materiais. Assim, e com o auxílio de leitores óticos, é possível simplificar toda a movimentação de materiais dentro dos armazéns, nomeadamente a receção e carga dos materiais, inventariação, recolha para consumo nas ordens de fabrico e recolha para expedição final para o cliente.

Em relação ao processo de gestão de stocks, os dados pessoais associados são de todos os colaboradores que movimentaram os materiais, desde a entrada do material em armazém, ao seu consumo nas ordens de fabrico, até à sua saída do armazém por venda do produto. Também os documentos, mapas e relatórios referentes a gestão de stocks podem ser visualizados e exportados do Sistrade® MIS | ERP.

4.1.5. Soluções de Gestão WEB

O Sistrade® MIS | ERP tem também outras funcionalidades que permitem agilizar toda a operação de uma empresa. Tais funcionalidades são: manutenção de equipamentos, controlo de qualidade, gestão de energia, *business intelligence*, gestão de projetos, gestão de investigação, desenvolvimento e inovação e gestão de dados pessoais.

A manutenção de equipamentos permite hierarquizar os ativos da empresa e apresentar detalhe desses mesmos ativos rastreando o seu percurso. A manutenção poderá ocorrer de duas formas, ou preventiva, antecipando possíveis falhas de desempenho, ou corretiva, por forma a repor o funcionamento normal do ativo. O registo de incidências permite verificar o histórico de manutenções. Na realização da manutenção é gerada uma ordem de manutenção onde são registadas todas as informações associadas a essa manutenção (dados do equipamento, material necessário, descritivo da ocorrência, documentação associada, colaboradores envolvidos, etc.), incluindo a possibilidade de recorrer a subcontratação de

serviços de manutenção. É possível também efetuar a gestão de stocks e *spares (*peças sobresselentes*)*, gerindo todas as peças e materiais necessários para efetuar a manutenção. Todas estas atividades podem ser planeadas num diagrama de *Gantt*, estando este integrado com o planeamento de produção.

A manutenção de equipamentos visa elencar os ativos existentes numa empresa e gerir todas as manutenções associadas a esses ativos. Assim, os dados pessoais existentes neste processo limitam-se à identificação dos colaboradores que detetaram a falha do equipamento, bem como dos colaboradores que estiveram envolvidos no restauro do ativo à normalidade. Esses colaboradores são identificados pelo seu número e nome. Os dados pessoais, posteriormente, podem ser visualizados em diversos documentos, mapas e relatórios relativos à manutenção do equipamento.

Durante o processo produtivo de uma empresa é necessário garantir a qualidade dos produtos efetuando Controlo de Qualidade. Este módulo permite controlar a qualidade de diversos parâmetros em diferentes pontos do processo de produção, desde o controlo de matérias-primas, a semi-fabricados e acabando no produto final. Automaticamente e durante o processo produtivo, o sistema alerta para inspeções a serem efetuadas, permitindo o registo do resultado do ensaio/teste efetuado. Com base nos resultados obtidos podem ser efetuadas calibrações aos equipamentos para garantir a conformidade do produto final.

O controlo de qualidade apenas regista dados pessoais por forma a identificar quem realizou esse controlo. A identificação é efetuada através do número e nome do colaborador. Essa identificação perdura no sistema através da sua presença em documentos, mapas e relatórios respeitantes ao controlo de qualidade, podendo ser visualizados e exportados do sistema.

O sistema de gestão de energia permite rastrear todos os recursos energéticos e monitorizar todos os seus custos. Através de analisadores de energia é possível saber quais são os equipamentos ou setores produtivos que consomem mais, permitindo efetuar uma gestão energética, alocando as operações com maior consumo energético para períodos com um custo energético mais barato. Através da análise dos picos energéticos, é possível corrigir a rede elétrica para aumentar o tempo de vida dos equipamentos. Cruzando com as ordens de fabrico e o consumo energético durante a produção é possível calcular a pegada ecológica dos produtos acabados.

O módulo de gestão de energia visa monitorizar os recursos energéticos da empresa e é desprovido de dados pessoais. Apenas integra os analisadores de corrente elétrica e extrai os consumos de uma instalação fabril.

O módulo de *business intelligence* é transversal ao sistema e permite retirar análises

multidimensionais para melhorar o processo de tomada de decisão. Assim, permite analisar os dados registados nos restantes módulos (administrativo & financeiro, comercial & orçamentação, produção, stocks & compras, etc.), e apresentá-los de uma forma analítica e gráfica conforme as necessidades da organização em causa. Alguns dos *dashboards* comuns são os de vendas, onde são analisadas as vendas e finanças da organização; os de compras, com análise de compras e de stocks; e os de produção, com indicadores de produção.

A Gestão de Dados Pessoais tenta efetuar essa gestão através do registo de autorizações de uso dos mesmos, permitindo ainda o seu esquecimento.

A gestão de dados pessoais pretende atingir a conformidade com o RGPD, assegurando a gestão das autorizações de uso desses mesmos dados e também permitindo o seu esquecimento através da eliminação dos dados. Esta funcionalidade, no entanto, está conectada à Gestão de Terceiros, onde são geridos os dados empresariais e não os dados pessoais. Esta gestão não permite uma característica importante na gestão de dados pessoais: a granularidade.

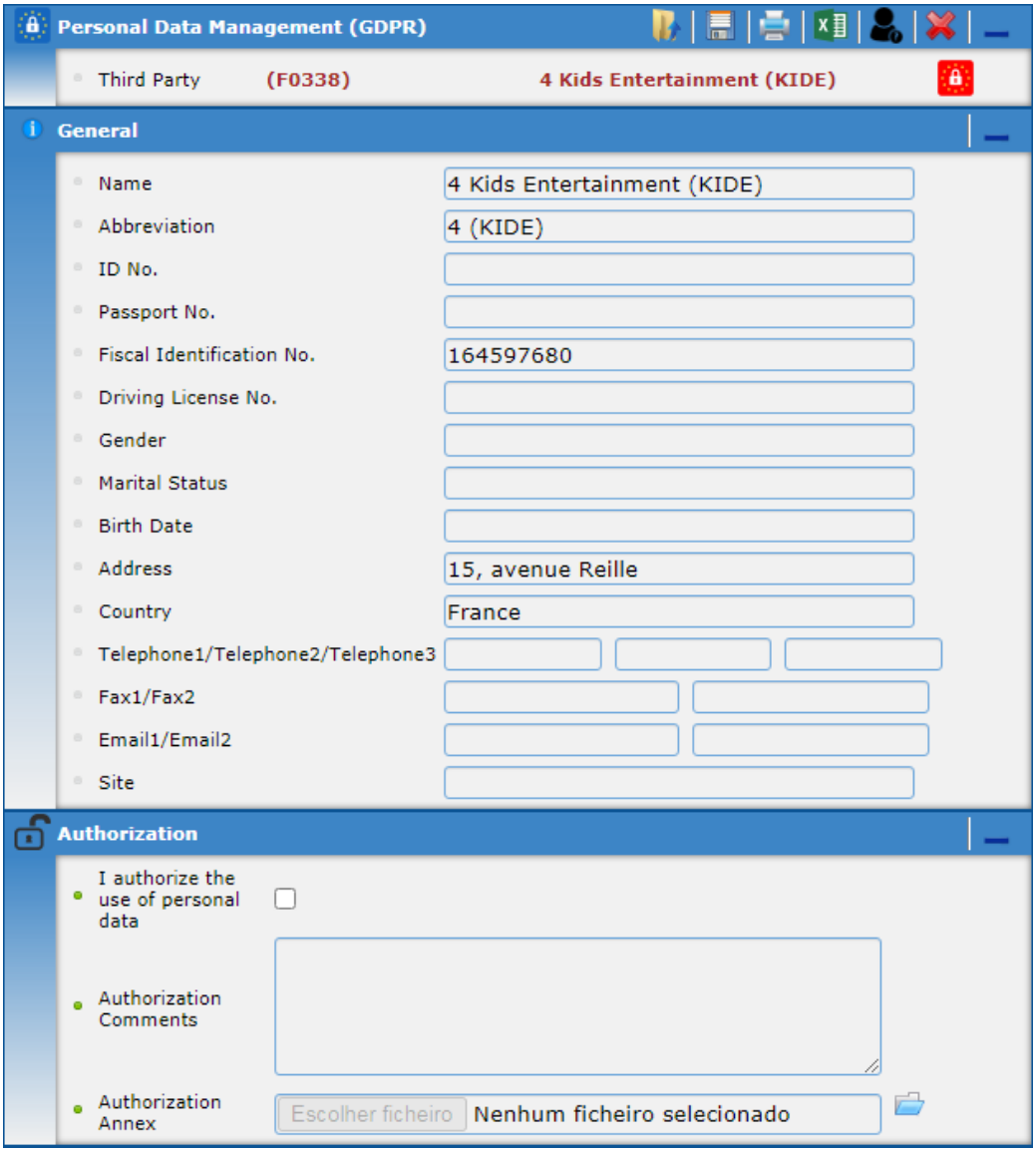


Figura 20 – Gestão de Dados Pessoais

Fonte: Sistrade

4.2. Avaliação do impacto dos tratamentos de dados

Após a identificação dos processos e o respectivo mapeamento dos tratamentos de dados pessoais nos diversos módulos / funcionalidades do Sistrade® MIS | ERP, foi efetuada uma avaliação do impacto desses tratamentos.

4.2.1. Administrativa & Financeira

Neste módulo, foi identificado dois tipos de tratamentos de dados, um relativo às funcionalidades de contabilidade, tesouraria e imobilizado, e outro em relação à funcionalidade de Recursos Humanos.

O tratamento de dados pessoais nas funções de contabilidade, tesouraria e imobilizado, enquadra-se como um processamento de dados utilizados para garantir a rastreabilidade de registos, nomeadamente quem os efetuou e se tinha autorização para o efeito. Devido à existência de um contrato de trabalho, o responsável pelo tratamento, que é a entidade patronal, terá já licitude para o fazer. Neste caso, o risco está associado a acessos não autorizados, divulgação não autorizada de dados e roubo de dados. Este risco é considerado de probabilidade baixa e com um impacto insignificante.

Na função de Recursos Humanos, os dados são mais sensíveis quer pela diversidade quer pela quantidade. Aqui o tratamento de dados é efetuado de duas formas: registo de quem efetua as operações e o cadastro dos colaboradores. Enquanto o registo de quem efetua as operações está relacionado com a rastreabilidade dos registo e da autorização do utilizador para efetuar tais registos, já o cadastro dos colaboradores está relacionado com o cumprimento de requisitos legais (nomeadamente comunicações às autoridades e segurança social). Aqui o responsável pelo tratamento é a entidade patronal e através do contrato de trabalho terá licitude para o devido tratamento. Já no caso, por exemplo, da entidade patronal decidir transferir essa base de dados de pessoal para um parceiro, entra num novo tipo de processamento de dados. O risco associado aos dados prende-se com a recolha de dados excessivo para a finalidade em causa, acessos não autorizados, divulgação não autorizada de dados e roubo de dados. Este risco é considerado de probabilidade média, mas com um impacto catastrófico caso exista uma violação de segurança. Esta função é fulcral na gestão de dados pessoais do Sistrade® MIS | ERP, visto ser a base de onde todas as outras funções recolhem dados. Assim, a instalação do sistema deverá ser acompanhada de cuidados específicos tendo por base princípios de justificação e minimização dos recolhidos e tratados.

SISTRADE MIS | ERP

Módulo: ***Administrativa & Financeiro***

FUNCIONALIDADES	DADOS PESSOAIS	OUTPUT	PROCESSAMENTO	JUSTIFICAÇÃO	RISCO	NÍVEL DE RISCO
Contabilidade	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Tesouraria	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Imobilizado	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Recursos Humanos	Diversos dados pessoais dos colaboradores	Cadastro do colaborador	Garantir cumprimento de requisitos legais Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Recolha de dados excessiva Acesso não autorizado Divulgação Roubo	

Tabela 1 – Risco no módulo Administrativo & Financeiro

4.2.2. Gestão Comercial & Orçamentação

Nas funcionalidades do módulo de Gestão Comercial & Orçamentação, o tratamento de dados efetuado é também muito limitado e restringe-se a garantir a rastreabilidade dos registos efetuados tendo como licitude o contrato de trabalho em vigor. Aqui o risco está relacionado com acessos não autorizados, divulgação não autorizada de dados e roubo de dados. Este risco é considerado de probabilidade baixa e com um impacto insignificante.

A vertente CRM e Gestão de proposta, apenas efetuam referência a dados pessoais no âmbito de quem encaminhou o processo internamente, no entanto é surpreendente um sistema de CRM e de Gestão de Propostas que não faça referência aos interlocutores nos parceiros, sendo um ponto onde eventuais auditores possam identificar que caso os dados pessoais não sejam guardados dentro do sistema poderão ser tratados de uma forma menos condizente com o RGPD. Assim, foi efetuado um inquérito junto de alguns clientes do Sistrade® MIS|ERP por forma a averiguar como efetuam a gestão de interlocutores nas suas organizações. É apresentado o questionário do inquérito, bem como o seu resultado, no anexo C. Desse inquérito podemos concluir que a maioria dos clientes regista os dados dos seus interlocutores em soluções alternativas como o Outlook e o próprio telemóvel, e consideram que seria interessante conseguir reunir essa informação no próprio sistema. Podemos afirmar que o acréscimo de funcionalidades relativas ao registo dos dados pessoais dos interlocutores a que se destinam, poderia conferir vantagem competitiva do Sistrade® MIS|ERP, dispensando outro tipo de sistemas que permitam gerir os dados pessoais dos interlocutores de CRM e Gestão de Propostas. Nesse caso, nessas novas funcionalidades, o tratamento passaria para um processamento de dados seria utilizado para um acompanhamento comercial ao interlocutor, sendo necessário um consentimento do mesmo para o tratamento desses dados (tendo sempre em atenção a justificação e a minimização dos dados tratados). Aqui o risco iria ser aumentado, passando para uma probabilidade média, com um impacto bastante mais significativo.

SISTRADE MIS | ERP

Módulo: *Gestão Comercial & Orçamentação*

FUNCIONALIDADES	DADOS PESSOAIS	OUTPUT	PROCESSAMENTO	JUSTIFICAÇÃO	RISCO	NÍVEL DE RISCO
CRM	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Acompanhar comercialmente o cliente	Consentimento obrigatório pelo interlocutor	Acesso não autorizado Divulgação Roubo	AS-IS TO-BE
Orçamentação	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Gestão de propostas	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Acompanhar comercialmente o cliente	Consentimento obrigatório pelo interlocutor	Acesso não autorizado Divulgação Roubo	AS-IS TO-BE
Encomendas	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Expedição	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Faturação	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	

Tabela 2 – Risco no módulo de Gestão Comercial & Orçamentação

4.2.3. Gestão da Produção

Relativamente às funcionalidades de Gestão de Produção, os dados são processados com o intuito de garantir quer a rastreabilidade dos registos quer atribuir a produtividade a quem de direito, e caso não existam acessos não autorizados, divulgação não autorizada de dados e roubo de dados, os dados estarão salvaguardados através da licitude que o contrato laboral lhe confere. Assim, o risco de violação de segurança tem uma probabilidade baixa e um impacto insignificante.

No entanto, no caso das funcionalidades provenientes pelo *Kaizen Dashboard* e pelo *Andon Board*, o risco poderá ser superior dependendo do local dos dispositivos e pela maior exposição de dados a que estão sujeitos, e também pela fácil identificação dos colaboradores pela exposição de fotos associada a registo de produção dos mesmos. Assim, o risco poderá ser classificado com uma probabilidade média e um impacto moderado.

SISTRADE MIS | ERP

Módulo: *Gestão de Produção*

FUNCIONALIDADES	DADOS PESSOAIS	OUTPUT	PROCESSAMENTO	JUSTIFICAÇÃO	RISCO	NÍVEL DE RISCO
PLM	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos e registo da produtividade	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Ordens de Fabrico	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos e registo da produtividade	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
SCADA	Nº colaborador Nome Foto	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos e registo da produtividade	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Kaizen Dashboard	Nº colaborador Nome Foto	Mapas	Garantir rastreabilidade dos registos e registo da produtividade	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Andon Board	Nº colaborador Nome Foto	Mapas	Garantir rastreabilidade dos registos e registo da produtividade	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Schedulling	Nº colaborador Nome	Grafico de Gantt, documentos, mapas e relatórios	Garantir rastreabilidade dos registos e registo da produtividade	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	

Tabela 3 – Risco no módulo de Gestão de Produção

4.2.4. Gestão de Stocks & Compras

O tratamento de dados efetuado no módulo de Gestão de Stocks & Compras está relacionado com a criação, encaminhamento e aprovações efetuadas no âmbito do aprovisionamento, gestão de fornecedores e gestão de stocks. Assim, o tratamento efetuado visa a rastreabilidade dos registos e através da licitude conferida pelo contrato de trabalho ao responsável pelo tratamento dos dados (entidade patronal), o maior risco é o acesso não autorizado, a divulgação não autorizada e o roubo de dados. O impacto do tratamento é baixo, pois a probabilidade é baixa e o impacto insignificante.

SISTRADE MIS | ERP

Módulo: *Gestão de Stocks & Compras*

FUNCIONALIDADES	DADOS PESSOAIS	OUTPUT	PROCESSAMENTO	JUSTIFICAÇÃO	RISCO	NÍVEL DE RISCO
Aprovisionamento	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Gestão de Fornecedores	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Gestão de Stocks	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	

Tabela 4 – Risco no módulo de Gestão de Stocks & Compras

4.2.5. Soluções de Gestão WEB

Por fim, no tratamento de dados no módulo de Gestão de Soluções WEB, os dados são processados com o intuito de observar, monitorar ou controlar os colaboradores. A entidade patronal, como responsável pelo tratamento e com a licitude dada pelo contrato laboral,

deverá assegurar que o acesso seja autorizado, a divulgação autorizada e sejam tomadas precauções em relação à proteção dos dados. Aqui a probabilidade de violação de segurança é baixa e o impacto insignificante.

Referência especial para a Gestão de Dados Pessoais onde, apesar de se tentar efetuar uma gestão de dados pessoais, é efetuada uma gestão dos dados empresariais com associação de uma autorização.

SISTRADE MIS | ERP

Módulo: ***Soluções de Gestão WEB***

FUNCIONALIDADES	DADOS PESSOAIS	OUTPUT	PROCESSAMENTO	JUSTIFICAÇÃO	RISCO	NÍVEL DE RISCO
Manutenção de Equipamentos	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Controlo de Qualidade	Nº colaborador Nome	Documentos, mapas e relatórios com referência aos colaboradores	Garantir rastreabilidade dos registos	Licitude concedida pelo contrato de trabalho	Acesso não autorizado Divulgação Roubo	
Gestão de Energia	Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável	
Gestão de Dados Pessoais (AS-IS)	Apenas dados empresariais	Não aplicável	Não aplicável	Não aplicável	Não aplicável	

Tabela 5 – Risco no módulo de Soluções de Gestão WEB

4.2.6. Síntese da avaliação

Resumindo a avaliação de impacto do tratamento de dados pessoais nos diversos módulos e funcionalidades do Sistrade® MIS | ERP, conclui-se que existem várias funcionalidades com impacto insignificante e com uma baixa probabilidade de ocorrência. As funcionalidades com um impacto um pouco superior são o *Kaizen Dashboard* e o *Andon Board* pela maior exposição a que estão sujeitos. O maior impacto é apresentado pela funcionalidade dos Recursos Humanos, onde a base de trabalho são os dados pessoais e os mesmos existem em maior volume. Serão ainda sugeridas algumas alterações nas funcionalidades CRM e Gestão de Propostas do módulo de Gestão Comercial & Orçamentação, pois são funcionalidades onde não estando sistema prevenido para o alojamento de dados pessoais, numa eventual auditoria poderia colocar-se a questão de onde estariam esses dados sujeitos a uma violação de segurança ainda maior. Podemos visualizar a probabilidade e o impacto das várias funcionalidades de todos os módulos do Sistrade® MIS | ERP na matriz de risco seguinte:

		IMPACTO		
		Insignificante	Moderado	Catastrófico
PROBABILIDADE	Alta			
	Média		GP - Kaizen Dashboard, Andon Board	AF - Recursos Humanos GC - CRM "TO BE" GC - Gestão de Propostas "TO BE"
	Baixa	AF - Contabilidade, Tesouraria e Imobilizado GC - Orçamentação, Encomendas, Expedição e Faturação GC - CRM e G. Propostas "AS IS" GP - PLM, Ordens Fabrico, SCADA e Schedulling SC - Aprovisionamento, Fornecedores e Stocks GW - Manutenção, Qualidade e Energia		

Tabela 6 – Matriz de risco do Sistrade® MIS | ERP

Quanto aos cenários de implementação do Sistrade® MIS | ERP, são possíveis dois cenários: a implementação *on premise*, que se caracteriza pela instalação em servidores do próprio cliente, e a implementação *cloud*, que implica acesso por parte do cliente a servidores da própria Sistrade.

Estes dois cenários de implementação trazem preocupações diferentes em relação à proteção de dados. Enquanto na implementação *on premise*, que é o cenário mais comum, responsabiliza mais a empresa cliente, tendo estes o papel de responsável pelo tratamento (*data controller*) e o papel de subcontratante (*data processor*), o cenário cloud responsabiliza a própria Sistrade como subcontratante (*data processor*).

5. Especificação de plataforma

5.1. Mitigação dos riscos de violação

Numa fase de mitigação dos riscos de violação, os processos com maior probabilidade e impactos, e por conseguinte os processos que carecem de análise são os processos de Recursos Humanos no módulo de Gestão Administrativa & Financeira, o CRM e a Gestão de Propostas, com a sugestão de novas funcionalidades na Gestão Comercial, e na Gestão de Produção, as funcionalidades de *Andon Board* e *Kaizen Dashboard*.

Em relação ao processo de Recursos Humanos, são dois os problemas identificados: o acesso aos cadastros e a extração de listagens. A acessibilidade é preocupante visto serem dados bastante sensíveis, no entanto, tendo a empresa licitude para tratar os mesmos, o acesso e tratamento terão de ser limitados. A Gestão de Acessos presente no Sistrade® MIS|ERP permite limitar o acesso, no entanto configurações mal parametrizadas podem sempre ocorrer. Uma solução poderá passar pela implementação deste módulo em servidor separado, efetuando integrações de informação sempre que necessário. Assim, possíveis configurações mal parametrizadas poderão ser mais facilmente detetadas. Para complementar o registo de logs das operações mais sensíveis, com notificação do encarregado pela proteção de dados das operações mais sensíveis. Apresentamos na figura seguinte um modelo de implementação para esta solução.

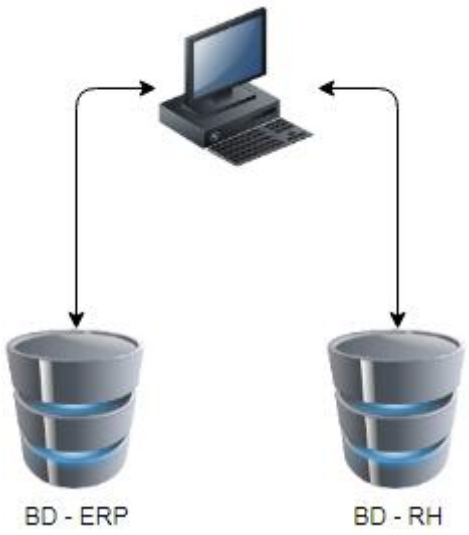


Figura 21 – Modelo de implementação do módulo de Recursos Humanos

Já quanto ao problema da extração de dados, uma possível medida de mitigação do risco poderá ser a colocação de avisos quanto aos riscos de violação de dados no momento da extração desses dados (ver modelo na figura 22), bem como de notificações desta ação

enviadas por e-mail para o encarregado da proteção de dados ou caso não exista, administrador de sistemas da empresa, conforme sugestão na figura 23.

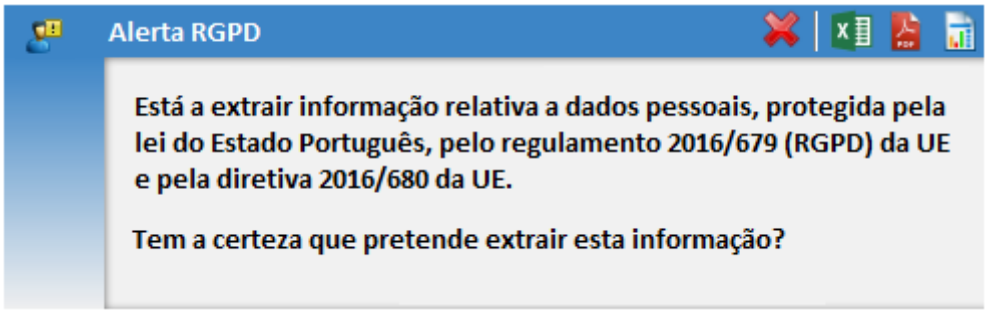


Figura 22 – Modelo de alerta na extração de dados

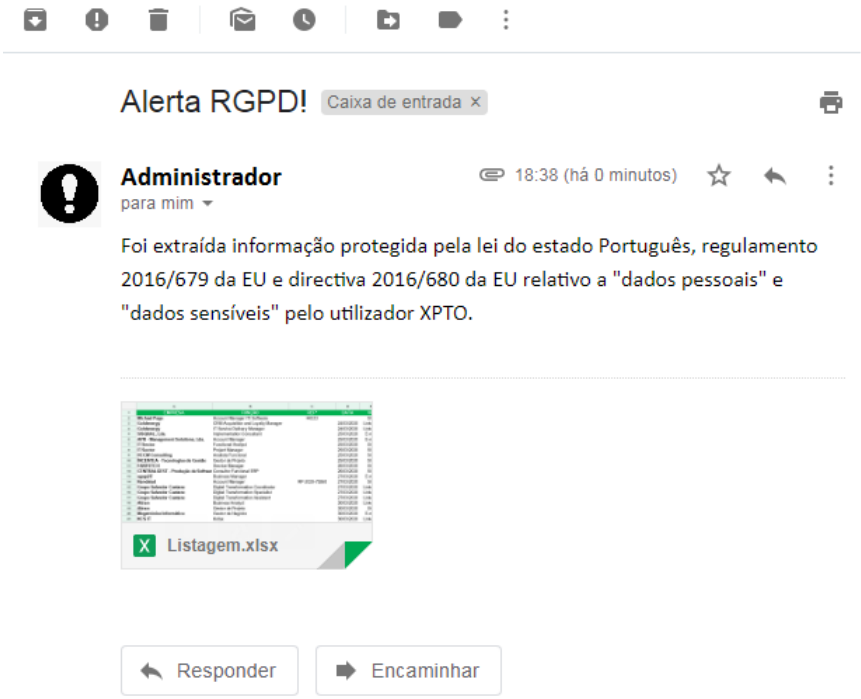


Figura 23 – Modelo de e-mail de notificação ao Encarregado de Proteção de Dados

Relativamente à Gestão Comercial nas suas funcionalidades de CRM e Gestão de Propostas, a solução para mitigar o risco de violação de dados passa pela implementação de um suporte para os interlocutores, registando o mesmo de acordo com as normas em vigor do RGPD. Assim, à manutenção de terceiros poderia ser acrescentado um separador denominado "Interlocutores", com capacidade para registar os diferentes interlocutores dos diversos parceiros de negócio e dos diversos contactos. Especial cuidado deverá ser colocado na especificação do ciclo de vida destes registos, de forma a que a minimização seja aplicável.

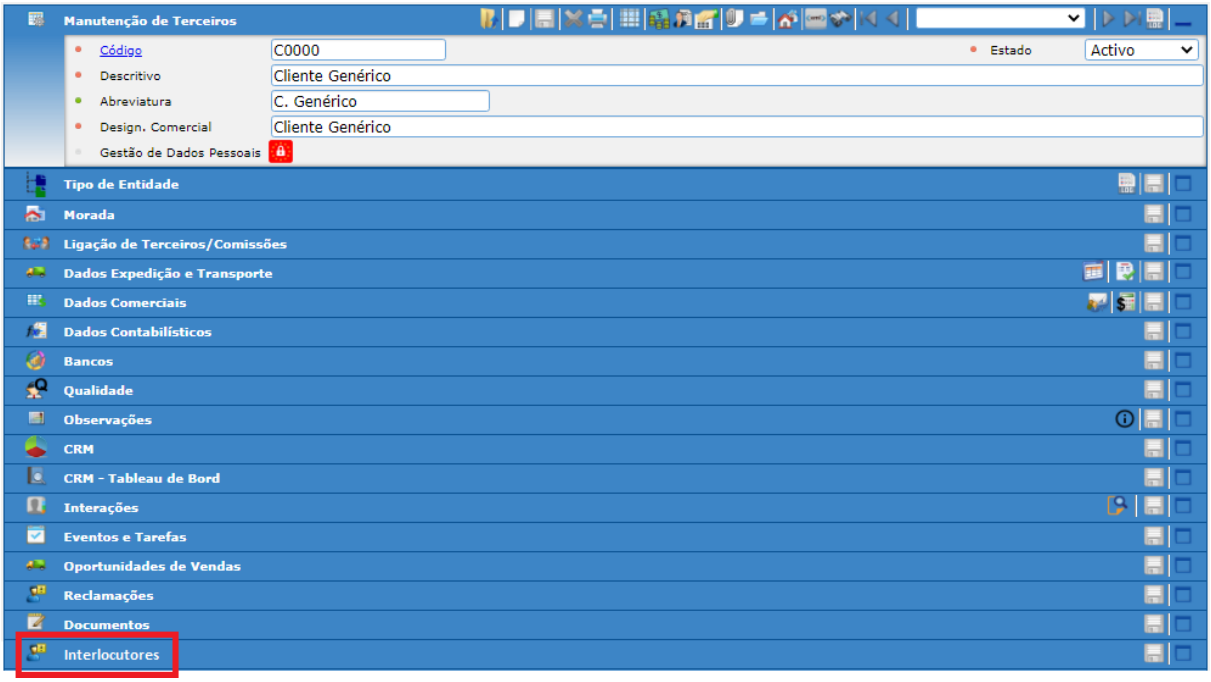


Figura 24 – Sugestão de secção de interlocutores na Manutenção de terceiros

Neste separador de "Interlocutores" poderiam ser registados alguns dados relativos aos diversos interlocutores, efetuando ainda a ligação ao módulo de Gestão de Dados Pessoais que atualmente está ligado ao próprio terceiro, no conceito Sistrade® MIS|ERP: empresa.

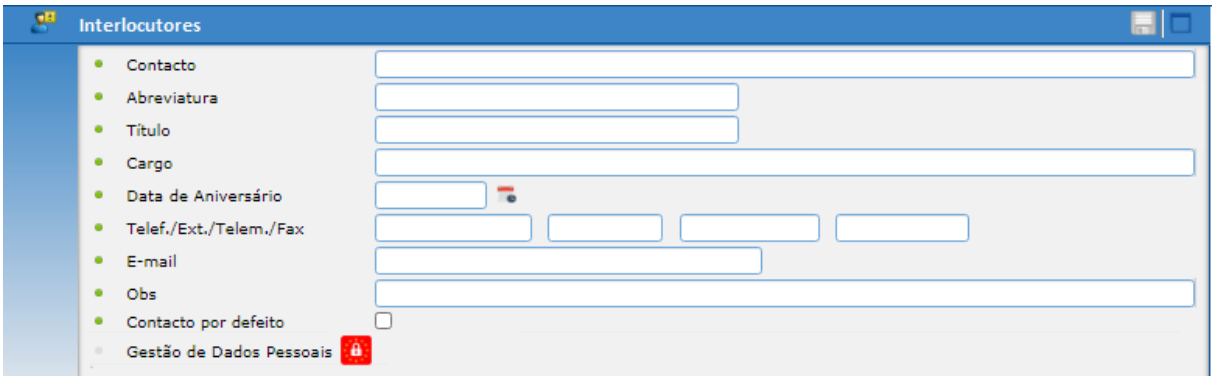


Figura 25 – Sugestão de registo de interlocutores

Assim, na Gestão de Dados Pessoais poderia ser efetuado o registo de algumas informações que conforme o artigo 13º do RGPD é obrigatório facultar quando os dados pessoais são recolhidos junto do titular.

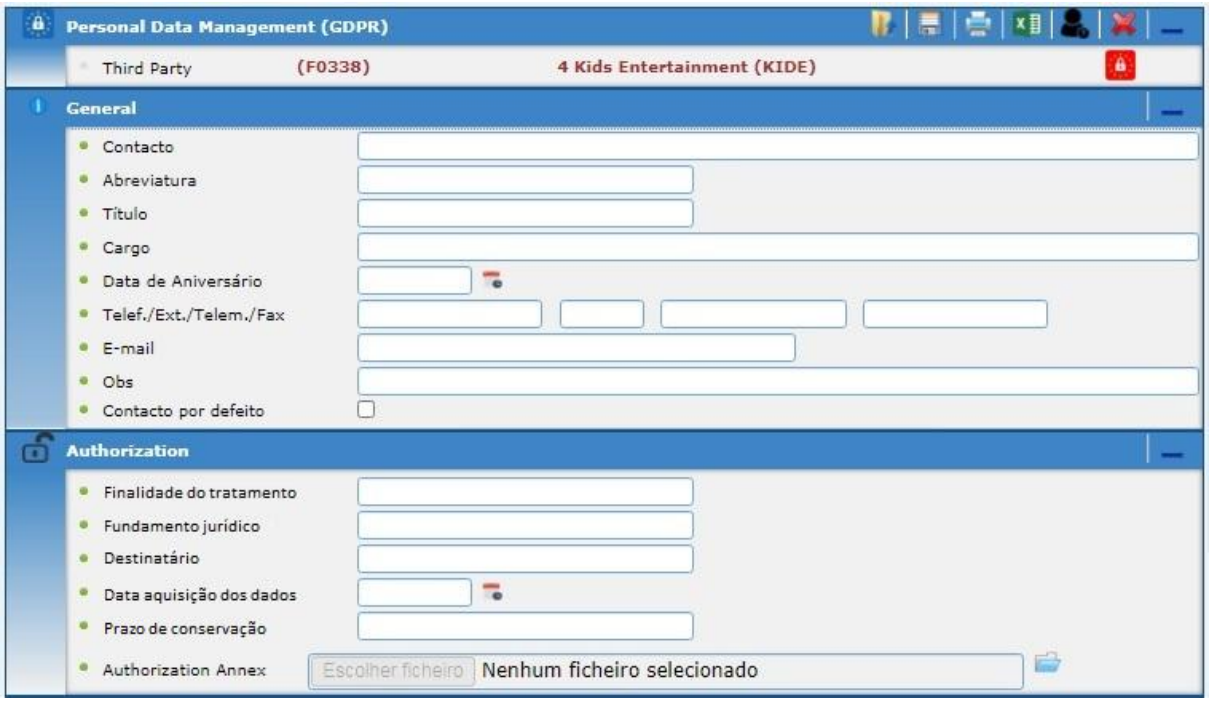


Figura 26 – Sugestão de Gestão de Dados Pessoais

Com o desenvolvimento desta Gestão de Dados Pessoais, e estando integrado com a funcionalidade Interlocutores, poderia ser desenvolvido e aproveitado noutros âmbitos do Sistrade® MIS|ERP, nomeadamente identificar interlocutores em outras funcionalidades como por exemplo: encomendas, gestão de propostas, expedição, faturação, compras e gestão de fornecedores.

A aquisição de dados pessoais deverá ser efetuada aquando do pedido de contacto via site, tendo o titular de dados de autorizar o consentimento. Essa autorização é solicitada através de e-mail, conforme a sugestão apresentada a seguir.

Consentimento RGPD

Administrador <privacidade@xpto.pt>
para Jose

Caro(a) **Prospect**,

O Regulamento Geral de Protecção de Dados é aplicável desde 25 de Maio de 2018.
Este diploma vem, entre outros objectivos, reforçar os direitos dos titulares dos dados.

Solicitamos assim que nos dê o seu consentimento através do link, para podermos contactá-lo para efeitos de marketing.

Informação nos termos do artigo 13º do Regulamento Geral de Protecção de Dados:

1. Identificação e contactos do responsável - **XPTO, S.A, contacto: privacidade@xpto.pt. Telefone: 222 333 444**
2. Finalidades do tratamento - contacto para efeitos de marketing
3. Fundamento jurídico para o tratamento - consentimento
4. Destinatários ou categorias de destinatários – Departamento Comercial e Marketing
5. Transferência de dados para fora do Espaço Económico Europeu – Não há
6. Prazo de conservação dos dados – 3 anos após o último contacto
7. A comunicação de dados - Não há obrigação legal de nos fornecer os seus dados pessoais
8. Decisões Automatizadas – Não há.

Caso pretenda ler a nossa política de privacidade na integra poderás fazê-lo em https://www.xpto.pt/privacidade.pdf.

Cumprimentos,
XPTO

Figura 27 – Sugestão de consentimento

Por forma a mitigar os riscos de violação no módulo de Gestão de Produção, quer na funcionalidade de *Andon Board*, quer na funcionalidade de *Kaizen Dashboard*, apresentamos dois modelos: ou o consentimento dos colaboradores para apresentação dos seus dados de produção, ou então efetuar a identificação da máquina ou da linha de produção em vez de efetuar referência ao colaborador.

No primeiro modelo, apresentamos uma minuta de consentimento da utilização dos dados pessoais dos colaboradores, assim como os dados de produção dos mesmos, para apresentação nos locais autorizados. Apresentamos também uma sugestão de cláusula para os contratos de trabalho dos colaboradores em causa. Ambos os documentos sugeridos podem ser consultados no anexo D.

No segundo modelo apresentamos algumas sugestões de alteração do ecrã (ver figura 28), onde se substitui o nome e foto dos colaboradores pelo nome da linha de produção e uma imagem identificativa da mesma.

Figura 28 – Sugestão de apresentação de *Andon Board*

Assim, consegue-se a pseudonimização, onde o tratamento de dados pessoais é efetuado de forma que impossibilita a atribuição a um titular de dados específico sem recorrer a informações suplementares. As informações suplementares devem ser mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Em relação aos cenários de implementação, uma possível medida de mitigação dos riscos de violação seria a implementação pela Sistrade de certificação em sistema de gestão da segurança da informação (ISO 27001) no caso do cenário *cloud* garantindo assim que todas as implementações nos seus servidores cumpram normas de segurança. Já no cenário *on premise* a responsabilidade é da própria empresa cliente, no entanto disponibilizar esse *know how* e dar apoio na segurança da informação ao cliente seria uma alternativa para ajudar no cumprimento do RGPD.

5.2. Especificação do processo de auditoria interna

Reduzido o risco através de novos processos e funcionalidades no Sistrade® MIS|ERP, é necessário especificar um processo de auditoria interna que ateste a conformidade do sistema com o RGPD. Assim, apresentamos algumas questões organizadas em 3 áreas que poderiam ser implementadas como um questionário dentro do Sistrade® MIS|ERP (ver anexo E). Essas

áreas seriam: gestão, consentimentos e base de dados.

Na área da gestão as questões estão relacionadas com o regulamento interno, a política de privacidade da organização, a avaliação das recolhas de dados, a necessidade de nomear um Encarregado de Proteção de Dados, e a avaliação da necessidade de formação aos colaboradores. Deve ser aferido se a organização tem a documentação que prova a conformidade com o RGPD, nomeadamente em relação ao seu regulamento interno e sua divulgação, e aos consentimentos necessários.

No que diz respeito aos consentimentos, as principais questões são em relação à avaliação dos mesmos na base de dados atual, à gestão dos mesmos por parte do titular dos dados, nomeadamente de uma forma granular e ao consentimento por "*opt in*".

Quanto às bases de dados, as principais preocupações estão relacionadas com a encriptação da mesma e conforme o regulamento, "*Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco [...]*" (Parlamento Europeu, 2016), a partilha de bases de dados com terceiros, e a fuga de informação.

O processo de auditoria ajuda a alertar e a clarificar alguns pontos importantes para atingir a conformidade perante o Regulamento Geral da Proteção de Dados.

5.3. Modelos de relatórios

Na secção "Mitigação dos riscos de violação" foram já apresentados alguns modelos de documentos que ajudam a minimizar o risco e a aumentar o cumprimento do Regulamento Geral de Proteção de Dados, como por exemplo o consentimento de uso de imagem, a cláusula para o contrato de trabalho, o alerta de extração de dados (quer para o utilizador, quer para um encarregado de proteção de dados), assim como e-mail de solicitação de consentimento.

No seguimento de um processo de auditoria e por forma a verificar o devido cumprimento do RGPD podem ser criados *dashboards* retirando alguma informação de gestão para o encarregado de proteção de dados. Assim, podem ser criados por exemplo *dashboards* de formação dada aos colaboradores sobre proteção de dados, bem como sobre o devido consentimento dos contactos presentes na base de dados da empresa.

Figura 29 – Modelo de dashboard

6. Conclusões e perspetivas de desenvolvimento

Concluído o trabalho deste projeto de dissertação é possível retirar várias conclusões e reflexões.

Inicialmente permitiu o contacto com um ERP, analisando os diferentes módulos do mesmo, identificando os processos e mapeando os tratamentos dos dados pessoais efetuado. De seguida, permitiu realizar uma avaliação do impacto dos tratamentos efetuados. Tal avaliação permitiu chegar a algumas conclusões sobre como mitigar o risco de violação de dados, ajudando a chegar à conformidade com o RGPD através de um *roadmap* de desenvolvimentos.

Podemos dividir esse *roadmap* de desenvolvimentos em três fases: vitórias rápidas (desenvolvimento fáceis e rápidos de implementar), melhorias mandatórias (desenvolvimentos importantes a efetuar) e melhorias de longo prazo (desenvolvimentos a longo prazo). Como vitórias rápidas temos o caso dos consentimentos dos colaboradores em relação ao *Andon Board* e ao painel de controlo *Kaizen*. Já em termos de melhorias mandatórias temos a implementação do servidor de RH em separado e as alterações das apresentações em *Andon Board* e painel de controlo *Kaizen*. Em relação a melhorias de longo prazo temos as alterações às funções de CRM e de Gestão de Propostas.

Quanto a perspectivas de futuro seria a implementação do *roadmap* de desenvolvimento sugerido, sempre acompanhado por alguém com formação específica da área, podendo ser ainda desenvolvido trabalho em relação à segurança da informação e efetuar uma análise às condições de segurança da infraestrutura que suporta todo o sistema, analisando as diferenças das soluções caso seja adotado nas instalações ou na nuvem.

Em resumo, os objetivos propostos inicialmente foram alcançados, ajudando as organizações que adotarem o software Sistrade® MIS | ERP a ficar em conformidade com o Regulamento Geral de Proteção de Dados.

De referir que a conformidade com o referido regulamento não depende só de qualquer sistema, nem da sua utilização, devendo ser uma missão de todos os colaboradores de uma empresa, e assumir que os ataques têm uma incidência inicial através de técnicas de engenharia social, passando para controlos do utilizador final, pela proteção do servidor e finalizando ao nível aplicacional.

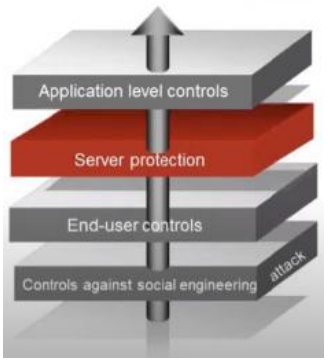


Figura 30 – Incidência de ataques

Referências bibliográficas

Adams, A., & Sasse, M. A. (1999). User are not the enemy. Communications of the ACM, 42(12).

Ashenden, D. (2008). Information Security management: A human challenge? Information Security Technical Report, 13(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Bell, D. (1980). The Social Framework of the Information Society. The Microelectronics Revolution: The Complete Guide to the New Technology and Its Impact on Society.

Chen, D. (2012). Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering, 1(973), 647–651. https://doi.org/10.1109/ICCSEE.2012.193

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11, 127–153.

Freitas, C., & Mira, M. (2018). RGPD nas PME GDPR in SMEs. 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), 1–6. https://doi.org/10.23919/CISTI.2018.8399272

Hintze, M. (2019). Privacy Statements Under the GDPR. Seattle University Law Review, 42, 1129–1154.

Hungarian National Strategy of Informatics (1995). Governamental Informatics Strategy discussion document

International Organization for Standardization. (2018). ISO 27005: Information Security Risk Management.

Jd, E. H. F., & Freeman, E. H. (2007). Holistic Information Security : ISO 27001 and Due Holistic Information Security : ISO 27001 and Due Care. https://doi.org/10.1080/10658980701746478

Karvalics, L. Z. (2007). Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression). From theory to political practice, 29

Mason, R. O. (1986). Four Ethical Issues of the Information Age. MIS Quarterly,

10(March). https://doi.org/10.2307/248873

Masuda, Y. (1980*).* The Information Society and Post-Industrial Society*. Washington*: World Future Society. pp. vii–viii, 31–33

Mendes, Pedro (2018). Análise de Risco no GDPR. Dissertação de Mestrado, Faculdade de Ciências, Universidade de Lisboa. https://repositorio.ul.pt/bitstream/10451/35494/1/ulfc124806_tm_Pedro_Mendes.pdf

Moore, Nick (1998). The information society. In: World Information Report (UNESCO Reference Books, Bernan Assoc, Geneva).

Naisbitt, J. (1985). Reinventing the Corporation: Transforming Your Job and Your Company for the New Information Society. Warner Books.

Nascimento, T. (2019). Portal do DPO - Encarregado de Protecção de Dados. Retrieved from https://www.portaldodpo.pt/

Papanikas, D., Ntouskas, T., & Polemi, D. (2012). Trusted collaborative services for the IT security management of SMEs/mEs. International Journal of Electronic Security and Digital Forensics, 4. https://doi.org/10.1504/IJESDF.2012.048413

Parlamento Europeu. "Regulamento 2016/679 de 27 de Abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) L119". Jornal Oficial das Comunidades Europeias, (2016):1-88. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

Reinsel, D., Gantz, J., & Rydning, J. (2018). The Digitization of the World: From Edge to Core, IDC White Paper (November).

Tankard, C., & Pathways, D. (2016). What the GDPR means for. Network Security, 2016(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Vijayan, J. (2019). 25 data security stats that matter. Retrieved from https://techbeacon-com.cdn.ampproject.org/c/s/techbeacon.com/security/25-data-security-stats-matter

Y. Barlette and V. V. Fomin (2008). Exploring the Suitability of IS Security Management Standards for SMEs, Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, pp. 308-308

Anexos

Anexo A – Mapeamento dos tratamentos de dados

Formulário modelo

SISTRADE MIS | ERP			
Módulo:			
Funcionalidade:			
DADOS PESSOAIS:			
INPUT:			
PROCESSAMENTO:			
INTERVENIENTES:			
OUTPUT:			
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?		
	Processamento automatizado de dados com consequências legais?		
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?		
	Processamento de dados sensíveis?		
	Processamento de dados em grande escala?		
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?		
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?		
	Processamento de dados através de uso de novas tecnologias?		
	Transferência de dados para fora da União Europeia?		
	Processamento de dados que possa impedir indivíduos de exercer direitos?		
	Processamento de novos tipos de dados pessoais?		
	Novos tipos de processamento de dados?		
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?		
	Recolha de dados excessiva?		
	Acesso não autorizado aos dados?		
	Destruição ou alteração acidental/ilegal de dados?		
	Divulgação não autorizada de dados?		
	Roubo de dados?		
	Uso/armazenamento de dados desatualizados?		
	Utilização dos dados para além do que é expectável?		
	Utilização dos dados para além do que é socialmente aceitável?		
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?		

Figura 31 – Formulário modelo para mapeamento de dados

Recolha de dados – Administrativa & Financeira / Contabilidade

	SISTRADE MIS | ERP **Módulo:** *Administrativa & Financeiro* **Funcionalidade:** *Contabilidade*		
DADOS PESSOAIS:	Identificação do colaborador através do seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Registo das transações efetuadas pelo colaborador (registo de faturas de clientes e de fornecedores, contas correntes, etc.)		
INTERVENIENTES:	Técnico Administrativo e Financeiro, Diretor Financeiro		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 32 – Recolha do mapeamento de dados – Administrativa & Financeira / Contabilidade

Recolha de dados – Administrativa & Financeira / Tesouraria

	SISTRADE MIS | ERP **Módulo:** *Administrativa & Financeiro* **Funcionalidade:** *Tesouraria*		
DADOS PESSOAIS:	Identificação do colaborador através do seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Registo das transações efetuadas pelo colaborador (recebimentos, pagamentos, etc.)		
INTERVENIENTES:	Técnico Administrativo e Financeiro, Diretor Financeiro		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 33 – Recolha do mapeamento de dados – Administrativa & Financeira / Tesouraria

Recolha de dados – Administrativa & Financeira / Imobilizado

SISTRADE MIS | ERP			
Módulo:	***Administrativa & Financeiro***		
Funcionalidade:	***Imobilizado***		
DADOS PESSOAIS:	Identificação do colaborador através do seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Registo das transações efetuadas pelo colaborador (registo do imobilizado, depreciações, alienações, abates, reparações, etc.)		
INTERVENIENTES:	Técnico Administrativo e Financeiro, Diretor Financeiro		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 34 – Recolha do mapeamento de dados – Administrativa & Financeira / Imobilizado

Recolha de dados – Administrativa & Financeira / Recursos Humanos

	SISTRADE MIS | ERP **Módulo:** ***Administrativa & Financeiro*** **Funcionalidade:** ***Recursos Humanos***		
DADOS PESSOAIS:	Identificação do colaborador através do seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Registo do cadastro do colaborador, Gestão de horarios e faltas, Processamento de salários, Gestão de formação, Gestão de Segurança, Higiene e Saúde no trabalho, etc.		
INTERVENIENTES:	Técnico Recursos Humanos, Diretor Recursos Humanos		
OUTPUT:	Documentos, mapas e relatórios com dados dos colaboradores.		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Sim	Licitude pelo CT
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Sim	Licitude pelo CT
	Processamento de dados em grande escala?	Sim	Licitude pelo CT
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Média
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Média
	Roubo de dados?	Sim	Média
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 35 – Recolha do mapeamento de dados – Administrativa & Financeira / Recursos Humanos

Recolha de dados – Gestão Comercial & Orçamentação / CRM

	SISTRADE MIS | ERP		
	Módulo:	***Gestão Comercial & Orçamentação***	
	Funcionalidade:	***CRM***	
DADOS PESSOAIS:	Identificação do colaborador através do seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Registo do cadastro da empresa, sem referência a interlocutores. Registo dos dados pessoais do colaborador que criou ou encaminhou o processo.		
INTERVENIENTES:	Técnico Marketing & Vendas, Diretor Comercial		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 36 – Recolha do mapeamento de dados – Gestão Comercial & Orçamentação / CRM

Recolha de dados – Gestão Comercial & Orçamentação / Orçamentação

SISTRADE MIS | ERP			
Módulo:	***Gestão Comercial & Orçamentação***		
Funcionalidade:	***CRM***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Registo do pedido de orçamento, elaboração do orçamento, com aprovação técnica e financeira		
INTERVENIENTES:	Técnico Vendas, Diretor Produção e Diretor Comercial		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 37 – Recolha do mapeamento de dados – Gestão Comercial & Orçamentação / Orçamentação

Recolha de dados – Gestão Comercial & Orçamentação / Gestão de Propostas

	SISTRADE MIS | ERP **Módulo:** ***Gestão Comercial & Orçamentação*** **Funcionalidade:** ***Gestão de Propostas***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Gestão dos Orçamentos e encaminhamento para Ordem de Produção. Nota: Onde estão os dados dos interlocutores do cliente / prospect?		
INTERVENIENTES:	Técnico Vendas		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 38 – Recolha do mapeamento de dados – Gestão Comercial & Orçamentação / Gestão de Propostas

Recolha de dados – Gestão Comercial & Orçamentação / Encomendas

	SISTRADE MIS | ERP **Módulo:** *Gestão Comercial & Orçamentação* **Funcionalidade:** *Encomendas*		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Gestão do estado das encomendas, desde a adjudicação do orçamento, passando para a produção como pendente até aprovado para produção. Controlo o limite de crédito do cliente.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 39 – Recolha do mapeamento de dados – Gestão Comercial & Orçamentação / Encomendas

Recolha de dados – Gestão Comercial & Orçamentação / Expedição

SISTRADE MIS | ERP			
Módulo:	***Gestão Comercial & Orçamentação***		
Funcionalidade:	***Expedição***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Transferência do produto para o cliente final. Criação de Guias de Remessa e Guias de Transporte para oficializar transferência.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 40 – Recolha do mapeamento de dados – Gestão Comercial & Orçamentação / Expedição

Recolha de dados – Gestão Comercial & Orçamentação / Faturação

	SISTRADE MIS | ERP		
	Módulo:	***Gestão Comercial & Orçamentação***	
	Funcionalidade:	***Faturação***	
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Emitir faturas, notas de débito, notas de crédito, etc. Possibilidade de agregação de faturas e de faturação eletrónica.		
INTERVENIENTES:	Técnico Administrativo e Financeiro, Diretor Financeiro		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 41 – Recolha do mapeamento de dados – Gestão Comercial & Orçamentação / Faturação

Recolha de dados – Gestão de Produção / PLM

SISTRADE MIS | ERP			
Módulo:	***Gestão de Produção***		
Funcionalidade:	***PLM***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Gestão do ciclo de vida do produto (conceção, fabricação e final de vida). Associação do produto em árvore, controlo de versões, números de séries, testes e ensaios.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 42 – Recolha do mapeamento de dados – Gestão de Produção / PLM

Recolha de dados – Gestão de Produção / Ordens de Fabrico

SISTRADE MIS | ERP	
Módulo:	***Gestão de Produção***
Funcionalidade:	***Ordens de Fabrico***

DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema e consola de recolha de dados em chão de fábrica		
PROCESSAMENTO:	Diretor de Produção recebe as encomendas, bem como outras necessidades de produção, e encaminha para o chão de fábrica aquilo que se deve produzir. Operadores registam tempos de produção na consola de recolha de dados.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 43 – Recolha do mapeamento de dados – Gestão de Produção / Ordens de Fabrico

Recolha de dados – Gestão de Produção / SCADA

SISTRADE MIS | ERP			
Módulo:	***Gestão de Produção***		
Funcionalidade:	***SCADA***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema e consola de recolha de dados em chão de fábrica		
PROCESSAMENTO:	Monitorização em tempo real do processo produtivo. Identificação dos colaboradores que operam nas máquinas e as respectivas ordens de fabrico.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 44 – Recolha do mapeamento de dados – Gestão de Produção / SCADA

Recolha de dados – Gestão de Produção / Kaizen Dashboard

SISTRADE MIS | ERP

Módulo: *Gestão de Produção*
Funcionalidade: *Kaizen Dashboard*

DADOS PESSOAIS:	Identificação do colaborador pelo seu número, nome e foto		
INPUT:	Diversos dados disponíveis no sistema		
PROCESSAMENTO:	Manipulação dos dados recolhidos anteriormente no sistema. Apresentação desses dados conforme as necessidades.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Média
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Média
	Roubo de dados?	Sim	Média
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 45 – Recolha do mapeamento de dados – Gestão de Produção / Kaizen Dashboard

Recolha de dados – Gestão de Produção / Andon Board

SISTRADE MIS | ERP			
Módulo:	***Gestão de Produção***		
Funcionalidade:	***Andon Board***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número, nome e foto		
INPUT:	Diversos dados disponíveis no sistema		
PROCESSAMENTO:	Apresentação dos dados do sistema relativo a produção. Diversas visualizações: por turnos, por máquina, por colaborador, comparativos, etc.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Média
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Média
	Roubo de dados?	Sim	Média
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 46 – Recolha do mapeamento de dados – Gestão de Produção / Andon Board

Recolha de dados – Gestão de Produção / Schedulling

SISTRADE MIS | ERP			
Módulo:	***Gestão de Produção***		
Funcionalidade:	***Schedulling***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número, nome e foto		
INPUT:	Diversos dados disponíveis no sistema		
PROCESSAMENTO:	Sequenciação das diversas tarefas associadas às ordens de fabrico aprovadas.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Gráfico de Gantt com planeamento referindo os colaboradores alocados às diversas tarefas. Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 47 – Recolha do mapeamento de dados – Gestão de Produção / Schedulling

Recolha de dados – Gestão de Stocks & Compras / Aprovisionamento

	SISTRADE MIS | ERP **Módulo:** *Gestão de Stocks & Compras* **Funcionalidade:** *Aprovisionamento*		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Análise das necessidades de material, com sugestão das compras a efetuar. Identificados os colaboradores que sugeriram as compras a efetuar, bem como quem aprovou a compra.		
INTERVENIENTES:	Diretor de Produção e Diretor de Compras		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 48 – Recolha do mapeamento de dados – Gestão de Stocks & Compras / Aprovisionamento

Recolha de dados – Gestão de Stocks & Compras / Gestão de Fornecedores

	SISTRADE MIS | ERP		
	Módulo:	***Gestão de Stocks & Compras***	
	Funcionalidade:	***Gestão de Fornecedores***	
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Análise dos diversos fornecedores para melhor suprir as necessidades de compras.		
INTERVENIENTES:	Diretor de Produção e Diretor de Compras		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 49 – Recolha do mapeamento de dados – Gestão de Stocks & Compras / Gestão de Fornecedores

Recolha de dados – Gestão de Stocks & Compras / Gestão de Stocks

SISTRADE MIS | ERP

Módulo: *Gestão de Stocks & Compras*
Funcionalidade: *Gestão de Stocks*

DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Monitorização de todo o inventário da empresa. Registo de diversas ações relativas ao material: entrada de matéria prima em armazém, saída para produção, entrada em armazém de produto acabado, saída do produto acabado para expedição, etc.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 50 – Recolha do mapeamento de dados – Gestão de Stocks & Compras / Gestão de Stocks

Recolha de dados – Soluções de Gestão WEB / Manutenção

SISTRADE MIS | ERP			
Módulo:	***Soluções de Gestão WEB***		
Funcionalidade:	***Manutenção***		
DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Monitorização de todo os ativos da empresa. Registo do plano de manutenção preventiva e das manutenções correctivas. Registo do responsável por efetuar a manutenção e do material necessário.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 51 – Recolha do mapeamento de dados – Soluções de Gestão WEB / Manutenção

Recolha de dados – Soluções de Gestão WEB / Controlo de Qualidade

SISTRADE MIS | ERP

Módulo: *Soluções de Gestão WEB*
Funcionalidade: *Controlo de Qualidade*

DADOS PESSOAIS:	Identificação do colaborador pelo seu número e nome		
INPUT:	Através do login no sistema		
PROCESSAMENTO:	Monitorização da qualidade do processo produtivo. Registo de medições efetuadas aos produtos durante o processo produtivo. Identificação do colaborador que regista as medições.		
INTERVENIENTES:	Diretor de Produção e colaboradores do Dep. de Produção		
OUTPUT:	Documentos, mapas e relatórios com referência aos colaboradores que intervieram no processo		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Sim	Licitude pelo CT
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Sim	Baixa
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Sim	Baixa
	Roubo de dados?	Sim	Baixa
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 52 – Recolha do mapeamento de dados – Soluções de Gestão WEB / Controlo de Qualidade

Recolha de dados – Soluções de Gestão WEB / Gestão de Energia

	SISTRADE MIS | ERP **Módulo:** *Soluções de Gestão WEB* **Funcionalidade:** *Gestão de Energia*		
DADOS PESSOAIS:	Não aplicável		
INPUT:	Não aplicável		
PROCESSAMENTO:	Monitorização do consumo energético através de analisadores de energia.		
INTERVENIENTES:	Não aplicável		
OUTPUT:	Documentos, mapas e relatórios dos consumos efetuados.		
TRATAMENTO:		**Sim / Não**	**Observações**
	Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)?	Não	
	Processamento automatizado de dados com consequências legais?	Não	
	Processamento de dados utilizados para observar, monitorar ou controlar indivíduos?	Não	
	Processamento de dados sensíveis?	Não	
	Processamento de dados em grande escala?	Não	
	Processamento sobre conjunto de dados provenientes de diferentes fontes ou com diferentes propósitos?	Não	
	Processamento de dados de indivíduos considerados vulneráveis (crianças, idosos, etc.)?	Não	
	Processamento de dados através de uso de novas tecnologias?	Não	
	Transferência de dados para fora da União Europeia?	Não	
	Processamento de dados que possa impedir indivíduos de exercer direitos?	Não	
	Processamento de novos tipos de dados pessoais?	Não	
	Novos tipos de processamento de dados?	Não	
RISCOS:		**Sim / Não**	**Probabilidade**
	Recolha de dados não justificada?	Não	
	Recolha de dados excessiva?	Não	
	Acesso não autorizado aos dados?	Não	
	Destruição ou alteração acidental/ilegal de dados?	Não	
	Divulgação não autorizada de dados?	Não	
	Roubo de dados?	Não	
	Uso/armazenamento de dados desatualizados?	Não	
	Utilização dos dados para além do que é expectável?	Não	
	Utilização dos dados para além do que é socialmente aceitável?	Não	
	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar?	Não	

Figura 53 – Recolha do mapeamento de dados – Soluções de Gestão WEB / Gestão de Energia

Anexo B – Processos

Administrativa & Financeira

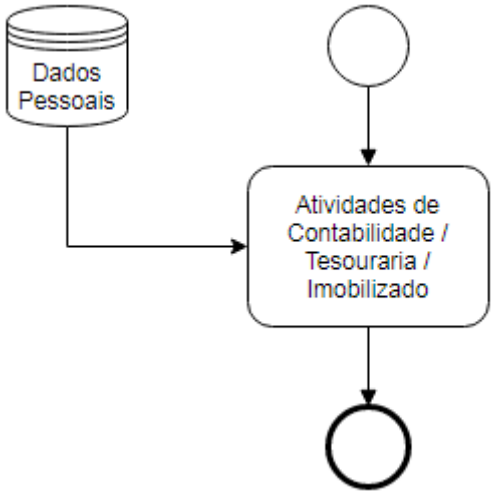


Figura 54 – Processo contabilístico, tesouraria e imobilizado

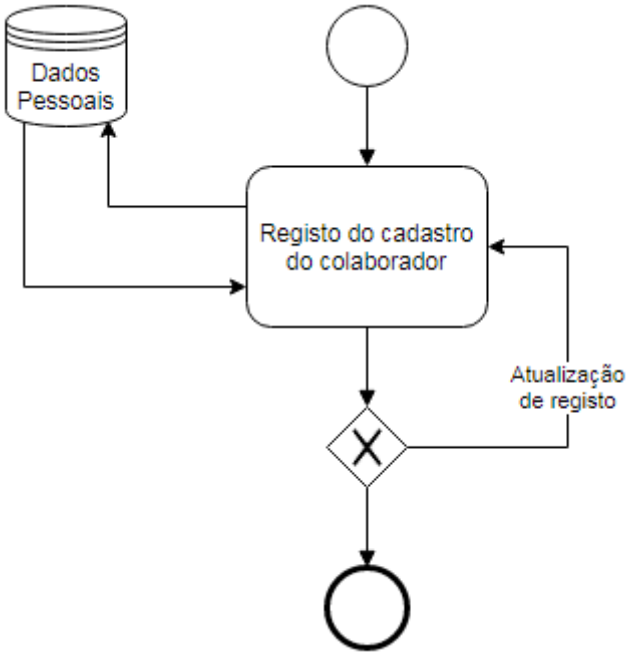


Figura 55 – Processo Recursos Humanos: cadastro do colaborador

Gestão Comercial & Orçamentação

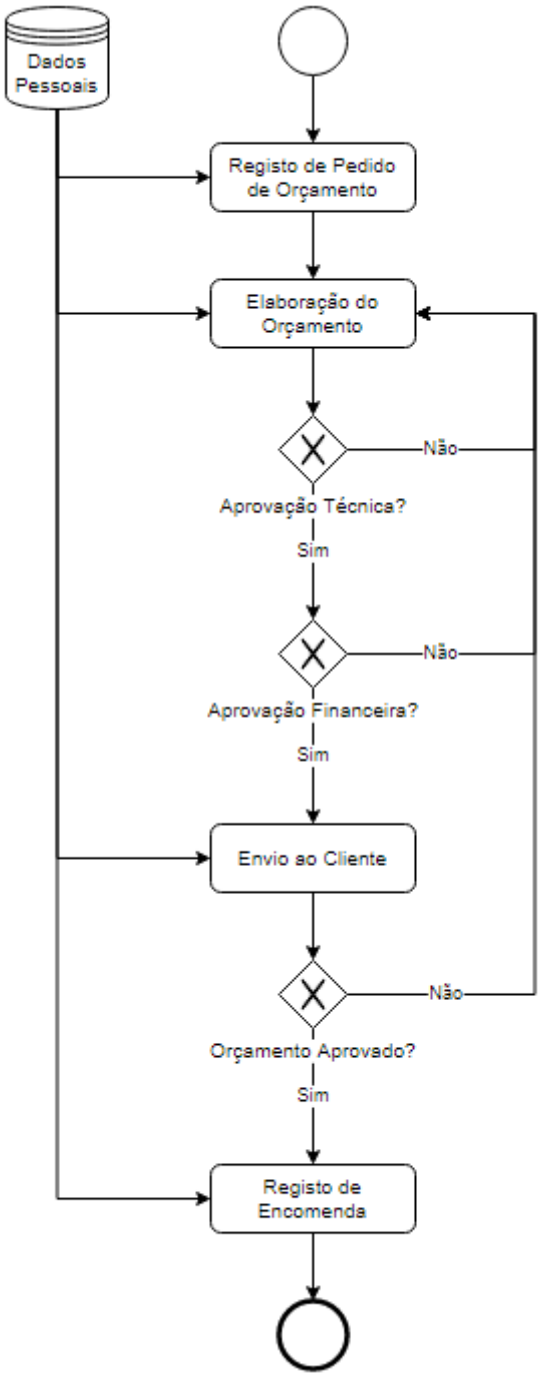


Figura 56 – Processo Comercial & Orçamentação

Gestão da Produção

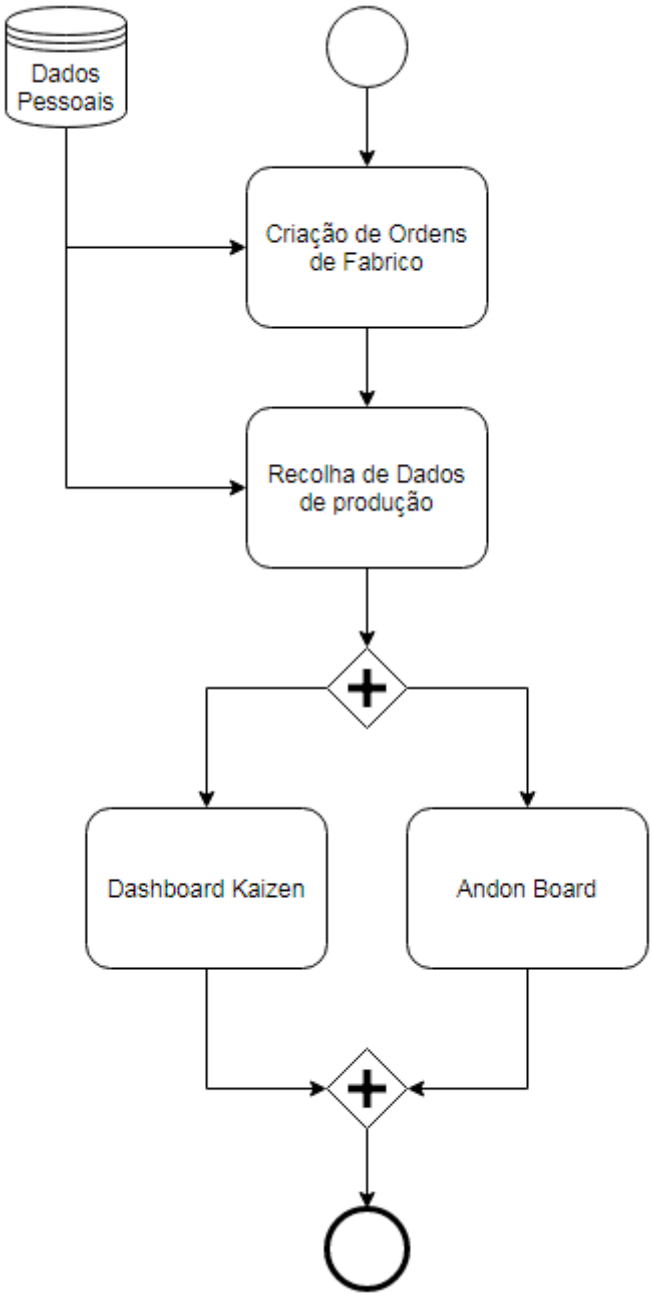


Figura 57 – Processo Produção

Gestão de Stocks & Compras

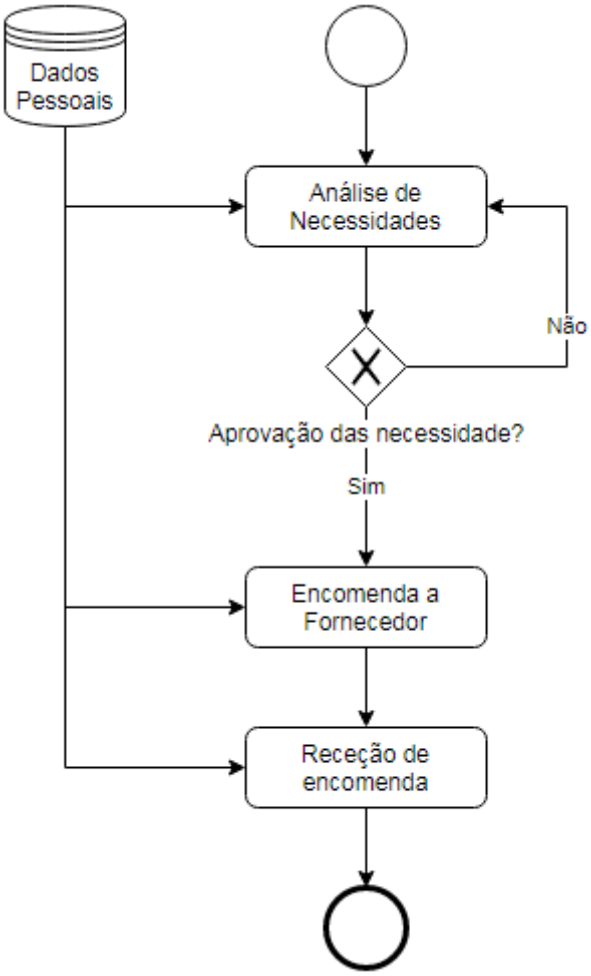


Figura 58 – Processo Stocks & Compras

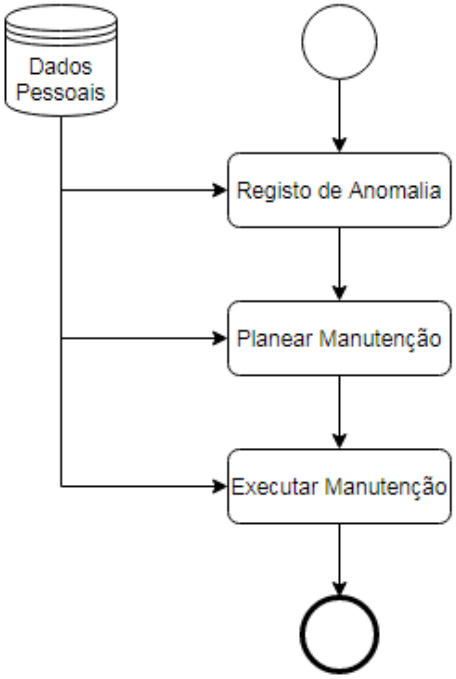


Figura 59 – Processo de manutenção de equipamentos

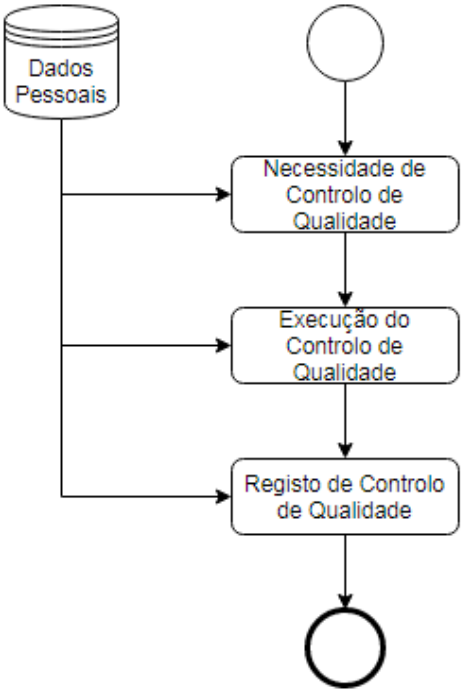
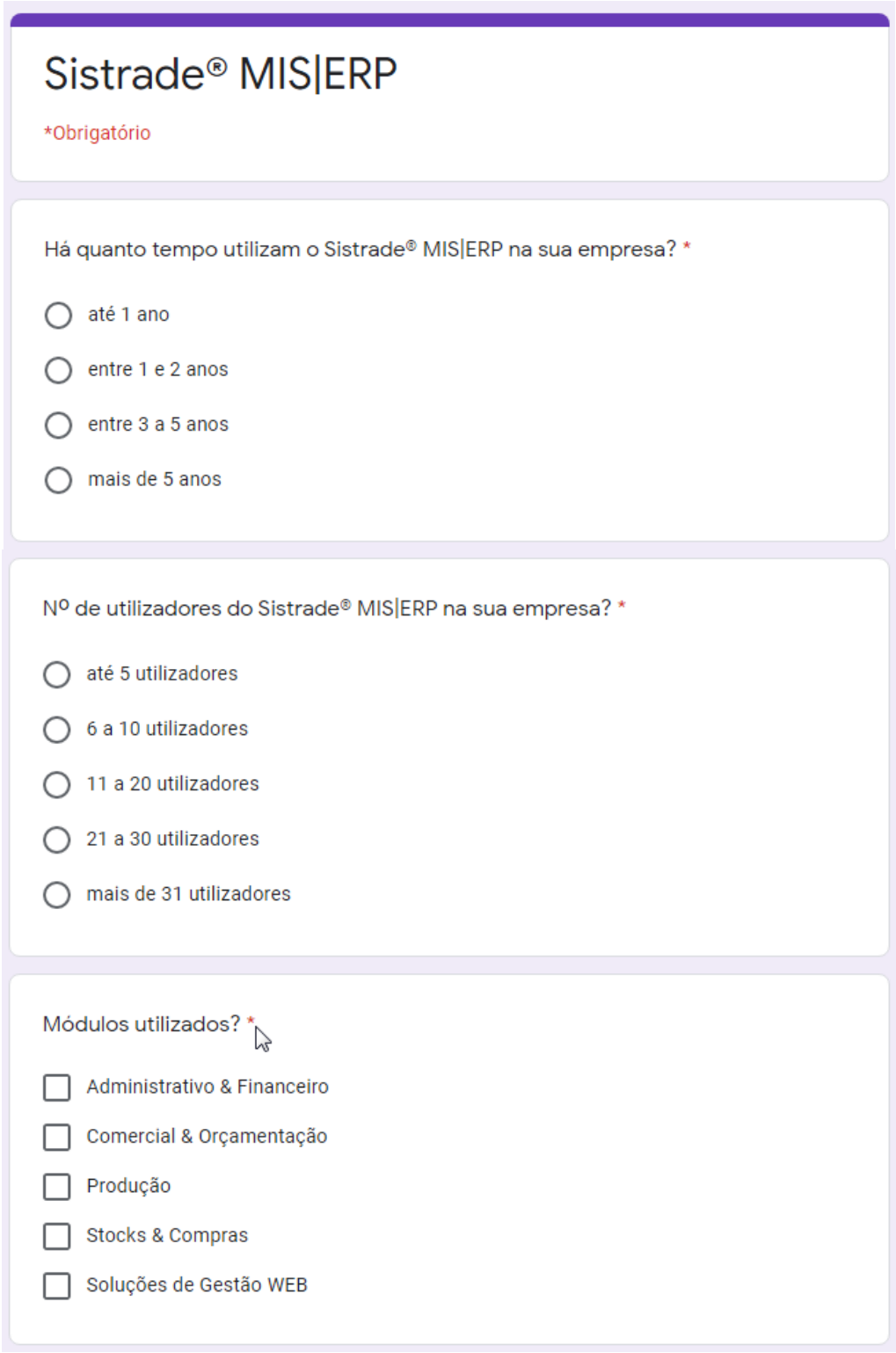


Figura 60 – Processo de Controlo de Qualidade

Anexo C – Inquérito

Modelo



Sistrade® MIS|ERP

*Obrigatório

Há quanto tempo utilizam o Sistrade® MIS|ERP na sua empresa? *

- até 1 ano
- entre 1 e 2 anos
- entre 3 a 5 anos
- mais de 5 anos

Nº de utilizadores do Sistrade® MIS|ERP na sua empresa? *

- até 5 utilizadores
- 6 a 10 utilizadores
- 11 a 20 utilizadores
- 21 a 30 utilizadores
- mais de 31 utilizadores

Módulos utilizados? *

- Administrativo & Financeiro
- Comercial & Orçamentação
- Produção
- Stocks & Compras
- Soluções de Gestão WEB

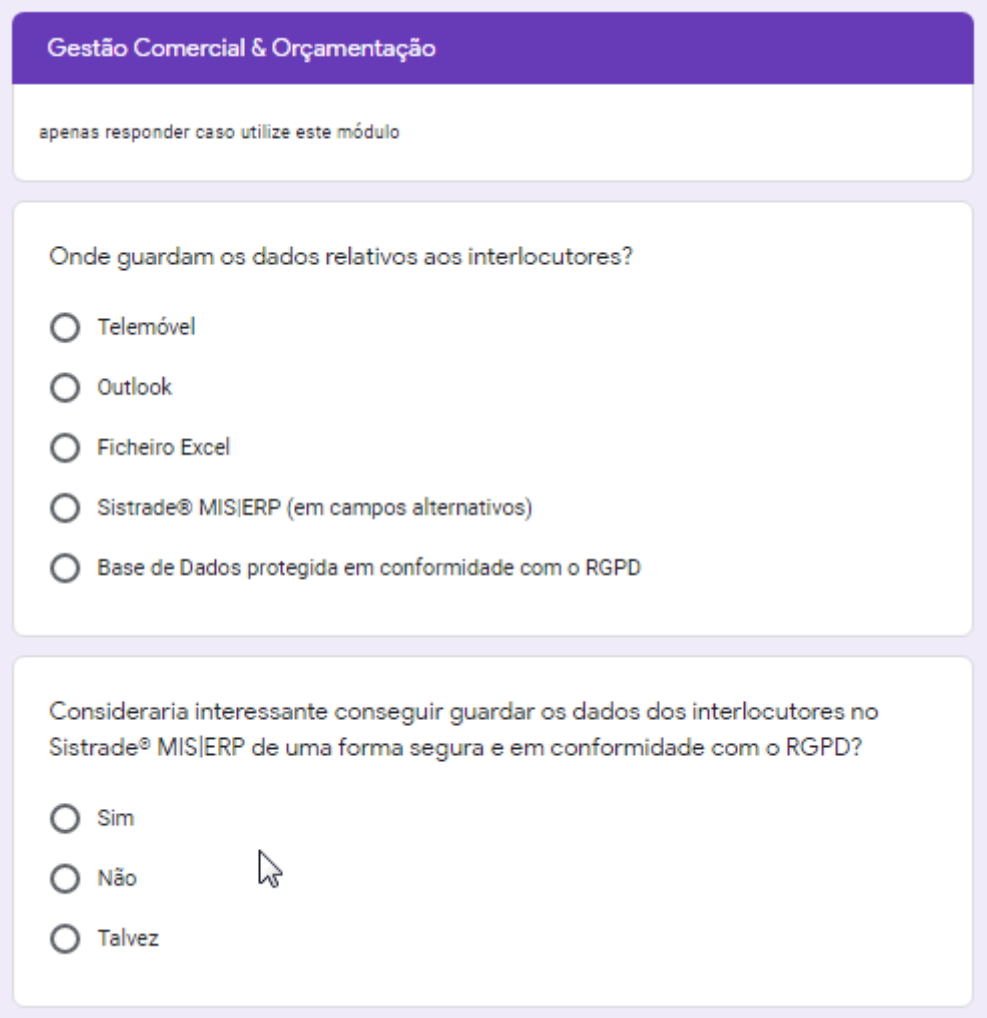
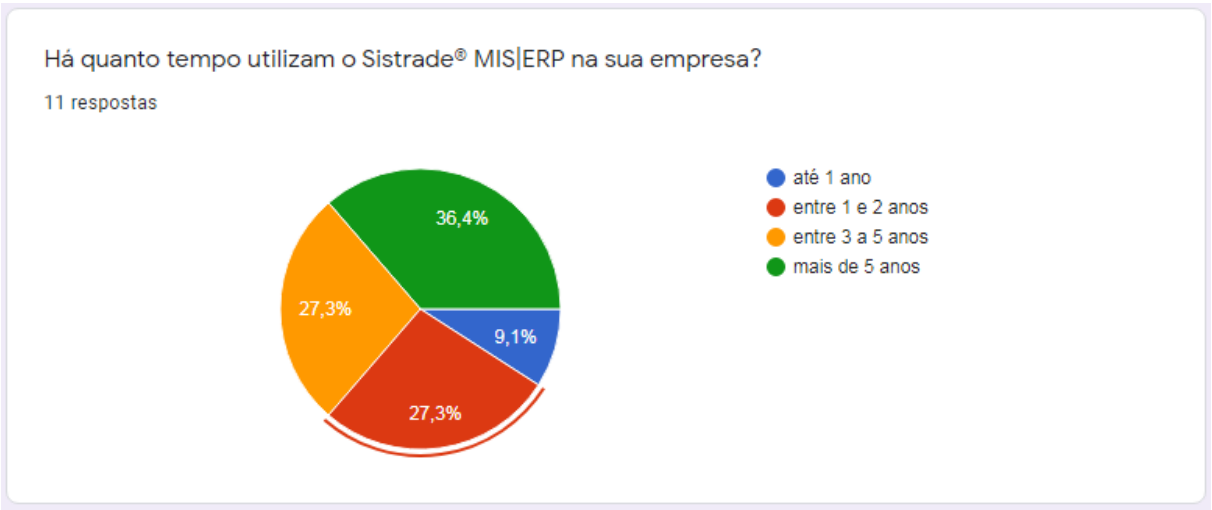


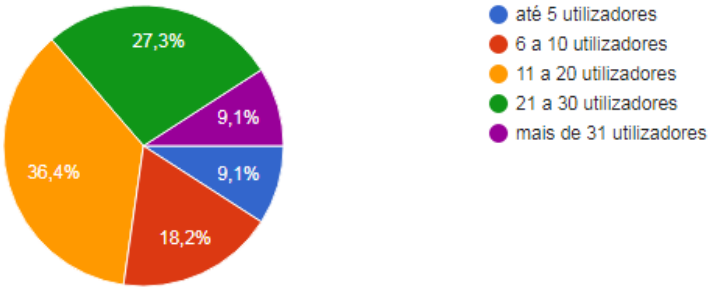
Figura 61 – Modelo de inquérito

Resultado



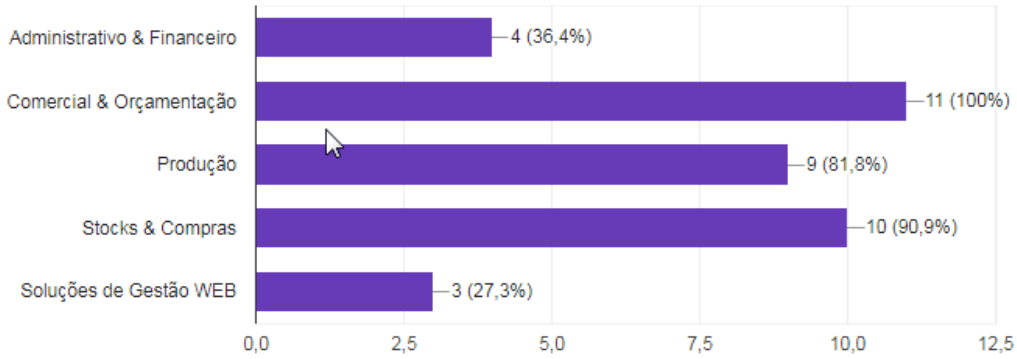
Nº de utilizadores do Sistrade® MIS|ERP na sua empresa?

11 respostas



Módulos utilizados?

11 respostas



Gestão Comercial & Orçamentação

Onde guardam os dados relativos aos interlocutores?

10 respostas

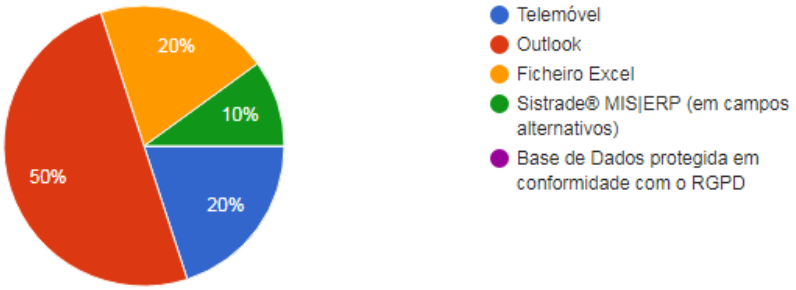


Figura 62 – Resultados do inquérito

Anexo D – Modelos de documentos

Modelo de consentimento de uso de imagem

DECLARAÇÃO DE AUTORIZAÇÃO/
CONSENTIMENTO DE USO DE IMAGEM

Eu,_____(Nome), trabalhador(a) da _____(Empresa), declaro que autorizo e dou o meu consentimento expresso para a recolha e utilização da minha imagem em formato foto e/ou vídeo nos suportes comunicacionais, durante a realização/divulgação de atividades no âmbito da execução do contrato de trabalho.

Os dados pessoais recolhidos serão utilizados para as seguintes finalidades:

- Marketing e divulgação interna e externa através de diversos meios de comunicação, tais como quadros físicos informativos, material de apoio à formação, Relatório de contas, redes internas (intranet, e-mail interno, newsletters, Portal do Colaborador, SharePoint, televisão interna), plataformas de comunicação, redes sociais (Linkedin, Facebook, etc.), internet (incluindo nos websites), conferências e eventos ligados aos diversos sectores;
- Fins históricos da **<empresa>**.

O presente consentimento é dado de forma livre e não é necessário para a execução de nenhum contrato ou prestação de serviço. Os dados pessoais tratados serão mantidos nas plataformas de comunicação durante cinco anos e, depois disso, poderão ser utilizados para fins históricos durante dez anos e poderão ser transmitidos a entidades com quem a **<empresa>** contrate a execução dessas finalidades. Este consentimento poderá ser retirado a qualquer momento. A retirada do consentimento não torna ilícitos os tratamentos efetuados com base no consentimento anteriormente concedido.

Como titular de dados tenho o direito de solicitar à empresa o acesso, a retificação, o apagamento, a limitação do tratamento, a oposição e a portabilidade dos dados pessoais que me digam respeito. Caso deseje retirar o seu consentimento ou exercer os seus direitos contacte por escrito **<e-mail DPO>**. Estão disponíveis na Política de Privacidade da **<empresa>** informações adicionais sobre o tratamento de dados pessoais e os direitos dos titulares de dados, que pode ser consultada em **<site>**. O responsável pelo tratamento é a **<empresa>**, com morada na **<morada>** e correio eletrónico **<e-mail DPO>**. Para o esclarecimento de dúvidas relativas ao tratamento de dados pessoais p.f. contacte o DPO através de **<e-mail DPO>**.

Declaro, ainda, que tomei conhecimento e entendi todas as informações facultadas no presente documento e que fui informado(a) de que todas as imagens e vídeos que forem divulgados em redes externas se tornam públicos.

Consentimento recolhido em _____ (data)

Local _____

_____ (assinatura)

Modelo de cláusula no contrato de trabalho

CONTRATO DE TRABALHO

Entre

1º **<Entidade patronal>**

e

2º **<colaborador>**

(…)

DADOS PESSOAIS

1. O primeiro outorgante, na qualidade de responsável pelo tratamento de dados, realizará operações de tratamento de dados pessoais do Segundo outorgante, titular dos dados, reconhecendo o Segundo outorgante que a comunicação dos dados pessoais constitui uma obrigação contratual e legal, assim como um requisito necessário para a celebração e execução do presente contrato.

2. As atividades de tratamento destinam-se às atividades relacionadas com a administração e gestão do contrato de trabalho e da relação laboral entre os outorgantes, nomeadamente o processamento de salários e/ou outras relacionadas com a gestão de pessoal, sendo os referidos dados pessoais e tratamentos necessários quer para a execução do contrato entre as partes, quer para o cumprimento das obrigações legais a que o primeiro outorgante se encontra sujeito, nomeadamente, no âmbito da legislação laboral, de segurança social e fiscal.

3. O primeiro outorgante poderá ainda realizar o tratamento de dados pessoais necessários para o efeito dos interesses legítimos prosseguidos pelo primeiro outorgante ou por terceiros, nomeadamente, quando o tratamento dos dados pessoais seja estritamente necessário e proporcional de modo a garantir a segurança das redes e da informação, em conformidade com a política interna de proteção de dados do primeiro outorgante.

4. O primeiro outorgante irá proceder, nomeadamente, ao tratamento das categorias de dados pessoais do segundo outorgante melhor identificados no anexo 1 a este contrato.

5. Sem prejuízo do numero anterior, o primeiro outorgante irá igualmente realizar o tratamento dos documentos do segundo outorgante identificados no anexo 1, assim como da informação existente nesses mesmos documentos.

6. O segundo outorgante tem desde já conhecimento e reconhece que poderão ocorrer tratamentos de categorias especiais de dados pessoais quando:

a) necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do primeiro outorgante ou do segundo outorgante em matéria de legislação laboral, de segurança social e de proteção social; ou,

b) necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do segundo outorgante.

7. Os tratamento de categorias especiais de dados pessoais e informação complementar a estes tratamentos, encontram-se melhor descritos na política interna de proteção de dados do primeiro

outorgante, ou, no âmbito de outras políticas e/ou regulamentos internos do primeiro outorgante.

8. O primeiro outorgante, no âmbito das atividade relacionadas com a administração e gestão do contrato de trabalho e da relação laboral entre as partes, poderá comunicar e/ou transferir os dados pessoais do segundo outorgante às entidades a seguir identificadas, não excluindo outras entidades não mencionadas, mas que tenham legitimidade legal para proceder ao tratamento dos dados em questão:

a) IGFSS – Instituto de Gestão Financeira da Segurança Social;
b) AT – Autoridade Tributária;
c) Instituições Bancárias e Seguradoras;
d) INE – Instituto Nacional de Estatística;
e) ACT – Autoridade para as Condições do Trabalho;
f) Entidade que tem a seu cargo o desempenho das funções relativas à Segurança, Higiene e Medicina no Trabalho;
g) Qualquer outra entidade à qual tenham sido atribuídas funções de processamento de salários e/ou outras relacionadas com a gestão de recursos humanos.

9. As comunicações e/ou transferências referidas no número anterior têm como finalidade, nomeadamente:

a) o cálculo e pagamento de retribuições, prestações acessórias, ou outros abonos e gratificações;
b) o cálculo, retenção na fonte e operações relativas a descontos na retribuição, obrigatórios ou facultativos, decorrentes de disposição legal;
c) a realização de operações estatísticas não nominativas relacionadas com o processamento de salários no âmbito da entidade processadora;
d) o cumprimento das obrigações a que o primeiro outorgante se encontra sujeito, nomeadamente, no âmbito da legislação laboral, de segurança social e fiscal.

10. Os referidos dados pessoais, e outros que venham a ser objeto de tratamento pelo primeiro outorgante, serão obtidos através do presente contrato de trabalho, bem como através de outros documentos que venham a ser solicitados pelo primeiro outorgante, no exercício das funções do segundo outorgante e, no decorrer da relação laboral entre as partes.

11. As referidas comunicações e/ou transferências terão como finalidade operações e atividades relacionadas com a administração e gestão do contrato de trabalho e da relação entre as partes, e, para o efeito dos interesses legítimos prosseguidos pelo primeiro outorgante, garantindo o primeiro outorgante que em caso de qualquer transferência de dados que ocorra para fora do espaço da União Europeia, tanto o primeiro outorgante com o terceiro destinatário dos dados pessoais em questão, cumprirão com as suas obrigações legais quanto às condições de tal transferência, nomeadamente, no que respeita à aplicação de medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco.

12. O primeiro outorgante irá conservar os dados pessoais apenas durante o período necessário à execução das finalidades a que os mesmos se destinam e ao cumprimento das suas obrigações legais tendo em consideração para a definição deste período, quer as melhores praticas, quer as obrigações legais a que o primeiro outorgante se encontra sujeita, nomeadamente, no âmbito da legislação laboral, de segurança social e fiscal.

13. O segundo outorgante declara expressamente que antes da assinatura do presente contrato foi informado pelo primeiro outorgante dos seus direitos, nomeadamente, no que respeita ao acesso

aos dados pessoais que lhe digam respeito, à sua retificação ou apagamento, à limitação ou oposição ao tratamento, a apresentar reclamações junto à autoridade de controlo, bem como, do direito à portabilidade dos dados, reconhecendo que estes direitos poderão ser limitados em cumprimento das obrigações legais a que o primeiro outorgante se encontra sujeito, nomeadamente, no âmbito da legislação laboral, de segurança social e fiscal.

14. A forma de exercício dos direitos referidos no número anterior poderá encontrar-se melhor descrita na política interna de proteção de dados do primeiro outorgante.

15. Qualquer outro tratamento de dados pessoais do segundo outorgante que o primeiro outorgante venha para outras finalidades que não as identificadas na presente cláusula, bem como, o tratamento posterior dos dados pessoais para uma finalidade que não seja aquela para o qual os dados pessoais tenham sido recolhidos, ou, a existência de decisões automatizadas, incluindo a definição de perfis, será objeto de informação do segundo outorgante através do regulamento e/ou politica própria, onde se identifiquem as categorias de dados pessoais, finalidades, base jurídica para o tratamento e quaisquer outras informações pertinentes.

ANEXO 1

Dados pessoais sujeitos a tratamento:

- **Dados de identificação:** nome completo, data de nascimento, morada, correio eletrónico e telemóvel;
- **Dados de documento de identificação:** nº de identificação civil, local de emissão, data de emissão, validade, nº de segurança social, nacionalidade e naturalidade;
- **Dados bancários:** nome do banco, NIB e IBAN;
- **Situação académica:** habilitações literárias, estabelecimento de ensino e média final;
- **Situação fiscal:** nº identificação fiscal, código da repartição das finanças, estado civil, grau de incapacidade, nº titulares e nº dependentes;
- **Documentos:** documento de identificação, fotografia, currículo vitae, comprovativo de NIB, certificado de habilitações, certificado de trabalho e boletim de vacinação.

Anexo E – Processo de auditoria

SISTRADE MIS | ERP Processo Auditoria		
Assunto	**Questão**	**Resposta**
Gestão	O regulamento interno reflete todas as preocupações e ações tomadas pela empresa para a conformidade com o RGPD	
	O regulamento interno está devidamente divulgado pelos colaboradores?	
	A política de privacidade é transparente e conciso para o utilizador?	
	Existe registo dos colaboradores que lidam com dados pessoais, com as respectivas justificações e responsabilidades?	
	A informação recolhida é a absolutamente necessária? Consegue justificar os dados recolhidos e a forma de tratamento dos mesmos?	
	Necessita de obter um Encarregado de Proteção de Dados?	
	Necessita de dar formaçao aos colaboradores?	
Consentimentos	Os dados recolhidos na base de dados foram recolhidos com o consentimento necessário? É possível prová-lo?	
	O utilizador consegue gerir os seus consentimentos (alterar ou apagar)?	
	O consentimento é granular?	
	O consentimento foi obtido via double opt in?	
Base de Dados	A base de dados foi adquirida de um terceiro?	
	Partilha a sua base de dados com terceiros?	
	A base de dados está encriptada?	
	Tem conhecimento de alguma fuga de informação?	
	Participou essa fuga de informação às autoridades competentes?	