# Regulamento Geral de Proteção de dados

## RGPD e geolocalização com articulação NIS2

ICA | Versão 2.3 | 25 de setembro de 2026

Regras de proteção de dados para todas as partes interessadas, gestão de incidentes e continuidade dos serviços de alimentação coletiva. Integra 24 grupos de partes interessadas, 23 anexos operacionais e 10 árvores de decisão.

Documento para aprovação interna. A aplicação legal da NIS2 à entidade permanece sujeita à avaliação documentada do Anexo 20; a inclusão deste capítulo não constitui declaração de enquadramento ou de conformidade.

## Controlo e estado do documento

| Campo | Identificação |
|---|---|
| Organização | ICA — [DENOMINAÇÃO SOCIAL COMPLETA, NIF E MORADA] |
| Código | MAN-RGPD-01 · versão 2.3 |
| Data de revisão | 25 de setembro de 2026 |
| Responsável pelo tratamento | [ENTIDADE E CONTACTOS POR TRATAMENTO] |
| Contacto de privacidade / incidentes | [CONTACTOS E SUPLENTE PARA URGÊNCIAS] |
| EPD | [DECISÃO DE DESIGNAÇÃO; NOME/CONTACTO QUANDO DESIGNADO] |
| Aprovação e entrada em vigor | [ÓRGÃO, DATA E ASSINATURA] |
| Revisão | Pelo menos anual; antecipada por alteração legal, operacional ou incidente. |
| Distribuição | Interna e controlada. Avisos externos próprios nos pontos de recolha. |

## O que esta edição consolida

Revisão do manual existente, com alargamento do mapa de partes interessadas, aprofundamento dos procedimentos, modelos de informação e evidência, proteção dos utentes e regras expressas de respeito pela raça, etnia, cor da pele, tradições, cultura e religião. Mantém as matérias de geolocalização, tecnologias digitais, segurança, direitos e avaliação de impacto. Integra oito árvores de decisão nas secções de aplicação, com ações, responsabilidades e ligação aos anexos. Esta edição integra a articulação NIS2 e o regime português, dois novos fluxogramas e quatro anexos de cibersegurança, mantendo os conteúdos de proteção de dados e diversidade.

## Condições de aplicação

Os cenários descritos não confirmam que todos os tratamentos existam na ICA. O responsável de cada processo deve assinalar a aplicabilidade, identificar a realidade da sua unidade e completar os campos entre parênteses retos. Os prazos marcados como propostas internas só se aplicam após validação; não são apresentados como imposições legais.

A aprovação documental não prova conformidade nem autoriza um tratamento ilícito. A cobertura efetiva resulta da ligação entre as pessoas abrangidas, os fluxos reais, as bases jurídicas, os controlos implementados e a evidência de verificação. Assuntos sem informação empresarial suficiente permanecem identificados para decisão, sem pressupor a sua resolução. A análise de aplicabilidade e o calendário NIS2 constam do Anexo 20.

# Roteiro de consulta


| Bloco | Conteúdo | Pág. |
|---|---|---|
| A | Política, governação, partes interessadas e diversidade | 6 |
| B | Ciclo de vida, segurança, NIS2 e incidentes | 22 |
| C | Geolocalização: finalidade, limites e configurações | 38 |
| D | Tecnologias digitais e contextos específicos | 42 |
| E | Instrumentos operacionais e modelos editáveis | 48 |
| Fontes | Referenciais legais e técnicos | 79 |
| Aprovação | Verificação e aprovação interna | 81 |


## Anexos para utilização


| Anexo | Instrumento | Pág. |
|---|---|---|
| 1 | Registo de atividades de tratamento | 49 |
| 2 | Triagem de AIPD | 50 |
| 3 | Teste de interesse legítimo | 51 |
| 4 | Registo de violação de dados | 52 |
| 5 | Exercício de direitos | 53 |
| 6 | Ficha de geolocalização | 54 |
| 7 | Aprovação de novos tratamentos | 55 |
| 8 | Conservação: ficha e regras de referência | 56 |
| 9 | Partes interessadas e fichas de aplicação | 58 |
| 10 | Avisos de privacidade por público | 64 |
| 11 | Qualificação de papéis e comunicação de dados | 66 |
| 12 | Diligência e contrato de subcontratação | 67 |
| 13 | AIPD e matriz de riscos para as pessoas | 68 |
| 14 | Resposta a incidentes e modelos de comunicação | 69 |

| Anexo | Instrumento | Pág. |
|---|---|---|
| 15 | Instrução alimentar e representação | 70 |
| 16 | Consentimento, oposição e prova de informação | 71 |
| 17 | Saída, eliminação e preservação excecional | 72 |
| 18 | Plano de implementação e verificação da cobertura | 73 |
| 19 | Respeito pelas diferenças e não discriminação | 74 |
| 20 | Aplicabilidade e calendário NIS2 | 75 |
| 21 | Ativos riscos e controlos | 76 |
| 22 | Registo integrado de incidente | 77 |
| 23 | Continuidade ensaio e retoma | 78 |

# Localização das árvores de decisão

Consultar a árvore junto do procedimento correspondente. As caixas pretas assinalam início e conclusão; os retângulos cinzentos indicam ações; os losangos laranja contêm decisões. Seguir os ramos Sim ou Não e as notas de aplicação.

| N.º | Árvore de decisão | Local no manual | Pág. |
|---|---|---|---|
| 7 | Diversidade e não discriminação | Secção 3.6 | 14 |
| 2 | Pedidos de exercício de direitos | Secção 7 | 19 |
| 8 | Conservação e eliminação de dados | Secção 8 | 21 |
| 1 | Novos tratamentos de dados | Secção 9 | 23 |
| 5 | Partilha de dados com terceiros | Secções 11 e 12 | 26 |
| 3 | Violações de dados pessoais | Secção 14 | 34 |
| 4 | Geolocalização em contexto laboral | Secções 16 a 23 | 41 |
| 6 | Dietas e instruções alimentares | Secção 28 | 45 |
| 9 | Aplicabilidade do regime de cibersegurança | Secção 13.3 | 29 |
| 10 | Resposta integrada ao incidente | Secção 14.2 | 35 |

As árvores resumem os procedimentos e são lidas em conjunto com as respetivas secções. Uma decisão interna não afasta requisitos legais. O EPD aconselha e monitoriza; o responsável pelo tratamento conserva a competência de decisão.

# A Política corporativa e governação

## 1 Objeto e âmbito

O presente manual estabelece as regras aplicáveis ao tratamento de dados pessoais pela ICA, independentemente do suporte, tecnologia, local ou categoria de titular. Abrange trabalhadores, candidatos, clientes, utilizadores, fornecedores, prestadores, visitantes, parceiros e demais pessoas singulares cujos dados sejam tratados. Integra o compromisso de igualdade e de respeito pelas diferenças de raça, etnia, cor da pele, tradições, cultura e religião, desenvolvido na secção 3.6.

Aplica-se a websites, aplicações, correio eletrónico, plataformas, sistemas de gestão, videovigilância, controlo de acessos, dispositivos móveis, sensores, viaturas, sistemas de geolocalização, serviços em nuvem, ferramentas de inteligência artificial, arquivos físicos e operações executadas por terceiros em nome da organização.

## 2 Princípios obrigatórios

| Princípio | Regra operacional |
|---|---|
| Licitude, lealdade e transparência | Tratar apenas com fundamento válido e informar de forma compreensível |
| Limitação das finalidades | Definir a finalidade antes da recolha e controlar reutilizações |
| Minimização | Recolher apenas o estritamente necessário |
| Exatidão | Permitir atualização e corrigir dados inexatos |
| Limitação da conservação | Apagar ou anonimizar quando termina a necessidade |
| Integridade e confidencialidade | Aplicar segurança adequada ao risco |
| Responsabilidade demonstrável | Conservar decisões, avaliações, registos e evidências |
| Proteção desde a conceção e por defeito | Incorporar privacidade no desenho e nas configurações iniciais |

## 3 Papéis e responsabilidades

EPD significa encarregado de proteção de dados. A organização documenta se a sua designação é obrigatória; quando exista, assegura a independência, os recursos e a ausência de conflitos de interesses. A decisão sobre finalidades e meios permanece com o responsável pelo tratamento. AIPD significa avaliação de impacto sobre a proteção de dados.

| Interveniente | Responsabilidade essencial |
|---|---|
| Órgão de gestão | Aprovar a política, atribuir recursos e aceitar riscos residuais relevantes |
| Responsável pelo tratamento | Determinar finalidades e meios e assegurar conformidade |
| Encarregado de proteção de dados | Aconselhar, monitorizar, cooperar com a CNPD e atuar como ponto de contacto |
| Responsáveis de processo | Manter o registo do tratamento, aplicar prazos e comunicar alterações |
| Recursos humanos | Aplicar regras reforçadas a dados laborais, saúde e monitorização |
| Tecnologias de informação e segurança | Implementar controlos, registos de atividade, cópias de segurança, gestão de acessos e resposta técnica |

| Interveniente | Responsabilidade essencial |
|---|---|
| Compras e jurídico | Avaliar fornecedores, contratos, subcontratantes e transferências |
| Utilizadores autorizados | Aceder apenas por necessidade funcional e reportar incidentes |

## 3.1 Partes interessadas e expectativas

Uma parte interessada pode ser titular dos dados, representar titulares, definir finalidades, prestar serviços ou fiscalizar o cumprimento. A mesma entidade pode assumir papéis distintos em tratamentos diferentes. A ICA identifica, para cada tratamento, o interesse afetado, as obrigações aplicáveis, o canal de interação e a evidência da decisão. A matriz seguinte é uma base para validação por processo; não presume que todos os grupos se aplicam a todos os contratos. [R1, R8]

| Parte interessada | Necessidade e papel a verificar | Responsável e resposta mínima |
|---|---|---|
| 01 · Administração e órgãos sociais | Decisão, supervisão e dados dos próprios titulares. Transparência sobre remunerações, assinaturas e participações. | Gestão / Jurídico: acesso por competência; atas com dados mínimos; decisões e delegações documentadas. |
| 02 · Trabalhadores e antigos trabalhadores | Contratação, execução e cessação; remunerações, formação, avaliação e defesa de direitos. | RH: informação específica, arquivo segmentado, retirada de acessos na saída e conservação por classe documental. |
| 03 · Candidatos, estagiários e trabalhadores temporários | Seleção e integração; igualdade, confidencialidade e informação sobre fontes e testes. | RH: separar seleção atual de bolsa futura; delimitar papéis de agências e instituições de ensino. |
| 04 · Familiares, dependentes e contactos de emergência | Benefícios, obrigações legais ou contacto em emergência; dados de pessoas distintas do trabalhador. | RH: finalidade delimitada, informação aos titulares quando devida e revisão dos contactos; não reutilizar para marketing. |
| 05 · Sindicatos e representantes dos trabalhadores | Representação, informação e consulta; filiação sindical especialmente protegida. | RH / Jurídico: verificar mandato e dever aplicável; acesso restrito e comunicação mínima; não divulgar listas sindicais. |
| 06 · Clientes institucionais e entidades adjudicantes | Gestão do contrato; acesso a evidências do serviço e deveres de prestação de contas. | Gestor do contrato: qualificar cada fluxo, separar indicadores de dados nominativos e formalizar os artigos 26.º/28.º quando aplicáveis. |
| 07 · Contactos de clientes e potenciais clientes | Relação profissional, propostas e comunicações; o contacto é uma pessoa singular. | Comercial: fundamento por finalidade, origem do contacto e oposição; contrato com a empresa não legitima automaticamente todos os dados do contacto. |
| 08 · Utentes e consumidores | Inscrição, refeições, pagamentos, reclamações e qualidade do serviço. | Operação: aviso acessível, identificação suficiente e canais reservados; usar estatísticas anónimas quando bastem. |
| 09 · Crianças e jovens | Proteção reforçada, linguagem adequada à idade e segurança na entrega da refeição. | Gestor / escola / Operação: validar representação e canais; excluir exposição pública de saúde, listas de dívidas e perfis comerciais. |
| 10 · Idosos e pessoas com necessidades de apoio | Autonomia, acessibilidade e assistência; proteção contra divulgação indevida. | Operação: comunicar diretamente quando possível; verificar poderes do acompanhante e não presumir incapacidade pela idade. |

| Parte interessada | Necessidade e papel a verificar | Responsável e resposta mínima |
|---|---|---|
| 11 · Utentes com alergias e dietas específicas | Exatidão das instruções alimentares e reserva de dados de saúde ou crenças. | Nutrição / Operação: dupla validação das alterações, acesso por tarefa e fundamentação cumulativa nos artigos 6.º e 9.º. |
| 12 · Familiares, cuidadores e representantes de utentes | Receber ou transmitir informação apenas dentro de poderes comprovados. | Operação: verificar identidade, legitimidade e âmbito; registar a verificação sem conservar cópias excessivas. |
| 13 · Fornecedores e prestadores individuais | Contratação, pagamentos e avaliação; dados de empresários individuais e contactos. | Compras / Financeira: separar dados empresariais de pessoais, limitar avaliações e validar destinatários de pagamentos. |
| 14 · Trabalhadores de fornecedores e parceiros | Acesso a instalações, qualificação e execução dos serviços. | Compras / Segurança: pedir comprovativos necessários, evitando salários, documentos de saúde ou identificações integrais sem fundamento. |
| 15 · Subcontratantes e subcontratantes ulteriores | Tratamento por instruções; segurança, assistência e cadeia de prestação. | Compras / TI: diligência, contrato, autorização da cadeia, transferências, testes de saída e prova de eliminação. |
| 16 · Profissionais de saúde, laboratórios e SST | Informação sujeita a sigilo; aptidão, vigilância da saúde ou investigação de incidente. | SST / Jurídico: identificar papéis reais e separar resultados clínicos de conclusões funcionais; limitar acesso a resultados individualizados. |
| 17 · Visitantes, transportadores e participantes | Acessos, segurança, eventos e eventuais imagens. | Segurança / organização do evento: aviso no ponto de recolha, identificadores mínimos e conservação curta validada. |
| 18 · Utilizadores digitais e destinatários de marketing | Website, aplicações, cookies, apoio e comunicações comerciais. | TI / Comunicação: escolhas granulares, bloqueio de tecnologias opcionais e cancelamento simples das comunicações. |
| 19 · Denunciantes, visados e testemunhas | Confidencialidade, não retaliação, defesa e apuramento imparcial. | Responsável do canal: arquivo segregado, identidade reservada e acesso limitado; não tratar uma denúncia como reclamação comum. |
| 20 · Auditores, certificadores e consultores | Evidências de conformidade; independência e confidencialidade. | Qualidade / Jurídico: amostra mínima, anonimização, consulta supervisionada e registo das extrações autorizadas. |
| 21 · Seguradoras, bancos e assessores jurídicos | Gestão de sinistros, pagamentos e defesa; funções próprias ou por conta de outrem. | Financeira / Jurídico: verificar papel, base e necessidade; enviar apenas documentos pertinentes por canal seguro. |
| 22 · CNPD, tribunais e outras autoridades | Fiscalização, investigação, obrigações legais e exercício de poderes públicos. | Jurídico / Privacidade: autenticar pedido, competência, âmbito e prazo; registar resposta e preservação de evidência. |
| 23 · Parceiros, comunidade e comunicação social | Projetos, ações sociais, contactos institucionais e informação pública. | Gestão / Comunicação: aprovar divulgação; usar informação agregada e autorizações específicas quando necessárias. |

| Parte interessada | Necessidade e papel a verificar | Responsável e resposta mínima |
|---|---|---|
| 24 · Pessoas falecidas e interlocutores legitimados | Proteção nacional de certos dados e exercício de direitos nos termos legais. | Jurídico / Privacidade: aplicar artigo 17.º da Lei n.º 58/2019, verificar designação/herdeiros e limites deixados pelo titular. |

### 3.2 Papéis, consulta e decisão

O contrato comercial não determina por si só o papel no RGPD. Em cada fluxo, o responsável do processo e Jurídico documentam quem define a finalidade e os meios essenciais, quem trata dados por instruções e se há decisão conjunta. A ICA pode atuar como responsável, subcontratante ou corresponsável conforme a operação; uma comunicação a um cliente não cria automaticamente direito a consultar posições ou percursos nominativos. Se houver responsabilidade conjunta, definir transparentemente as responsabilidades nos termos do artigo 26.º; se houver subcontratação, aplicar o artigo 28.º. [R1, R8]

| Situação | Consulta e decisão antes do tratamento | Registo mínimo |
|---|---|---|
| Novo serviço ou contrato | Operação + Jurídico classificam os papéis de cada entidade; Privacidade/EPD aconselha; Gestão aprova o desenho e os recursos. | Mapa de fluxos, acordo do artigo 26.º ou contrato do artigo 28.º quando aplicável, avisos. |
| Nova geolocalização laboral | Operação, RH, TI e Jurídico demonstram necessidade, horários, dados e alternativas; EPD aconselha; representantes são envolvidos quando exigido. | Ficha de geolocalização, triagem/AIPD, informação ao trabalhador e decisão de ativação. |
| Pedido de cliente por dados individuais | Gestor do contrato verifica finalidade e destinatário com Jurídico; consulta EPD se houver risco; disponibiliza só o necessário quando exista fundamento. | Pedido, base da comunicação, âmbito, autorização e registo de acesso. |
| Incidente ou pedido de direitos | Quem recebe comunica imediatamente ao canal interno; Privacidade coordena; responsável pelo tratamento decide e responde; subcontratante assiste. | Linha temporal, classificações, comunicações e comprovativo de fecho. |

O EPD, quando designado, aconselha e monitoriza com independência; não aprova em substituição do responsável pelo tratamento. Em caso de divergência, registar o parecer, a decisão fundamentada e o decisor. Os requisitos específicos, a importância e o estado de resposta a cada grupo constam do Anexo 9. [R1]

### 3.3 Proteção dos utentes e representação

Nos serviços de alimentação coletiva, a informação sobre alergias, intolerâncias, dietas terapêuticas ou outras condições de saúde é limitada ao necessário para preparar e entregar a refeição com segurança. O responsável do processo identifica a origem da instrução, a pessoa autorizada a atualizá-la, os destinatários e o prazo de conservação. A identificação deve permitir evitar trocas de refeições sem expor publicamente a condição de saúde do utente.

A condição de familiar ou cuidador não confere, por si só, acesso aos dados. Antes de prestar informação ou receber instruções em nome de um titular, verifica-se a representação ou autorização pertinente e o respetivo âmbito. A idade avançada não é tratada como incapacidade. A comunicação deve ser acessível ao titular e, quando aplicável, ao seu representante. [R1]

A recolha de dados de saúde depende da identificação cumulativa dos fundamentos aplicáveis dos artigos 6.º e 9.º. A existência de um contrato de alimentação, de uma prescrição dietética ou de um

pedido do cliente não dispensa essa análise. A ICA e a entidade cliente definem por escrito os respetivos papéis, os fluxos autorizados e a resposta a alterações, pedidos e incidentes. [R1, R8]

### 3.4 Participação e acompanhamento

Antes de um novo tratamento ou de uma alteração relevante, o responsável do processo identifica os grupos afetados e recolhe as suas necessidades através de canais adequados: reuniões com clientes, interlocutores dos utentes, estruturas representativas dos trabalhadores ou pedidos e reclamações. Na AIPD, pondera a recolha da opinião dos titulares ou dos seus representantes, quando adequado, e documenta a decisão, salvaguardando a segurança e os interesses protegidos. [R1, artigo 35.º, n.º 9]

As prioridades atendem à gravidade e probabilidade do dano para as pessoas, à vulnerabilidade dos titulares e à intrusão do tratamento. A influência comercial de uma parte interessada não reduz os direitos de outra. Divergências são registadas com o requisito em causa, alternativas, parecer do EPD quando exista, decisão fundamentada e responsável pela execução.

O responsável de cada processo revê os registos nas alterações contratuais ou tecnológicas, após incidentes e reclamações relevantes e, pelo menos, anualmente. Privacidade consolida as ações pendentes e apresenta à gestão os desvios, prazos e evidências de eficácia. Uma ação só é encerrada após verificação da sua execução.

### 3.5 Critério de cobertura e enquadramento do EPD

O RGPD protege pessoas singulares. Uma empresa, uma escola, uma autoridade ou um sindicato pode ser parte interessada sem ser titular de dados; os seus representantes, trabalhadores e interlocutores podem sê-lo. Um mesmo grupo pode acumular funções. A classificação não depende da designação comercial do contrato.

O mapa de 24 grupos da secção 3.1 é uma lista de verificação de âmbito. Cada unidade e contrato assinala «aplicável», «não aplicável, com fundamento» ou «por confirmar». Identifica ainda grupos adicionais, dados e serviços não previstos. Nenhum grupo se considera coberto apenas por constar da lista: exige-se ligação ao tratamento, aviso, responsável, prazo e evidência de controlo.

A Gestão documenta a obrigatoriedade de designar EPD à luz do artigo 37.º: autoridade/organismo público, com a exceção legal dos tribunais; atividades principais que exijam controlo regular e sistemático de titulares em larga escala; ou atividades principais de tratamento em larga escala de categorias especiais ou dados do artigo 10.º. A dimensão da empresa, isoladamente, não resolve a questão. Se designado, publicam-se os contactos, comunicam-se à CNPD e assegura-se acesso direto à gestão de topo. O EPD não determina as finalidades e os meios que depois fiscaliza. [R1]

| Decisão | Quem executa / decide | Controlo de independência |
|---|---|---|
| Novo tratamento | Responsável do processo prepara; Gestão decide; TI e Jurídico validam as respetivas matérias. | EPD aconselha; divergências ficam fundamentadas. |
| Pedido de direitos | Privacidade coordena; dono do sistema executa; responsável pelo tratamento responde. | EPD acompanha os casos complexos e o cumprimento dos prazos. |
| Violação de dados | TI contém; Privacidade e Jurídico avaliam; responsável pelo tratamento decide notificações. | EPD é envolvido atempadamente; ausência do decisor habitual não suspende o prazo. |
| Auditoria e revisão | Qualidade coordena evidência; responsáveis corrigem; Gestão assegura recursos. | O auditor evita avaliar exclusivamente controlos que executa. |

### 3.6 Igualdade, diversidade e respeito pelas diferenças

A ICA assume o respeito pela dignidade de cada pessoa e pelas diferenças de raça, etnia, cor da pele, tradições, cultura e religião, incluindo a ausência de crença religiosa. Este compromisso aplica-se a todas as partes interessadas e a todas as fases da relação: recrutamento, trabalho, contratação, atendimento, prestação alimentar, comunicação, exercício de direitos e resposta a reclamações. São incompatíveis com esta política a discriminação direta ou indireta, a segregação, o assédio, a humilhação, a estigmatização e a retaliação. A proteção abrange também deficiência, idade, sexo, orientação sexual e demais fatores legalmente protegidos; as adaptações necessárias não justificam recolha excessiva de dados.

As decisões assentam em critérios objetivos, necessários, proporcionais e documentados. Uma regra aparentemente igual para todos deve ser reavaliada se criar desvantagem injustificada para determinado grupo. Não se presume religião, origem étnica, nacionalidade, capacidade linguística ou necessidade alimentar a partir do nome, aparência, cor da pele, vestuário ou morada. O respeito por uma tradição não permite afastar a dignidade, a igualdade, os direitos de terceiros ou as exigências legais de segurança. [R3; R16; R17]

| Dimensão | Regra de atuação | Evidência sem exposição desnecessária |
|---|---|---|
| Raça, etnia e cor da pele | Não usar características protegidas para excluir, hierarquizar, selecionar ou atribuir tratamento desfavorável. Proibir rótulos e comentários depreciativos em registos e comunicações. | Critérios de decisão, revisão de queixas e formação; não criar listas de pessoas por raça ou cor. |
| Tradições e cultura | Ouvir a necessidade concreta, evitar estereótipos e adaptar comunicação e procedimentos quando adequado. Não tratar uma cultura como uniforme. | Pedido funcional e solução acordada, registados no mínimo necessário. |
| Religião e convicções | Respeitar crenças, práticas e ausência de crença. Não exigir declaração religiosa como condição geral de acesso a um serviço ou oportunidade. | Critério objetivo aplicado e medida adotada, sem cadastro de crenças. |
| Alimentação | Analisar restrições, ingredientes, práticas e horários solicitados, dentro das condições legais, de segurança e contratuais. Explicar limitações reais e procurar alternativa adequada. | Instrução alimentar validada; confirmação de ingredientes, preparação e condições efetivamente asseguradas. |
| Linguagem e acessibilidade | Usar linguagem respeitosa e compreensível; facultar apoio ou tradução quando necessário à compreensão, mantendo confidencialidade. Não presumir representação por pertença cultural. | Versão do aviso, meio de apoio e verificação da compreensão quando relevante. |
| Reclamação e reparação | Disponibilizar canal acessível, avaliação imparcial, proteção contra retaliação e correção de práticas discriminatórias. | Processo reservado, decisão fundamentada, ação e verificação de eficácia. |

Origem racial ou étnica e convicções religiosas ou filosóficas são categorias especiais do artigo 9.º. Informação sobre cor da pele, tradições, cultura, preferências ou dieta pode revelar essas categorias conforme o contexto. A política de igualdade não constitui fundamento autónomo para as recolher: primeiro verificar se a finalidade pode ser cumprida sem esse dado; se o tratamento for indispensável, documentar a base do artigo 6.º, a condição do artigo 9.º quando aplicável e as salvaguardas. Não inferir crenças ou etnia para criar perfis.

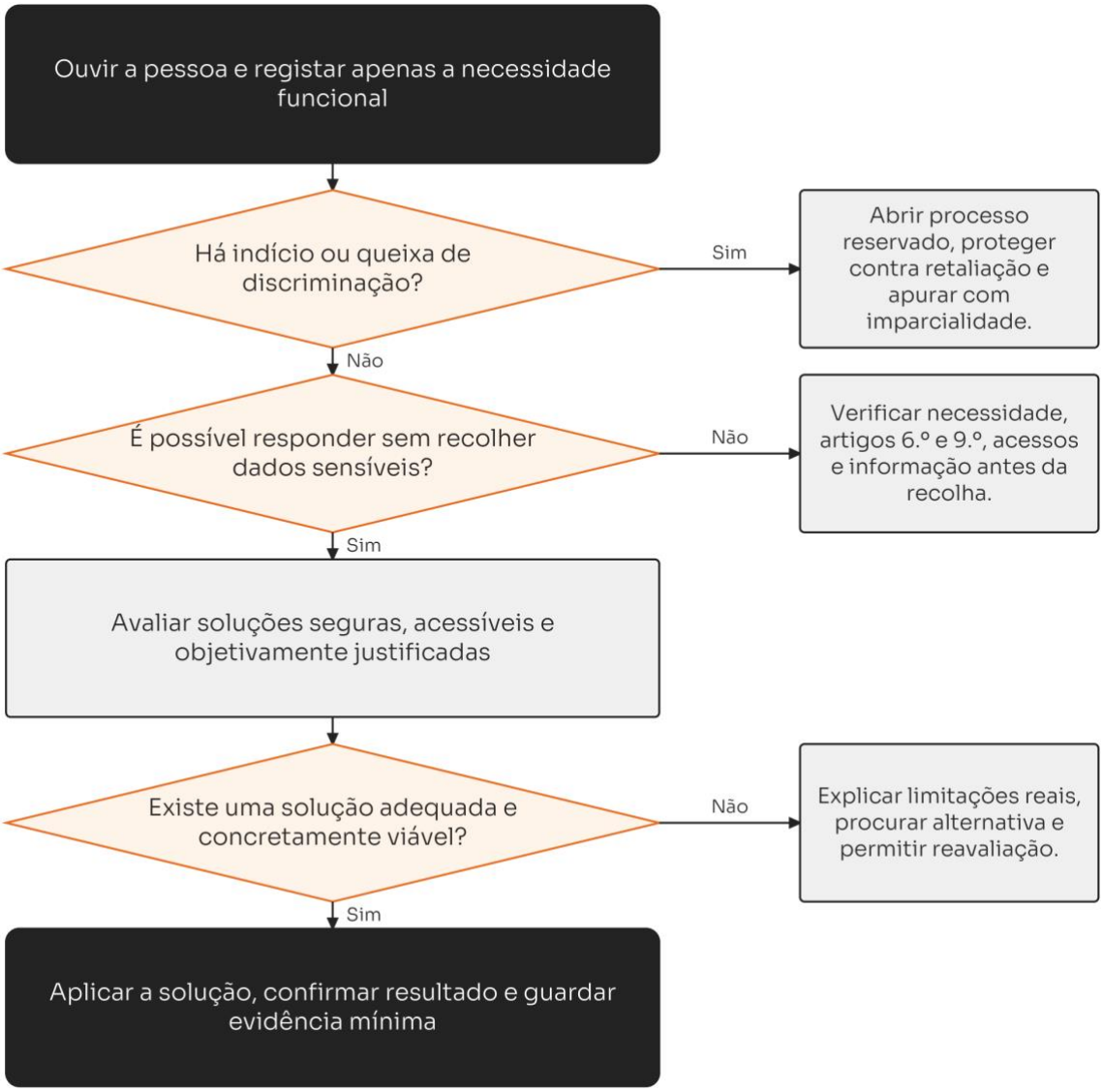
Para uma adaptação alimentar, registar a necessidade operacional — por exemplo, exclusão de determinado ingrediente — em vez de exigir a identificação da religião. Se o pedido envolver requisitos de preparação ou certificação religiosa, confirmar o que é efetivamente assegurado e explicar eventuais

limitações; não declarar uma refeição conforme com uma prática religiosa sem suporte verificável. A designação de uma dieta não dispensa controlo de alergénios nem autoriza divulgar a crença do utente.

Gestores, RH, Compras, Nutrição e responsáveis de unidade asseguram a aplicação. A formação inclui situações de discriminação direta e indireta, estereótipos, comunicação respeitosa, gestão de pedidos culturais/religiosos e proteção dos dados associados. A avaliação de fornecedores inclui compromisso equivalente no serviço prestado. O acompanhamento usa queixas, revisão de decisões e testes de acessibilidade; indicadores por características protegidas só são criados após análise específica da licitude e do risco. O Anexo 19 documenta a resposta e a verificação.

## Fluxograma 7  Diversidade e não discriminação

Respeitar raça, etnia, cor da pele, tradições, cultura e religião sem criar cadastros desnecessários.




**Quem atua.** Gestor da unidade articula com RH ou Nutrição; Privacidade/Jurídico analisa dados sensíveis e conflitos.

**Aplicação.** A investigação da queixa segue em paralelo com a análise da necessidade. Após validar a licitude de dados sensíveis, retomar a avaliação de soluções. Não inferir religião ou etnia pela aparência, nome ou dieta; fundamentar as decisões.

**Registos e referências.** Anexo 19. Manual, secção 3.6. RGPD, artigos 5.º, 6.º e 9.º; referenciais R3, R16 e R17.

## 4 Categorias de dados e titulares

| Categoria | Exemplos |
|---|---|
| Identificação e contacto | Nome, número de identificação, NIF, morada, telefone, correio eletrónico |
| Profissionais e laborais | Função, categoria, horários, desempenho, formação, assiduidade |
| Contratuais e financeiros | Contratos, faturação, pagamentos, dados bancários |
| Utilização e equipamento | IP, dispositivo, registos de acesso, eventos, credenciais |
| Imagem e segurança | CCTV, fotografia, controlo de acessos, registos de incidentes |
| Localização | IP aproximado, GPS, posição de viatura, percurso ou evento geográfico |
| Categorias especiais | Saúde, dados biométricos destinados à identificação inequívoca, filiação sindical e restantes categorias do artigo 9.º. |
| Conteúdos | Mensagens, formulários, ficheiros, pedidos e comunicações |

## 5 Finalidades e bases jurídicas

O tratamento de categorias especiais, incluindo dados de saúde, exige uma base do artigo 6.º e uma condição aplicável do artigo 9.º do RGPD. O interesse legítimo, por si só, não satisfaz esta segunda exigência. Dados sobre condenações e infrações penais exigem ainda o enquadramento do artigo 10.º. [R1]

A base jurídica é determinada por finalidade, e não por sistema ou formulário. O consentimento só será utilizado quando for livre, específico, informado, inequívoco e tão fácil de retirar como de prestar; no contexto laboral não deve ser adotado como solução automática devido ao desequilíbrio entre as partes.

| Finalidade típica | Base jurídica a avaliar | Evidência mínima |
|---|---|---|
| Execução de serviço ou contrato | Artigo 6.º, n.º 1, alínea b), quando o titular é parte no contrato; nos restantes fluxos, identificar fundamento próprio. | Contrato, pedido e especificação dos dados necessários |
| Faturação e obrigações fiscais | Obrigação jurídica | Norma aplicável e prazo legal |
| Gestão da relação laboral | Contrato, obrigação jurídica ou outro fundamento aplicável, conforme a finalidade e os limites laborais. | Processo de RH e informação ao trabalhador |
| Segurança de redes e sistemas | Interesse legítimo ou obrigação jurídica | Avaliação de interesse legítimo e política de registos de atividade |
| Marketing direto | Consentimento ou interesse legítimo quando admissível | Registo da opção e origem; verificar também a legislação sobre comunicações eletrónicas |
| Localização opcional numa aplicação | Consentimento, quando necessário | Aviso contextual e registo da escolha |
| Gestão de frota e proteção de ativos | Interesse legítimo ou outra base aplicável, após teste reforçado | Necessidade, proporcionalidade, informação e controlos |
| Defesa de direitos | Interesse legítimo e exercício de direitos | Registo do litígio e acesso restrito |

## 6 Transparência e recolha

A informação deve ser prestada no momento da recolha ou dentro do prazo legal quando os dados sejam obtidos de terceiros. Adota-se um modelo em camadas: aviso curto no ponto de contacto, resumo acessível e informação completa. O aviso deve identificar o responsável, finalidades, bases jurídicas, destinatários, transferências, prazos, direitos, contacto do encarregado e, quando aplicável, decisões automatizadas.

- Os formulários distinguem campos obrigatórios de opcionais e explicam as consequências da não prestação.
- As aplicações solicitam permissões no momento em que a funcionalidade é ativada, não de forma antecipada e genérica.
- Qualquer nova finalidade ou integração é analisada antes da reutilização dos dados.
- A informação dirigida a trabalhadores é separada da política externa quando os riscos e contextos diferem.

### 6.1 Dados recolhidos junto de terceiros e avisos por destinatário

Quando os dados não são obtidos diretamente do titular, acrescentam-se as categorias de dados e a sua origem, incluindo se provêm de fontes públicas. A informação é prestada em prazo razoável e, no máximo, em um mês; se houver comunicação com o titular, até à primeira comunicação; se se previr divulgação a outro destinatário, até à primeira divulgação. Aplica-se o momento mais cedo pertinente. Qualquer exceção do artigo 14.º, n.º 5, é individualmente fundamentada e acompanhada das salvaguardas devidas. [R1]

A ICA mantém avisos distintos para RH e recrutamento, utentes e representantes, contactos profissionais, visitantes/CCTV, geolocalização, canais digitais/marketing e denúncias. O manual interno não substitui esses avisos. O Anexo 10 define o conteúdo obrigatório e os módulos de adaptação. A divulgação do aviso não constitui consentimento e a assinatura de receção não autoriza finalidades adicionais.

## 7 Direitos dos titulares

Prazo de resposta: um mês a contar da receção. Quando necessário, tendo em conta a complexidade e o número de pedidos, o prazo pode ser prorrogado por mais dois meses, com comunicação fundamentada ao titular dentro do primeiro mês. A recusa deve indicar os motivos e os meios de reclamação e recurso. [R1, R4]

A organização assegura mecanismos acessíveis para o exercício dos direitos de acesso, retificação, apagamento, limitação, oposição, portabilidade, retirada do consentimento e proteção face a decisões exclusivamente automatizadas, nos termos aplicáveis.

| Etapa | Ação | Evidência |
|---|---|---|
| 1 Receção | Registar o pedido e confirmar canal | Número e data |
| 2 Identidade | Aplicar verificação proporcional ao risco | Método usado |
| 3 Triagem | Identificar direito, sistemas, responsáveis e eventuais exceções | Plano de resposta |
| 4 Execução | Pesquisar, bloquear, corrigir, exportar ou apagar | Registo técnico |
| 5 Resposta | Responder de forma clara dentro do prazo aplicável | Cópia da resposta |
| 6 Encerramento | Registar resultado e ações futuras | Processo encerrado |

### 7.1 Regras de execução por direito

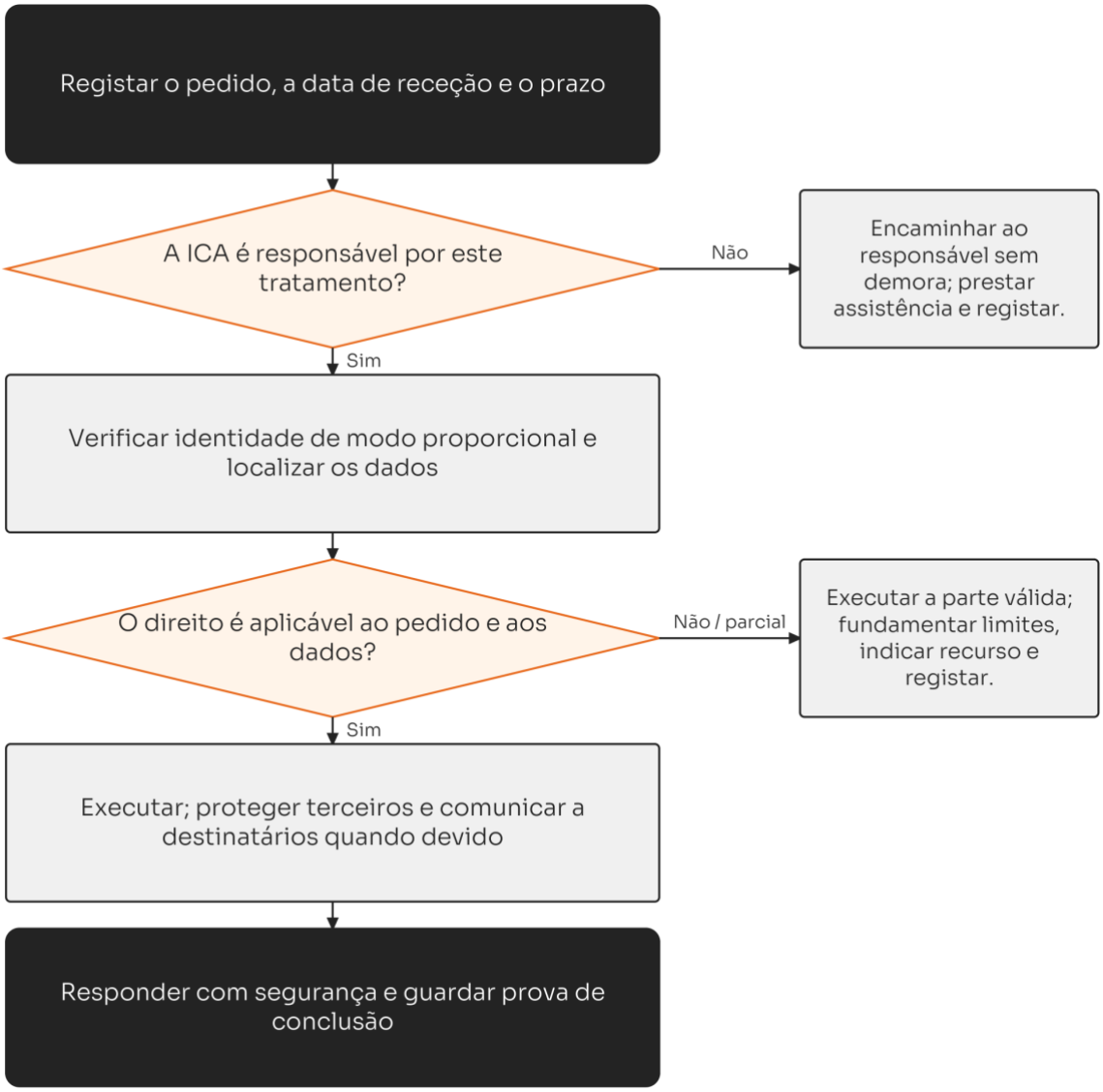
| Direito | Ação e limite a verificar |
|---|---|
| Acesso | Pesquisar dados e informação do artigo 15.º; entregar cópia inteligível e proteger direitos de terceiros por ocultação seletiva, sem recusa global automática. |
| Retificação | Corrigir dados inexatos e completar os incompletos; distinguir erro factual de opinião identificada como tal. |
| Apagamento | Eliminar quando se verifiquem os pressupostos; conservar apenas o que esteja abrangido por exceção legal fundamentada, com acesso restrito. |
| Limitação | Marcar e bloquear os dados abrangidos; comunicar antes de levantar a limitação e respeitar as condições do artigo 18.º. |
| Portabilidade | Aplica-se aos dados fornecidos pelo titular em tratamento automatizado baseado em consentimento ou contrato; usar formato estruturado, corrente e legível por máquina. |
| Oposição | Em interesse legítimo/interesse público, avaliar motivos imperiosos ou defesa de direitos; em marketing direto, cessar esse tratamento, incluindo perfis associados. |
| Retirada do consentimento | Disponibilizar canal tão simples como a adesão; cessar o tratamento abrangido sem afetar a licitude anterior e sem inventar uma base substitutiva. |
| Decisão automatizada | Verificar artigo 22.º, exceção admissível e salvaguardas; garantir intervenção humana efetiva, expressão do ponto de vista e contestação quando exigidas. |

Os pedidos são gratuitos, salvo condições excecionais do artigo 12.º, n.º 5, que a ICA deve demonstrar. Não se exige formulário obrigatório. Pedir identificação adicional apenas perante dúvidas razoáveis e na medida necessária; não guardar cópia integral do documento por rotina. Retificações, apagamentos e limitações são comunicados aos destinatários nos termos do artigo 19.º, salvo impossibilidade ou esforço desproporcionado fundamentados. O titular é informado desses destinatários se o solicitar. [R1, R4]

Se a ICA atuar como subcontratante, encaminha o pedido para o responsável sem demora injustificada e presta a assistência contratada; não decide por sua iniciativa sobre finalidades do cliente. Os pedidos recebidos em unidades, por telefone ou por qualquer trabalhador são encaminhados internamente no próprio dia útil, como meta operacional, mantendo a data original de receção.

## Fluxograma 2  Pedidos de exercício de direitos

Aplicar a pedidos de acesso, retificação, apagamento, limitação, oposição ou portabilidade.




**Quem atua.** Privacidade coordena; os responsáveis dos sistemas executam; o responsável pelo tratamento responde.

**Aplicação.** Responder em um mês. Prorrogação até mais dois meses apenas quando necessária, com motivo comunicado no primeiro mês. Não exigir formulário nem identificação excessiva.

**Registos e referências.** Anexos 5, 10 e 17. RGPD, artigos 12.º a 22.º. CNPD, Direitos dos titulares.

## 8 Conservação e eliminação

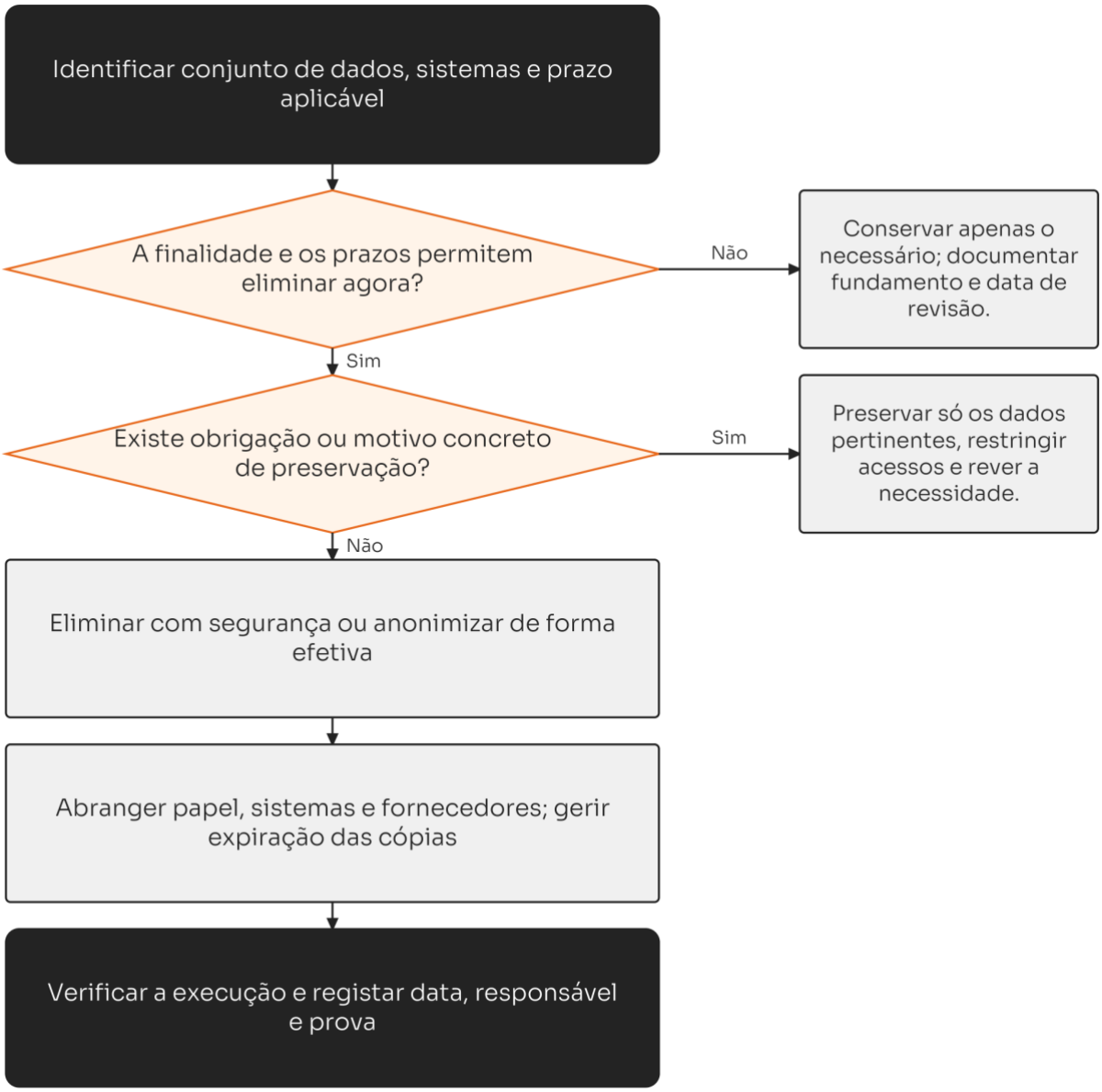
Cada prazo deve indicar uma duração concreta, o evento que inicia a contagem, o fundamento e o método de eliminação. Expressões como «prazo legal» ou «prazo curto» constituem instruções de preenchimento e não uma matriz de conservação concluída. O Anexo 8 permite documentar essa decisão.

Os prazos decorrem da finalidade, obrigação legal, necessidade operacional e risco para os titulares. Quando termine o prazo, os dados são apagados, destruídos com segurança ou anonimizados de forma efetiva. Uma ordem de preservação para litígio ou investigação suspende apenas a eliminação dos elementos relevantes.

| Conjunto | Regra consolidada | Responsável |
|---|---|---|
| Processos laborais | Prazo legal e contratual aplicável, com separação de saúde e disciplina | RH |
| Fiscal e faturação | Prazo legal aplicável | Financeira |
| Candidaturas | Prazo informado e limitado; renovação apenas com fundamento | RH |
| Registos de atividade de segurança | Prazo proporcional à deteção, investigação e defesa | TI e Segurança |
| CCTV | Prazo legal específico, salvo preservação justificada | Segurança |
| Localização pontual | Eliminar ou dissociar após a operação quando não seja necessária | Responsável do serviço |
| Histórico de percursos | Prazo curto, documentado por finalidade e sujeito a revisão | Frota ou Operações |
| Pedidos de direitos | Prazo necessário à prova do cumprimento e defesa | EPD ou Privacidade |

## Fluxograma 8  Conservação e eliminação de dados

Aplicar no fim do prazo, do serviço, da relação ou perante um pedido de apagamento válido.




**Quem atua.** O responsável de processo decide com Jurídico; TI e fornecedores executam; pessoa distinta verifica quando possível.

**Aplicação.** Não conservar todo o arquivo por existir um litígio. Após restauro, reaplicar supressões antes da utilização. A pseudonimização não equivale a anonimização; um pedido de apagamento exige análise das exceções legais.

**Registos e referências.** Anexos 8 e 17. RGPD, artigos 5.º, 17.º, 19.º e 28.º.

# B Ciclo de vida e procedimentos

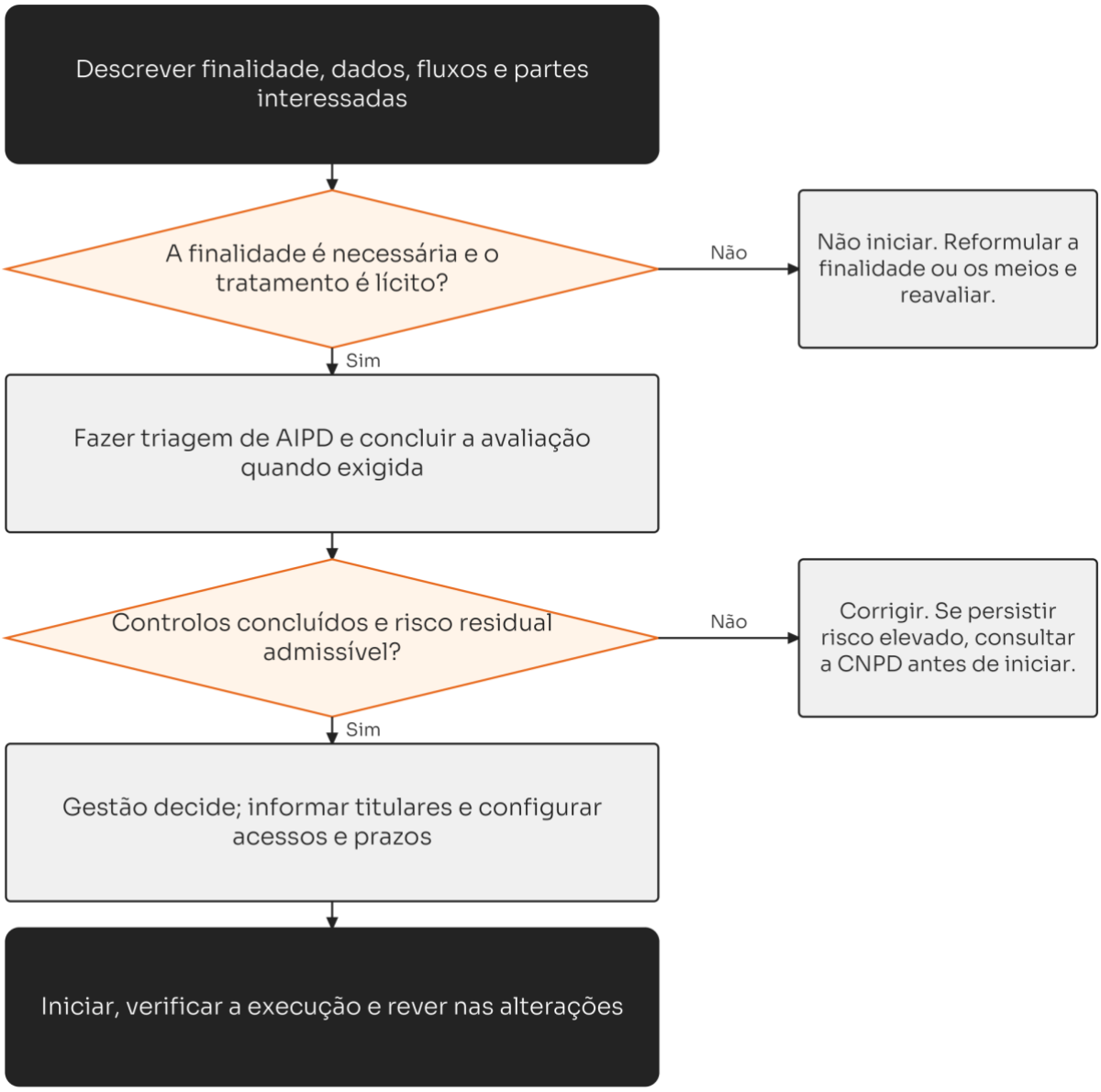
## 9 Proteção de dados desde a conceção

Todo o projeto, alteração de sistema, novo fornecedor, campanha, sensor ou funcionalidade que trate dados pessoais passa por uma avaliação prévia. O lançamento exige o cumprimento das condições legais e o fecho das ações críticas. A gestão pode aceitar apenas riscos residuais compatíveis com a lei; essa decisão não sana um tratamento ilícito nem substitui uma consulta prévia obrigatória à CNPD.

1. Descrever a finalidade, titulares, dados, fluxos e destinatários.
2. Confirmar base jurídica e compatibilidade com as expectativas do titular.
3. Reduzir dados, precisão, frequência, acessos e conservação.
4. Definir informação, exercício de direitos e configuração por defeito.
5. Avaliar segurança, fornecedores, transferências e continuidade.
6. Realizar triagem de avaliação de impacto e, quando necessário, uma AIPD completa.
7. Registar decisão, responsáveis, prazos e evidências de teste.

## Fluxograma 1  Novos tratamentos de dados

Antes de recolher dados ou alterar finalidades, sistemas, fornecedores ou destinatários.




**Quem atua.** Processo e Jurídico preparam; TI executa os controlos; Gestão decide. O EPD aconselha com independência.

**Aplicação.** A aprovação não sana ilicitude. A consulta prévia não é uma autorização automática: resolver as condições legais antes de iniciar.

**Registos e referências.** Anexos 1, 2, 3, 7, 9 e 13. RGPD, artigos 5.º, 6.º, 9.º, 25.º, 35.º e 36.º.

## 10 Registo das atividades de tratamento

Cada atividade dispõe de um registo atualizado com responsável, finalidades, categorias de titulares e dados, destinatários, transferências, prazos e medidas de segurança. O registo é revisto sempre que o processo, a tecnologia, o fornecedor ou a finalidade se altere.

### 10.1 Dois registos e ligação aos fluxos reais

Quando a ICA atua como responsável, mantém os elementos do artigo 30.º, n.º 1. Quando atua como subcontratante, mantém separadamente as categorias de atividades efetuadas por conta de cada responsável, os contactos das entidades, transferências e medidas de segurança, nos termos do n.º 2. Acrescenta, para gestão interna, bases jurídicas, sistemas, fonte, avisos, AIPD e contratos. Não invoca automaticamente a exceção para organizações com menos de 250 trabalhadores: esta não cobre, nomeadamente, tratamentos não ocasionais, de risco ou de categorias especiais. [R1]

## 11 Fornecedores e subcontratantes

| Fase | Controlo mínimo |
|---|---|
| Seleção | Diligência sobre segurança, localização dos dados, subcontratantes, incidentes e capacidade de apoiar direitos |
| Contrato | Instruções documentadas, confidencialidade, segurança, subcontratação, assistência, apagamento, auditoria e incidentes |
| Operação | Revisão de acessos, alterações, relatórios, certificados e subcontratantes posteriores |
| Saída | Devolução ou eliminação verificável, revogação de acessos e preservação apenas quando exigida |

### 11.1 Condições contratuais e verificação

O contrato de subcontratação identifica objeto, duração, natureza, finalidade, dados, titulares, obrigações e direitos do responsável. Prevê instruções documentadas, incluindo transferências; confidencialidade; segurança; condições de subcontratação ulterior; assistência aos direitos e aos artigos 32.º a 36.º; devolução ou eliminação, incluindo cópias, salvo conservação legal; informação e auditorias; e comunicação imediata de instrução considerada contrária ao RGPD. A mera cláusula genérica de confidencialidade não substitui estes elementos. [R1, artigo 28.º; R8] Articular ainda com a secção 13.6 para requisitos de cibersegurança e continuidade.

A autorização geral de subcontratação ulterior exige informação prévia de alterações e oportunidade real de oposição; a autorização específica identifica a entidade. As obrigações são transmitidas à cadeia e o subcontratante inicial mantém a responsabilidade perante o responsável nos termos legais. A avaliação usa evidências proporcionais: arquitetura, localização, testes, incidentes e capacidade de eliminação; uma certificação não dispensa verificar o serviço concreto. O Anexo 12 serve de guião contratual e de diligência.

## 12 Transferências internacionais

Antes de transferir dados para fora do Espaço Económico Europeu, a organização confirma a existência de decisão de adequação ou de outro mecanismo válido, avalia o contexto da transferência e aplica medidas suplementares quando necessário. A documentação identifica países, importadores, categorias de dados, mecanismo, avaliações e medidas técnicas ou contratuais.

### 12.1 Acesso remoto, mecanismos e avaliação do país terceiro

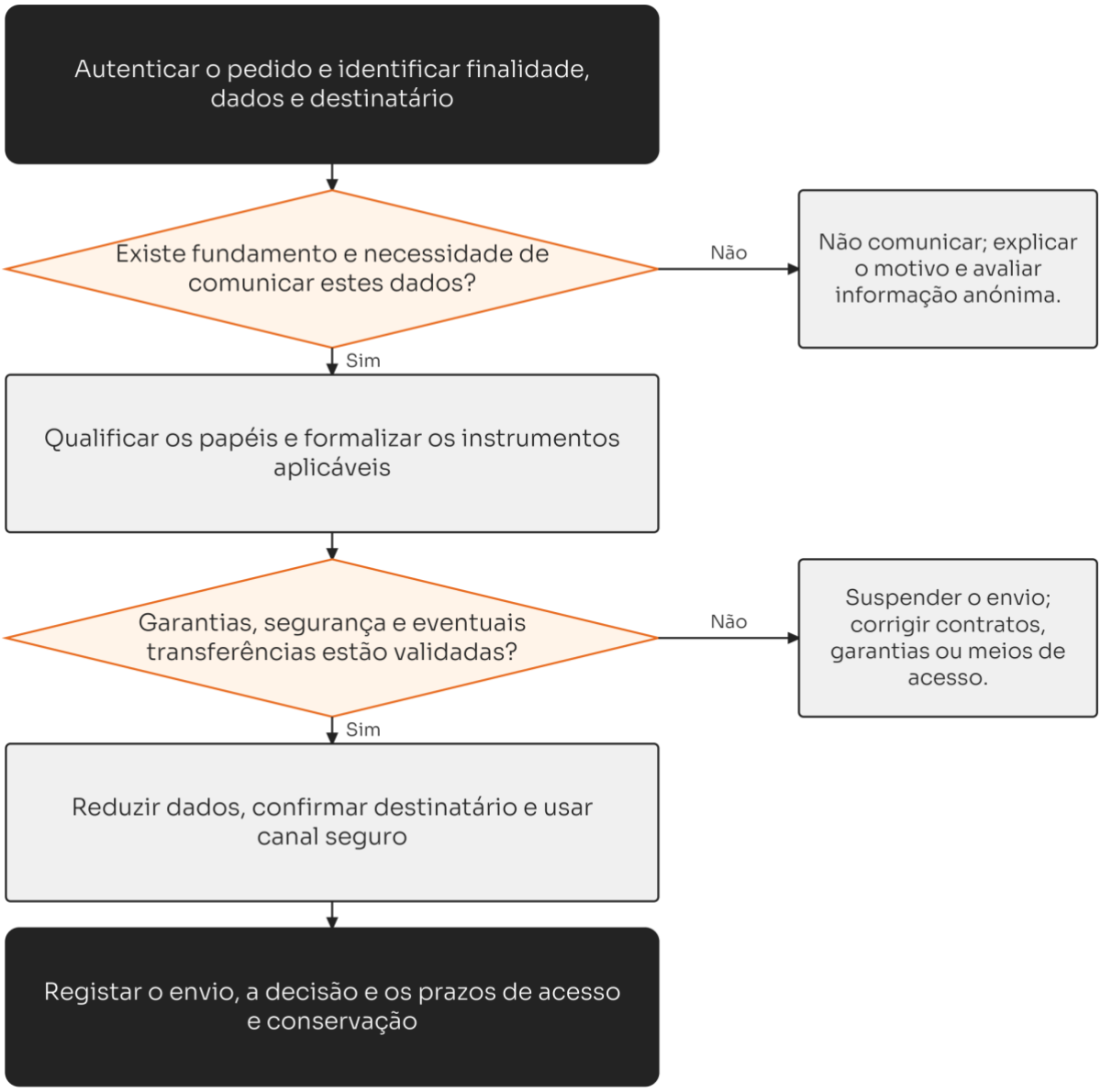
O mapa abrange alojamento, suporte remoto a partir de países terceiros, cópias, telemetria e subcontratantes ulteriores. Confirma-se se existe uma transferência na aceção do capítulo V. A localização

de um centro de dados no EEE não exclui acesso por outra entidade situada fora do EEE. Identificam-se exportador, importador, país, finalidade e mecanismo aplicável.

Quando se usam cláusulas contratuais-tipo, seleciona-se o módulo correto, completam-se anexos e avalia-se a eficácia no contexto real da transferência. Documentam-se legislação e práticas relevantes do país, medidas suplementares e possibilidade de suspensão. Uma decisão de adequação só é usada dentro do seu âmbito e enquanto vigente; as derrogações do artigo 49.º não são solução de rotina. Reavaliar em mudanças de fornecedor, país ou enquadramento. [R1; R14]

## Fluxograma 5  Partilha de dados com terceiros

Abrange clientes, fornecedores, auditores, autoridades e outros destinatários.




**Quem atua.** O gestor do processo verifica o pedido com Jurídico/Privacidade; TI assegura os meios técnicos.

**Aplicação.** Usar artigo 28.º para subcontratação e artigo 26.º para corresponsabilidade quando aplicáveis. Verificar capítulo V nas transferências internacionais. Se a ICA for subcontratante, seguir instruções documentadas, salvo obrigação legal. O contrato comercial não legitima qualquer acesso.

**Registos e referências.** Anexos 1, 9, 11 e 12. RGPD, artigos 5.º, 6.º, 9.º, 26.º, 28.º e 44.º a 49.º.

# 13 Segurança da informação

| Domínio | Controlos esperados |
|---|---|
| Identidades e acessos | Menor privilégio, MFA, segregação de funções, revisões e encerramento célere |
| Proteção técnica | Cifragem, gestão de chaves, configuração segura, correções, proteção de equipamentos terminais e redes |
| Registo e deteção | Registos de atividade protegidos, alertas, correlação e investigação |
| Resiliência | Cópias de segurança testadas, continuidade, recuperação e redundância adequada |
| Desenvolvimento | Requisitos de privacidade, testes, gestão de segredos e ambientes separados |
| Pessoas | Confidencialidade, formação, simulações e canais de reporte |
| Físico | Acessos, arquivo, destruição segura e proteção de equipamentos |

## 13.1 Regras para a operação diária

Os acessos são nominativos; contas partilhadas exigem exceção justificada e rastreabilidade equivalente. A admissão, mudança de função e saída desencadeiam revisão de permissões, dispositivos, chaves, caixas de correio e acessos de fornecedores. MFA é exigida nos acessos remotos e privilegiados sempre que tecnicamente disponível; exceções requerem controlos compensatórios, prazo e responsável.

Dados de utentes, saúde, trabalhadores e denúncias não circulam em contas pessoais, aplicações de mensagens ou dispositivos não aprovados. O envio externo exige confirmação do destinatário, limitação do conteúdo e proteção adequada. Proibir listas públicas de alergias, fotocópias abandonadas, palavras-passe visíveis e utilização de dados reais em testes sem avaliação e proteção equivalentes.

As cópias de segurança têm cifragem, acesso restrito, ciclo de expiração e testes de restauro. Uma reposição não pode reativar dados cuja eliminação ou limitação já tenha sido determinada: reaplica-se o registo de supressões antes da utilização. Anonimização é verificada quanto ao risco de reidentificação; pseudonimização mantém a natureza pessoal dos dados.

## 13.2 Cibersegurança e enquadramento NIS2

A ICA articula a proteção de dados pessoais com a segurança das redes e dos sistemas que suportam a atividade. A NIS2 é uma diretiva europeia, transposta em Portugal pelo Decreto-Lei n.º 125/2025. O Regulamento n.º 756/2026 concretiza o regime nacional e aprova o Quadro Nacional de Referência para a Cibersegurança. [R18–R20]

O RGPD mantém-se aplicável aos tratamentos de dados pessoais, independentemente do enquadramento NIS2. A gestão de cibersegurança abrange também informação não pessoal, disponibilidade de sistemas e continuidade do serviço. A AIPD avalia riscos para as pessoas; a análise de cibersegurança avalia ativos, ameaças e impactos operacionais, devendo ambas comunicar entre si.

| Natureza do requisito | Regra de aplicação |
|---|---|
| Obrigação legal | Identificar diploma, artigo, entidade abrangida, produção de efeitos e evidência. Não declarar cumprimento apenas pela aprovação do manual. |
| Requisito contratual | Registar cliente, cláusula, serviço, prazo e responsável. Um contrato pode exigir segurança sem transformar o fornecedor em entidade abrangida pela NIS2. |
| Medida interna | Aprovar controlos proporcionais ao risco, mesmo fora do âmbito NIS2; identificar exceções, medidas compensatórias e data de revisão. |

### 13.3 Avaliação de aplicabilidade à ICA

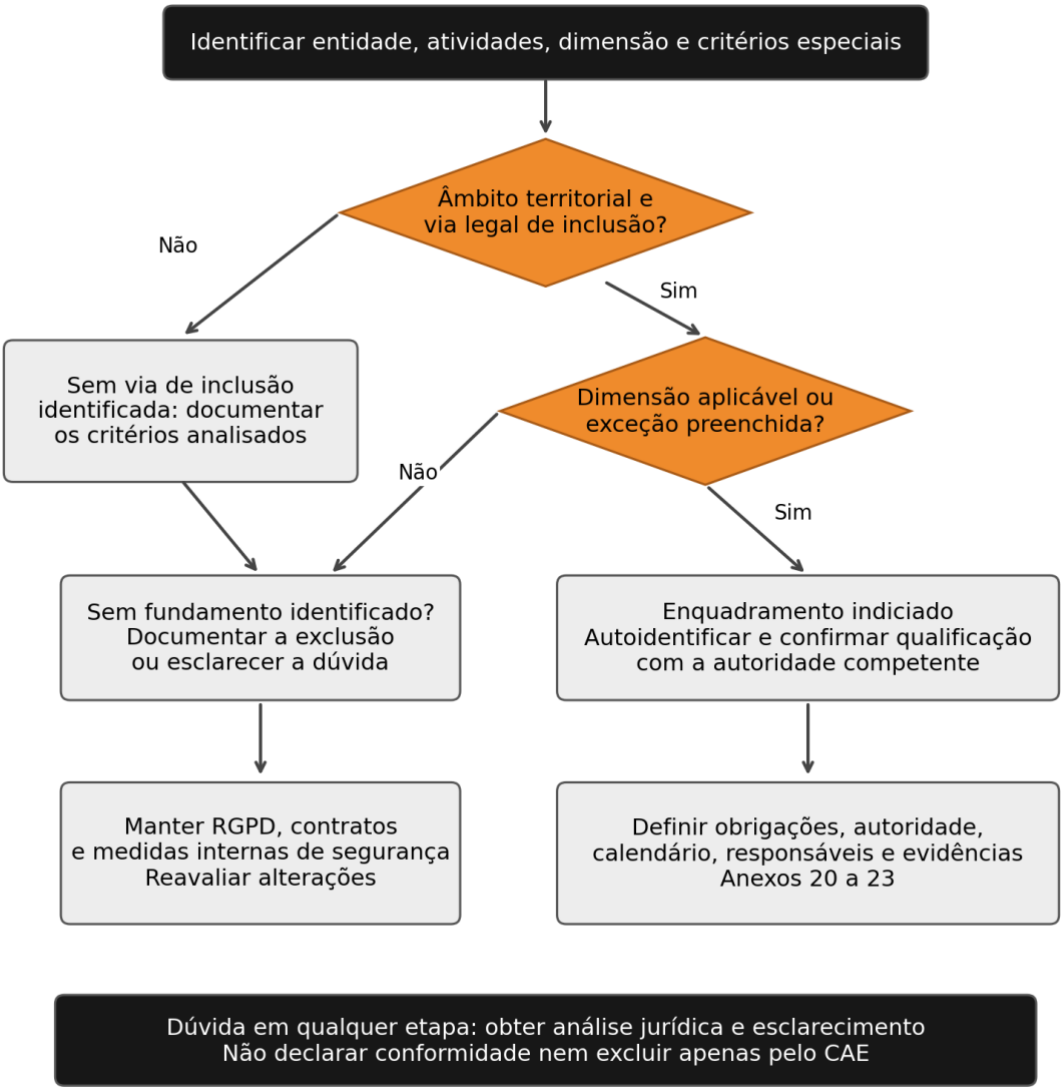
Jurídico, Administração, Financeira e Operação preenchem o Anexo 20 por entidade jurídica. Verificam atividades reais, CAE como elemento auxiliar, estabelecimento, dimensão e relações de grupo, critérios especiais e eventual identificação como entidade crítica. A expressão restauração coletiva, por si só, não decide a inclusão ou a exclusão.

O anexo II do regime nacional abrange empresas alimentares dedicadas à distribuição por grosso e à produção e transformação industriais. Confirmar se alguma operação da entidade corresponde a esse âmbito, incluindo unidades centrais de produção quando pertinente, sem presumir que toda a preparação de refeições é industrial. O fornecimento a hospitais ou escolas não torna automaticamente a ICA prestador de cuidados de saúde ou entidade pública. [R19, artigos 3.º a 8.º e anexos II e III]

Quando o enquadramento seja indiciado, verificar a autoidentificação, a qualificação pela autoridade competente e os deveres associados. O resultado de um simulador é auxiliar e não substitui a decisão da autoridade nem a autoidentificação obrigatória. A falta de dados é registada como por confirmar, com responsável e prazo de resolução. [R20, artigos 4.º e 8.º a 11.º]

## Fluxograma 9  Aplicabilidade do regime de cibersegurança

Utilizar antes da decisão de enquadramento e sempre que mudem as atividades, a dimensão, o grupo ou a qualificação da entidade.




Quem atua. Jurídico coordena a análise; Financeira e Operação comprovam os factos; Administração valida a posição interna. A qualificação administrativa compete à autoridade competente.

Registos e referências. Anexo 20. R19, artigos 3.º a 8.º; R20, artigos 4.º e 8.º a 11.º. Este fluxograma é uma triagem e exige a análise de todos os critérios legais.

## 13.4 Governação e calendário de cumprimento

A Administração atribui recursos, aprova as medidas e supervisiona a sua execução. A função de cibersegurança coordena riscos, inventário, incidentes e recuperação. O EPD mantém funções de aconselhamento e monitorização independentes; a acumulação com responsabilidades de decisão técnica exige avaliação de conflitos. [R18, artigo 20.º; R19, artigos 25.º, 31.º e 32.º]

| Função | Responsabilidade e evidência |
|---|---|
| Administração | Decisões, recursos, formação e acompanhamento de desvios; designação de responsáveis e suplentes. |
| Cibersegurança e TI | Inventário, controlos, deteção, contenção, recuperação, contacto técnico e registos de incidentes. |
| Jurídico e Privacidade | Enquadramento, calendário por obrigação, contratos, avaliação RGPD e comunicações legais; consulta ao EPD. |
| DQAS e Nutrição | Avaliar impacto na segurança alimentar, validar instruções de dieta e aprovar condições operacionais de retoma. |
| Operação e gestores de unidade | Ativar alternativa segura, confirmar versões e identidade dos destinatários, reportar falhas e registar decisões. |
| Compras e gestores de contrato | Controlar fornecedores, acessos remotos, dependências, tempos de resposta, exportação e saída. |

À data desta revisão, o Decreto-Lei n.º 125/2025 e o Regulamento n.º 756/2026 estão em vigor. Contudo, o artigo 10.º, n.º 2, do decreto-lei difere a produção de efeitos de disposições identificadas para 24 meses após a publicação da regulamentação aí referida. O artigo 35.º do regulamento distingue ainda disposições dependentes de instruções técnicas. Não existe uma dispensa geral de cumprimento durante 24 meses. [R19; R20]

O Anexo 20 deve conter um calendário por obrigação: autoidentificação e qualificação; comunicações e contactos; medidas e níveis de conformidade; gestão de riscos; reporte anual quando devido; inventário de ativos publicamente acessíveis; notificações de incidentes. Jurídico confirma a norma, o evento inicial, a data exigível e as instruções técnicas aplicáveis, mantendo evidência da consulta. As obrigações de segurança do artigo 32.º do RGPD continuam a ser exigíveis.

## 13.5 Medidas operacionais e demonstração de eficácia

O inventário associa cada ativo ao serviço, responsável, fornecedor, dados tratados, localização, dependências e criticidade. Inclui sistemas de dietas, encomendas, rastreabilidade, RH, faturação, geolocalização, correio, redes, sensores e equipamentos ligados, quando existam. O Anexo 21 liga riscos, controlos e evidências.

| Domínio | Aplicação e prova mínima |
|---|---|
| Acessos e identidades | Contas nominativas, menor privilégio, autenticação multifator, contas administrativas separadas e revogação na saída; testar amostras e exceções. |
| Redes e equipamentos | Separar redes de convidados, administração e equipamentos operacionais; controlar acessos remotos e configurações; manter inventário e atualizações. |
| Vulnerabilidades e alterações | Classificar urgência segundo exposição e impacto; corrigir e testar; documentar adiamentos, compensações e prazo de fecho. |
| Dados e comunicações | Cifrar quando adequado, gerir chaves, limitar extrações e proteger canais; conservar registos técnicos apenas pelo prazo fundamentado. |
| Deteção e resposta | Proteger e sincronizar registos, configurar alertas, encaminhar suspeitas e testar a equipa e suplentes. Não usar registos de segurança para vigilância laboral indevida. |
| Cópias e recuperação | Manter cópias protegidas contra alteração pelo atacante, separadas das credenciais de produção; testar restauro e integridade e reaplicar eliminações. |
| Pessoas e instalações | Formar por função, controlar dispositivos e suportes, acesso físico e emergência; adaptar instruções a necessidades de acessibilidade. |
| Fornecedores e desenvolvimento | Avaliar cadeia, componentes, alterações e serviços em nuvem; testar exportação, recuperação, encerramento e eliminação. |

Estes controlos são uma base operacional. Quando a entidade esteja abrangida, mapear integralmente os requisitos e critérios de verificação do QNRCS e dos anexos II e III do Regulamento n.º 756/2026 para o nível de conformidade aplicável. A matriz interna não substitui a matriz regulamentar nem os respetivos critérios. [R20]

## 13.6 Fornecedores e partes interessadas

Acrescentar à diligência do Anexo 12: dependências críticas, subfornecedores, acesso privilegiado, canal de urgência, comunicação de incidentes, capacidade de recuperação e plano de saída. Registar separadamente as obrigações contratuais dos clientes e a sujeição legal de cada entidade. Integrar o CNCS ou a autoridade setorial competente no grupo 22 do mapa de partes interessadas.

## 13.7 Continuidade dos serviços de alimentação

A Operação e a DQAS definem, por serviço crítico, o tempo máximo tolerável de interrupção, o objetivo de recuperação e a perda de dados tolerável, com a TI e os clientes envolvidos. Estes objetivos são aprovados e testados; não se inventam valores universais. Para instruções alimentares, a recuperação deve assegurar exatidão e atualidade antes de permitir a entrega.

| Cenário | Resposta operacional segura | Condição de retoma |
|---|---|---|
| Sistema de dietas indisponível | Ativar cópia operacional controlada; confirmar versão, alterações recentes e fonte autorizada. Se não for possível confirmar a dieta, interromper a entrega afetada e obter solução segura validada por Nutrição. | Instruções reconciliadas e validadas; teste da correspondência refeição e utente. |
| Alteração maliciosa de alergénios | Isolar a origem, preservar histórico e impedir utilização de instruções duvidosas; contactar fonte autorizada e avaliar refeições já fornecidas. | Integridade comprovada e avaliação de segurança alimentar concluída. |
| Falha de sensores ou registos de frio | Acionar procedimento HACCP de medição alternativa, equipamento adequado e avaliação dos alimentos. | Medições e alarmes verificados; decisão DQAS sobre produtos afetados. |
| Ransomware em sistemas centrais | Isolar sistemas afetados, usar contactos alternativos e processos manuais aprovados; não restaurar antes de conter a causa. | Restauro testado em ambiente controlado, acessos revistos e validação funcional. |
| Indisponibilidade da logística | Usar planeamento alternativo mínimo, confirmar entregas e proteger contactos e moradas. | Reconciliação de entregas e sincronização sem duplicação ou exposição. |

As cópias de contingência com dados pessoais ficam acessíveis apenas às funções necessárias, com data e versão visíveis, proteção física ou cifragem e substituição controlada. Após a retoma, reconciliar alterações efetuadas durante a falha e eliminar duplicados nos termos aprovados. O Anexo 23 documenta ativação, decisões, ensaio e retoma.

### 13.8 Exercícios e acompanhamento

Realizar exercício integrado com TI, Operação, DQAS, Privacidade, Jurídico e fornecedor crítico, abrangendo indisponibilidade do sistema de dietas e possível violação de dados. A periodicidade anual é uma proposta interna, sem afastar exigências regulamentares. Medir tempo de deteção e escalada, êxito do restauro, cumprimento dos objetivos aprovados, notificações devidas e fecho de ações. Reportar resultados e desvios à Administração.

# 14 Violações de dados pessoais

O responsável pelo tratamento notifica a CNPD sem demora injustificada e, sempre que possível, até 72 horas após ter conhecimento da violação, salvo se esta não for suscetível de gerar risco para os direitos e liberdades. Qualquer atraso é fundamentado. O subcontratante comunica ao responsável sem demora injustificada. [R1, R5]

Se for provável um risco elevado, os titulares são informados sem demora injustificada, sem prejuízo das exceções do artigo 34.º do RGPD. Todas as violações e as decisões de notificar ou não notificar ficam documentadas. A aprovação interna das comunicações não pode comprometer os prazos legais. [R1, R5]

Qualquer suspeita é comunicada imediatamente ao canal [CONTACTO DE INCIDENTES]. A equipa contém o incidente, preserva evidência, determina dados e titulares afetados, avalia probabilidade e gravidade do risco, documenta a decisão e notifica a autoridade e os titulares quando os critérios legais se verifiquem. Aplicar também as secções 14.2 e 14.3 e o Anexo 22 para avaliação de cibersegurança.

| Momento | Pergunta de controlo |
|---|---|
| Deteção | O que ocorreu, quando e como foi descoberto? |
| Contenção | Como interromper exposição, perda ou alteração sem destruir evidência? |
| Avaliação | Que dados, titulares, volume, contexto e consequências estão envolvidos? |
| Decisão | Existe risco ou risco elevado para os direitos e liberdades? |
| Comunicação | Quem deve ser notificado, por que canal e em que prazo? |
| Melhoria | Que causa raiz e ação corretiva impedem recorrência? |

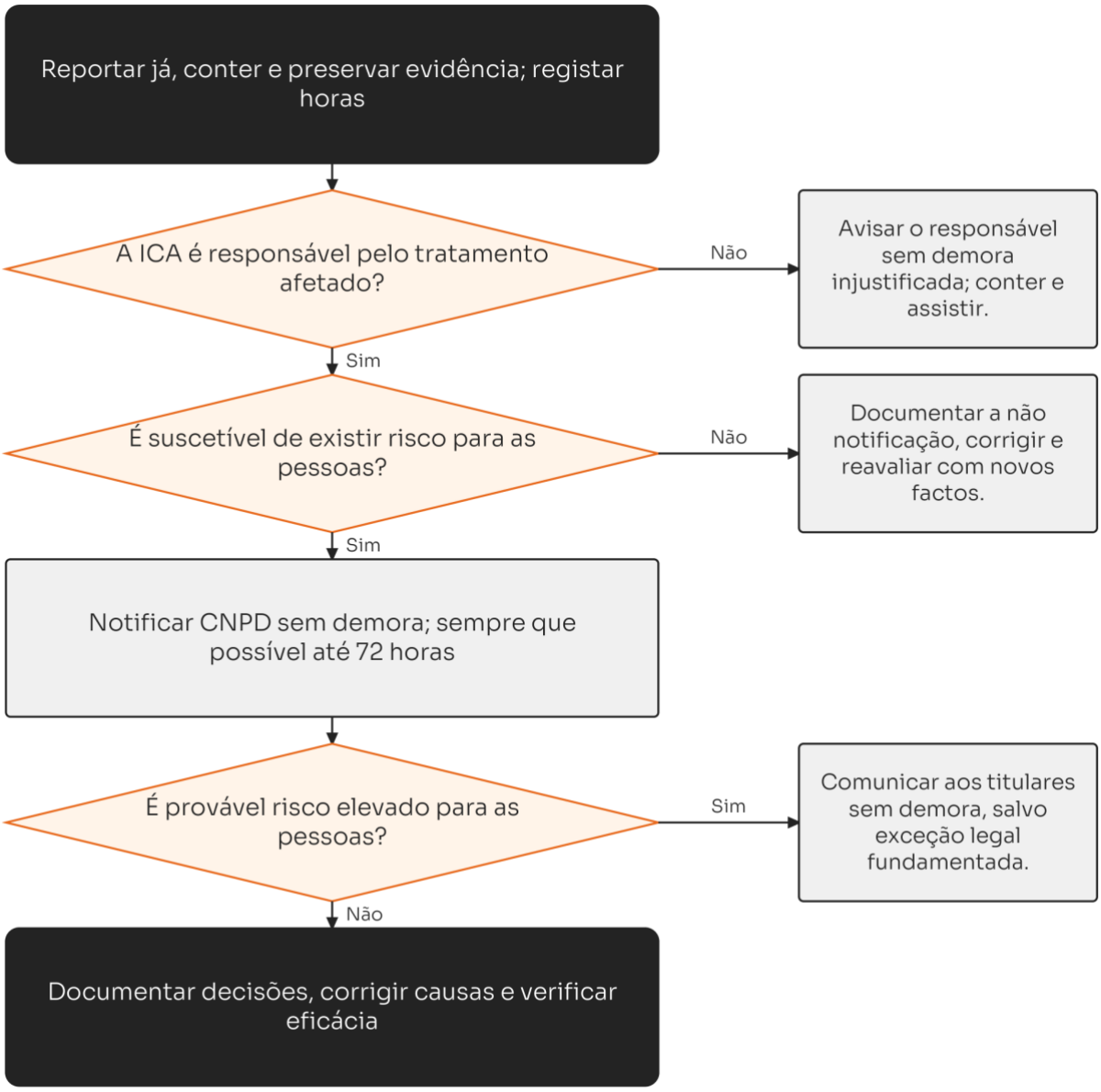
## 14.1 Decisão, continuidade e comunicação

Uma violação pode afetar confidencialidade, integridade ou disponibilidade, mesmo sem divulgação externa. Em alimentação coletiva, a indisponibilidade ou alteração de instruções de dieta pode também criar risco físico para o utente. Ativa-se o procedimento de continuidade com a última instrução validada e um interlocutor autorizado, evitando soluções improvisadas que exponham dados.

O registo distingue deteção, momento em que o responsável tomou conhecimento e subsequentes decisões. A contagem de 72 horas não aguarda o relatório técnico final; pode haver notificação faseada, com informação adicional sem demora injustificada. Registar natureza da violação, categorias e número aproximado de titulares e registos, contacto, consequências prováveis e medidas adotadas/propostas. A comunicação aos titulares usa linguagem clara e recomenda medidas concretas. [R1, artigos 33.º e 34.º; R5]

## Fluxograma 3  Violações de dados pessoais

Abrange perda, alteração, indisponibilidade, divulgação ou acesso indevido a dados.




**Quem atua.** TI contém; Privacidade e Jurídico avaliam; o responsável decide. Envolver o EPD quando designado.

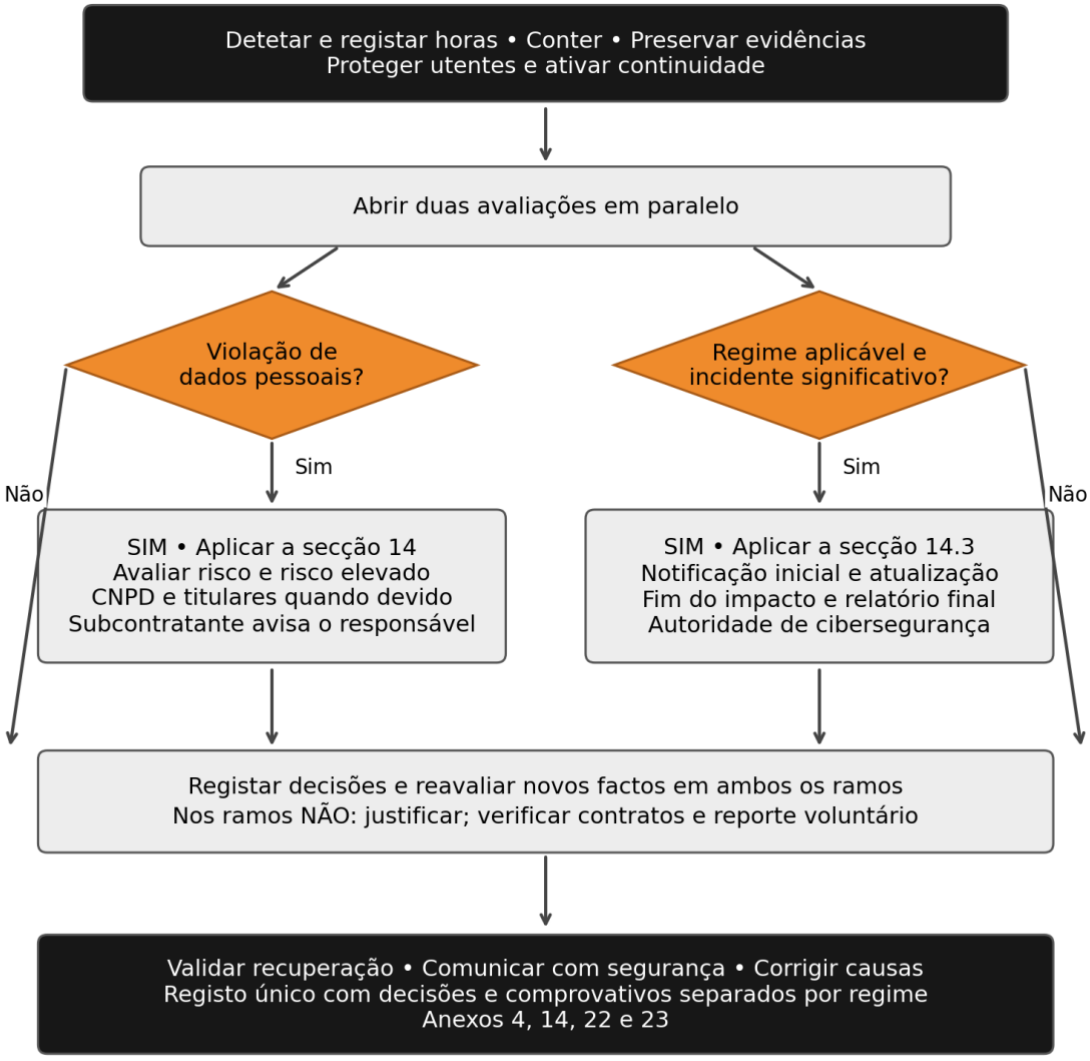
**Aplicação.** As 72 horas contam do conhecimento pelo responsável. Justificar atraso e notificar por fases se necessário. A comunicação aos titulares não espera pela CNPD. Após o ramo lateral, concluir o registo e as correções.

**Registos e referências.** Anexos 4 e 14. RGPD, artigos 33.º e 34.º. CNPD, Violação de dados.

## 14.2 Resposta integrada RGPD e cibersegurança

Abrir um registo único do incidente com duas avaliações autónomas. Uma falha pode ser uma violação de dados pessoais, um incidente de cibersegurança significativo, ambos ou nenhum dos dois. A falta de divulgação não exclui violação de disponibilidade ou integridade. A classificação de risco para as pessoas não é substituída pelo impacto económico no serviço.

Registar separadamente a deteção, o conhecimento da violação pelo responsável pelo tratamento e a verificação de que existe ou possa vir a existir um incidente significativo. Avaliar o número de utilizadores afetados, duração, gravidade da perturbação, impacto económico e social e critérios técnicos aplicáveis. Preservar evidência com integridade, registo de acessos e cadeia de custódia proporcional. [R1; R19, artigo 40.º; R20, artigo 20.º]




Fluxograma 10 Avaliação paralela e resposta ao incidente

Quem atua. TI contém; Operação e DQAS protegem a continuidade e os utentes; Privacidade e Jurídico avaliam deveres; responsáveis designados notificam sem aguardar reuniões que comprometam os prazos.

## 14.3 Notificações e controlo dos prazos

A tabela aplica o RGPD e o regime português de cibersegurança. As comunicações de cibersegurança pressupõem entidade abrangida e incidente sujeito a notificação obrigatória. Manter as avaliações e os comprovativos separados, mesmo quando exista um canal interoperável. [R1; R19, artigos 40.º a 44.º; R20, artigos 17.º e 20.º]

| Comunicação | Prazo e evento de contagem |
|---|---|
| RGPD ao responsável pelo tratamento | A ICA, quando subcontratante, comunica sem demora injustificada após conhecimento da violação; não aguarda a avaliação final do cliente. |
| RGPD à CNPD | Sem demora injustificada e, sempre que possível, até 72 horas após conhecimento pelo responsável; salvo se não for suscetível de gerar risco. Fundamentar atraso e completar por fases. |
| RGPD aos titulares | Sem demora injustificada, se provável risco elevado, sem prejuízo das exceções do artigo 34.º. |
| Cibersegurança inicial | Sem demora injustificada e até 24 horas após verificar que existe ou possa vir a existir incidente significativo; ressalva legal de incompatibilidade com mitigação ou resolução, a documentar. |
| Cibersegurança atualização | Quando necessário, até 72 horas após a verificação do incidente significativo, com avaliação de gravidade, impacto e indicadores disponíveis. |
| Cibersegurança fim do impacto | Sem demora injustificada e até 24 horas após o fim do impacto significativo. |
| Cibersegurança relatório final | Até 30 dias úteis após a notificação do fim do impacto significativo; atender a pedidos de relatórios intercalares nos termos do artigo 44.º. |
| Clientes e outros destinatários | Cumprir deveres legais e contratuais próprios; comunicar apenas informação necessária por canal seguro, sem substituir os destinatários legais anteriores. |

Exceção nacional. Se o incidente se resolver nas duas horas após a deteção, o artigo 41.º, n.º 2, prevê apenas a notificação de fim do impacto significativo no circuito de cibersegurança. Esta exceção não elimina obrigações RGPD. Registar os factos e o fundamento, incluindo a hora da resolução. Os prazos da tabela não são períodos de espera autorizados.

Usar a plataforma da autoridade competente e conservar o recibo. Em indisponibilidade técnica que impeça aguardar, aplicar o canal alternativo previsto no artigo 17.º do Regulamento n.º 756/2026, com contactos oficiais previamente confirmados. Não presumir que uma notificação ao CNCS foi recebida pela CNPD: confirmar destinatário, conteúdo e comprovativo de cada obrigação.

Registar decisões e comprovativos no Anexo 22. A investigação prossegue após o reporte inicial; o fecho exige validação técnica e operacional e ações corretivas verificadas.

## 15 Avaliação de impacto sobre a proteção de dados

A triagem verifica também a lista obrigatória do Regulamento n.º 798/2018 da CNPD. O rastreio de localização que permita avaliar ou classificar pessoas pode estar abrangido pelo n.º 5 dessa lista, nos termos e com a exceção aí previstos. Se, após as medidas previstas, persistir risco elevado, é obrigatória a consulta prévia à CNPD antes do tratamento. [R6, R7]

A AIPD é realizada antes de tratamentos suscetíveis de implicar elevado risco. A triagem considera, entre outros fatores, monitorização sistemática, observação de trabalhadores, localização contínua, grande escala, dados sensíveis, pessoas vulneráveis, cruzamento de bases, novas tecnologias, perfis e decisões com efeito significativo.

| Resultado da triagem | Decisão |
|---|---|
| Sem obrigação de AIPD identificada e sem indícios de risco elevado | Registar a triagem e implementar os controlos |
| Dúvida razoável ou múltiplos critérios | Realizar AIPD antes do lançamento |
| Risco elevado residual | Reformular o tratamento; se o risco elevado residual persistir, consultar previamente a CNPD antes de iniciar o tratamento |

# C Política específica de geolocalização

## 16 Princípio de utilização

A organização utiliza a localização menos precisa, menos frequente e durante o menor período que permita cumprir a finalidade. A geolocalização não é um objetivo autónomo: é uma operação de tratamento que deve provar necessidade, adequação e proporcionalidade.

Regra de decisão: se a finalidade puder ser atingida por endereço introduzido, zona, evento pontual, quilometragem, estado da tarefa ou outro meio menos intrusivo, não será criado um histórico contínuo de movimentos.

## 17 Níveis de localização

| Nível | Descrição | Exigência |
|---|---|---|
| 1 Aproximada | País, região ou cidade inferidos, por exemplo, através do IP | Informação e minimização |
| 2 Declarada | Morada, destino, estabelecimento ou zona introduzidos pelo titular | Finalidade e conservação definidas |
| 3 Precisa | Coordenadas GPS, GNSS, Wi-Fi, Bluetooth ou tecnologia equivalente | Justificação específica e controlo reforçado |
| 4 Contínua ou histórica | Recolha repetida, tempo real ou sequência de deslocações | AIPD a avaliar, acesso restrito e retenção curta |

## 18 Finalidades admissíveis e utilizações proibidas

| Pode ser admissível, após avaliação | Utilizações a excluir nesta política |
|---|---|
| Planeamento logístico e atribuição de serviço | Vigilância da vida privada ou fora do período autorizado |
| Proteção de viaturas, equipamentos ou cargas | Controlo do desempenho profissional por vigilância à distância |
| Segurança de pessoas em tarefas de risco | Ativação silenciosa ou finalidade oculta |
| Navegação ou funcionalidade pedida pelo utilizador | Inferência de saúde, religião, sindicato ou vida íntima |
| Prova de execução quando necessária e proporcional | Conservação indefinida de percursos |
| Prevenção e investigação de incidente concreto | Comunicação indiscriminada a gestores ou clientes |

## 19 Geolocalização em contexto laboral

A proteção de pessoas e bens ou exigências específicas da atividade carecem de demonstração concreta. O planeamento de rotas não justifica automaticamente a recolha contínua de percursos individualizados. Aplicam-se os limites do artigo 20.º do Código do Trabalho e do artigo 28.º da Lei n.º 58/2019. [R2, R3]

A utilização laboral é especialmente intrusiva e deve respeitar o RGPD, a legislação nacional de execução, o Código do Trabalho e as orientações da CNPD. O consentimento do trabalhador não constitui, por

regra, a base preferencial. A organização documenta uma finalidade legítima distinta do controlo do desempenho profissional e demonstra que não existe alternativa igualmente eficaz e menos intrusiva.

- O sistema funciona apenas nos períodos e situações necessários à finalidade autorizada.
- Quando exista utilização privada permitida, deve existir modo privado ou mecanismo equivalente que impeça a recolha fora do serviço, salvo situação excecional legalmente fundamentada.
- O trabalhador recebe informação específica sobre tecnologia, precisão, frequência, finalidades, acessos, prazos, destinatários, exercício de direitos e consequências.
- O acesso nominal é reservado a funções expressamente autorizadas; consultas excecionais ficam registadas e sujeitas a revisão.
- É proibida a utilização de vigilância à distância para controlar o desempenho profissional. Quando os dados estejam abrangidos pelo artigo 28.º, n.os 4 e 5, da Lei n.º 58/2019, a sua utilização disciplinar depende das condições aí previstas para a utilização no âmbito de processo penal. Uma decisão interna ou a informação ao trabalhador não afastam estes limites.
- As estruturas representativas dos trabalhadores são informadas ou consultadas quando a lei aplicável o imponha; RH e Jurídico documentam o enquadramento, os destinatários, o momento e a resposta. [R3, R9]

## 20 Viaturas, dispositivos e aplicações

| Cenário | Configuração por defeito |
|---|---|
| Viatura de serviço sem uso privado | Ativação limitada ao serviço e finalidade documentada |
| Viatura com uso privado autorizado | Modo privado simples, visível e auditável |
| Telemóvel ou tablet | Permissão apenas durante utilização, salvo necessidade comprovada de segundo plano |
| Equipamento ou carga | Associar o identificador ao trabalhador apenas quando indispensável |
| Aplicação para cliente | Alternativa manual quando a precisão não seja necessária |
| Emergência | Acesso excecional, registado e sujeito a revisão posterior |

## 21 Acessos, conservação e prova

O acesso a dados de localização exige perfil nominal e finalidade operacional. O sistema regista utilizador, data, hora, objeto consultado e, quando aplicável, motivo. Relatórios agregados são preferidos sempre que permitam alcançar o objetivo. Os prazos concretos são aprovados na matriz de conservação e revistos pelo menos anualmente.

| Tipo | Orientação consolidada |
|---|---|
| Evento pontual | Eliminar ou dissociar após conclusão, salvo necessidade documentada |
| Posição em tempo real | Não conservar por defeito quando apenas a visualização atual é necessária |
| Percurso operacional | Conservar pelo prazo mínimo necessário à finalidade declarada |
| Incidente ou litígio | Preservar apenas o segmento relevante com ordem documentada |
| Dados agregados | Confirmar que a anonimização é efetiva e resistente à reidentificação |

## 22 Aviso antes da ativação

O aviso contextual deve surgir antes da primeira recolha precisa e sempre que a finalidade se altere. Modelo curto:

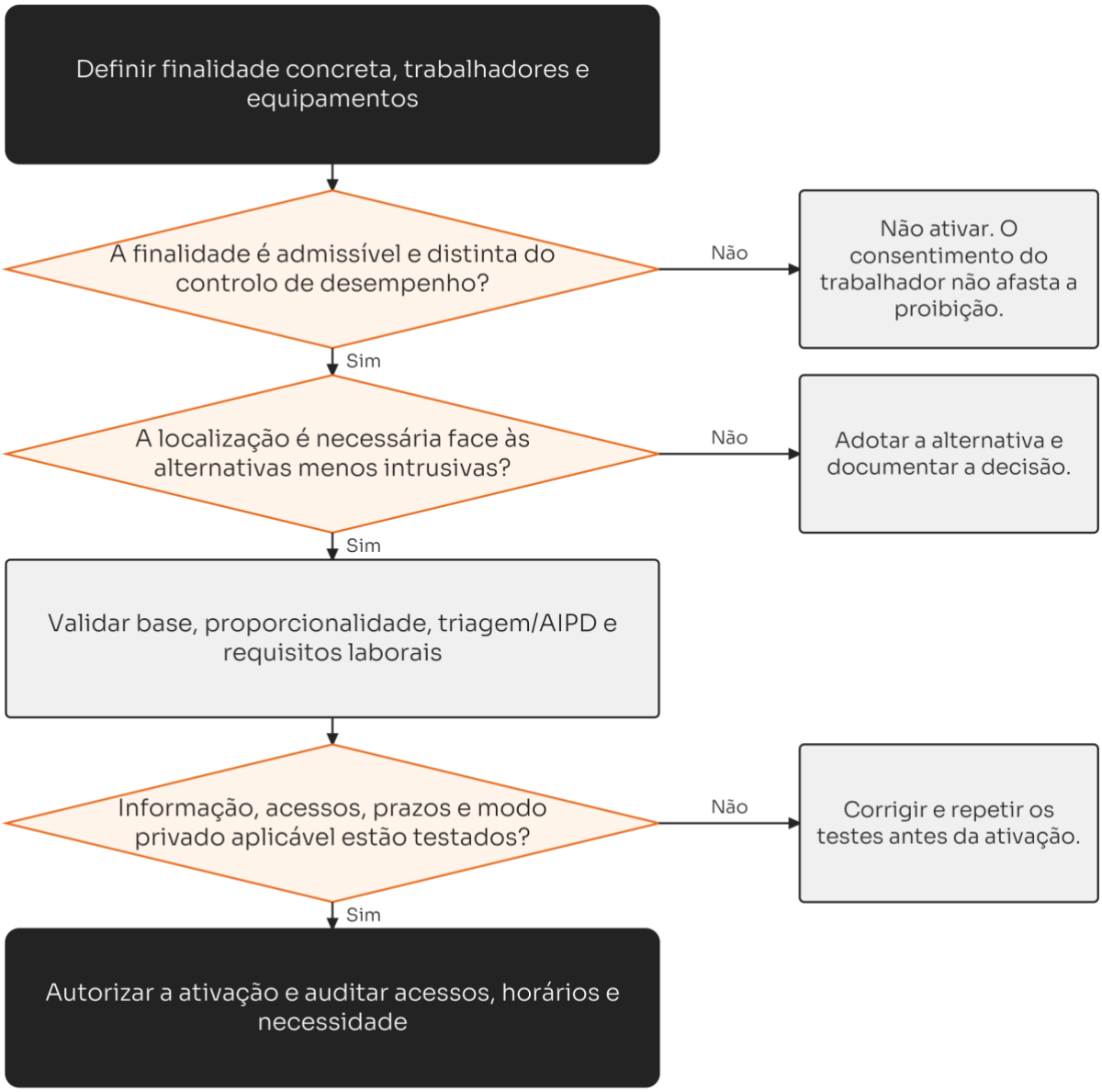
**Utilização da localização. Pretendemos utilizar [localização aproximada ou precisa] para [FINALIDADE], durante [PERÍODO OU FUNCIONAMENTO]. Conservamos os dados por [PRAZO] e partilhamos com [DESTINATÁRIOS OU NENHUNS]. Pode [RECUSAR, UTILIZAR ALTERNATIVA OU ATIVAR MODO PRIVADO], quando aplicável. Consulte a informação completa em [LIGAÇÃO OU CONTACTO].**

## 23 Lista de verificação de autorização

| Pergunta | Critério de aprovação |
|---|---|
| A finalidade é concreta? | Está escrita sem expressões genéricas como melhorar o serviço |
| É necessária localização? | A alternativa menos intrusiva foi testada e rejeitada com motivo |
| É necessária precisão? | A granularidade corresponde ao objetivo |
| É necessária continuidade? | A frequência está tecnicamente justificada |
| Existe base jurídica? | Foi validada por finalidade e categoria de titular |
| Há trabalhadores? | Foi realizada análise laboral específica |
| Há risco elevado? | A triagem de AIPD está documentada |
| O titular mantém controlo? | Existem informação, opção e canal de direitos adequados |
| A conservação é mínima? | Prazo, eliminação e preservação excecional estão configurados |
| Os acessos são controlados? | Perfis, registos de atividade e revisão estão ativos |

## Fluxograma 4  Geolocalização em contexto laboral

Aplicar antes da ativação e quando mudem a finalidade, a tecnologia ou a configuração.




**Quem atua.** Logística e RH justificam; TI configura; Jurídico valida; Gestão decide; EPD aconselha.

**Aplicação.** Limitar precisão e frequência. Impedir recolha fora do serviço quando não exista fundamento. Cumprir informação/consulta legalmente devida. Usos disciplinares exigem análise jurídica própria.

**Registos e referências.** Anexos 2, 6, 7, 8 e 13. Código do Trabalho, artigo 20.º; Lei n.º 58/2019, artigo 28.º.

# D Tecnologias digitais e contextos específicos

## 24 Inteligência artificial

Esta secção regula a proteção de dados no uso de IA. Antes da disponibilização de cada sistema, a análise jurídica deve identificar também as obrigações aplicáveis do Regulamento (UE) 2024/1689, em função do uso, do papel da organização e do calendário legal relevante.

A introdução de dados num sistema de inteligência artificial é uma operação de tratamento e não elimina as obrigações de privacidade. Antes da utilização, são avaliados o papel de cada interveniente, as condições contratuais, o destino dos dados, a conservação de instruções e conteúdos introduzidos, o uso para treino, os subcontratantes, as transferências, a segurança, a possibilidade de reidentificação e a intervenção humana.

- É proibida a introdução de dados pessoais, confidenciais ou de categorias especiais em ferramentas não aprovadas.
- As decisões com efeitos jurídicos ou impacto semelhante não devem basear-se exclusivamente em processamento automatizado sem fundamento e salvaguardas adequadas.
- Os resultados são verificados por pessoa competente antes de produzirem efeitos relevantes.
- Os dados de localização não são usados para inferir categorias sensíveis ou padrões pessoais incompatíveis com a finalidade declarada.
- O inventário de sistemas de IA identifica proprietário, fornecedor, versão, dados, finalidade, risco e controlos.

## 25 Cookies e tecnologias semelhantes

Os identificadores, pixels, armazenamento local e tecnologias semelhantes são inventariados e classificados. Os elementos estritamente necessários são separados dos opcionais. Quando o consentimento seja exigido, nenhuma tecnologia opcional é ativada antes da escolha, a recusa é tão acessível como a aceitação e as preferências podem ser alteradas a qualquer momento.

### 25.1 Comunicações comerciais, imagem e gravações

O envio de marketing eletrónico a pessoas singulares observa a Lei n.º 41/2004 e a orientação da CNPD. Verifica-se consentimento prévio ou a exceção legal para clientes, limitada aos seus pressupostos, incluindo produtos ou serviços próprios análogos e oposição simples e gratuita na recolha e em cada mensagem. Um endereço disponível na Internet ou uma lista comprada não prova autorização. A regra não se reduz a escolher «interesse legítimo» no RGPD. [R12]

Mantém-se lista mínima de supressão para evitar novo contacto após oposição, limitada a essa função. Fotografias, testemunhos, eventos e gravações de chamadas/reuniões têm finalidade, fundamento, destinatários e prazo próprios; publicidade externa não se presume incluída na presença num evento nem na relação laboral. Não gravar por mera conveniência quando bastem ata ou registo escrito.

## 26 Perfis e decisões automatizadas

Quando exista definição de perfis, a organização documenta dados utilizados, lógica geral, finalidade, consequências, base jurídica, exatidão, risco de discriminação, possibilidade de contestação e intervenção humana. Qualquer decisão exclusivamente automatizada abrangida pelo artigo 22.º do RGPD fica sujeita às condições e salvaguardas legais aplicáveis.

## 27 Formação, auditoria e melhoria

| Mecanismo | Periodicidade mínima proposta |
|---|---|
| Formação geral | Na integração e atualização anual |

| Mecanismo | Periodicidade mínima proposta |
|---|---|
| Formação por função | Antes de assumir acessos de risco e após mudanças relevantes |
| Revisão de acessos | Periódica e após mudança de função ou saída |
| Revisão do registo de tratamentos | Anual e após mudança material |
| Revisão de fornecedores | Segundo risco e antes de renovação |
| Teste de incidentes | Exercício periódico documentado |
| Política e matriz de conservação | Pelo menos anual ou após alteração legislativa/operacional |
| Geolocalização | Revisão anual de necessidade, precisão, acessos e prazos |
| Diversidade e não discriminação | Na integração e atualização por função; rever queixas, decisões e necessidades culturais/religiosas. |

## 28 Proteção de dados na alimentação coletiva

A segurança alimentar e a proteção de dados devem ser asseguradas no mesmo circuito. A minimização não pode retirar informação indispensável para evitar a entrega de uma refeição inadequada; deve eliminar a informação clínica e os destinatários que não são necessários. Um código de dieta não torna o registo anónimo se continuar associado a um utente.

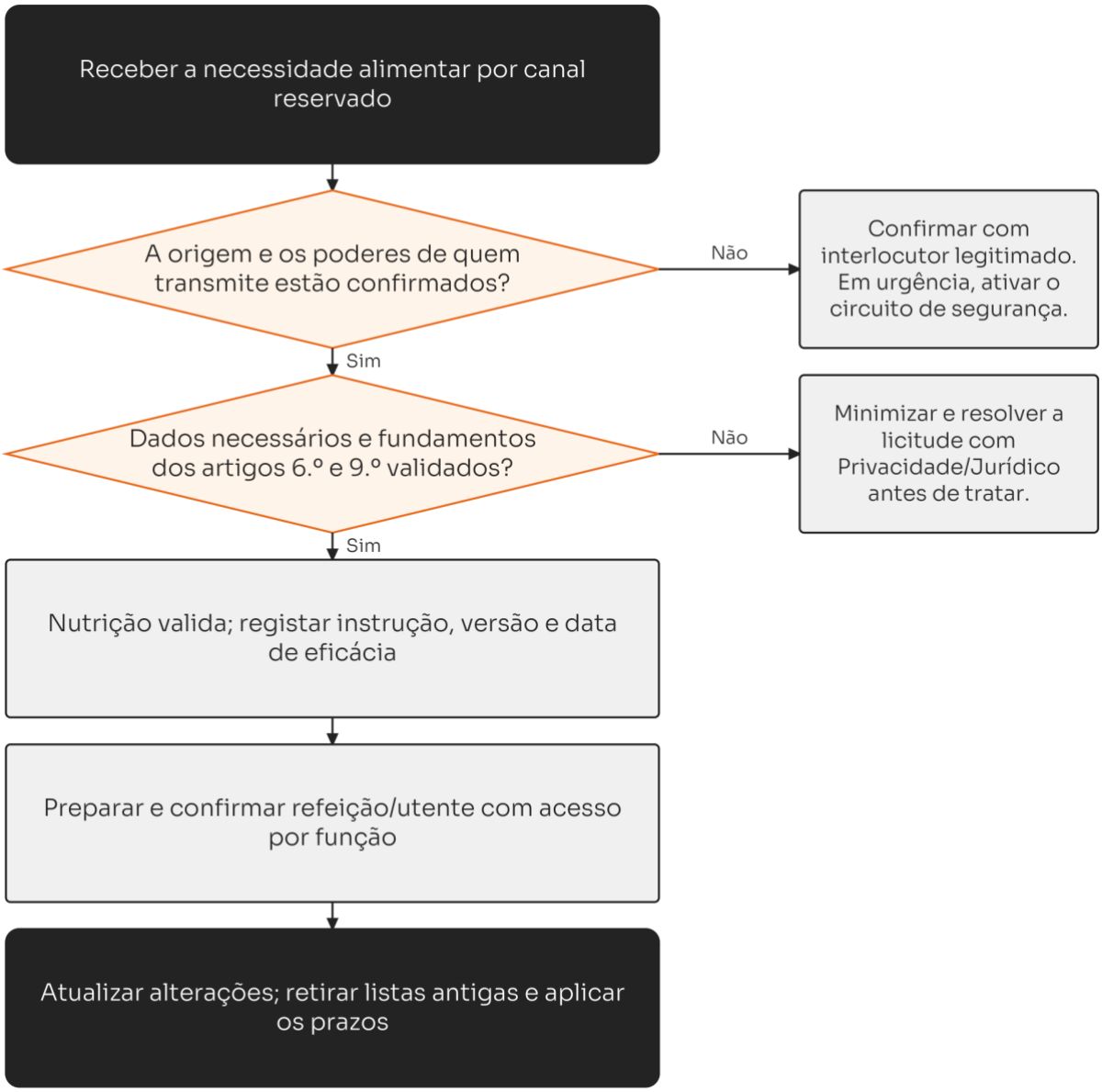
| Etapa | Regra obrigatória de organização | Evidência |
|---|---|---|
| Receber | Aceitar instruções por canal acordado; identificar entidade responsável, fonte autorizada e data de validade. | Registo de origem e versão da instrução. |
| Validar | Nutrição ou função competente esclarece ambiguidades com a fonte autorizada. Não inferir diagnóstico a partir de preferências. | Validação e dúvidas resolvidas. |
| Preparar | Equipa conhece restrições necessárias e identificador seguro; documentação clínica fica separada. | Lista operacional atual e perfis autorizados. |
| Entregar | Confirmar correspondência entre refeição e utente por procedimento definido, sem anunciar a condição de saúde. | Verificação proporcional ao risco. |
| Alterar | Registar quem solicitou e validou a alteração, momento de eficácia e retirada da versão anterior. | Histórico mínimo de alterações. |
| Encerrar | Retirar dados das listas ativas no termo do serviço; preservar apenas registos com necessidade e prazo fundamentados. | Registo de eliminação / arquivo restrito. |

Nos serviços escolares, hospitalares, sociais ou domiciliários, o contrato identifica quem informa os titulares, recebe prescrições, confirma representantes, atualiza dietas e responde a incidentes. A ICA não recebe automaticamente o processo clínico completo. Laboratórios e equipas de qualidade usam códigos e dados agregados quando a identificação não seja necessária; resultados nominativos de trabalhadores não integram relatórios gerais de cliente. Em indisponibilidade ou dúvida sobre a integridade das instruções, aplicar a secção 13.7 e o Anexo 23.

Os dados sobre alergias, intolerâncias e dietas terapêuticas exigem a condição do artigo 9.º adequada ao contexto. A exceção de cuidados de saúde não se aplica automaticamente a qualquer serviço de refeições: verificar finalidade, intervenientes e dever de sigilo. Dietas podem ainda revelar convicções religiosas; evitar registar a crença quando basta uma instrução alimentar. A regra dos 13 anos da lei portuguesa diz respeito ao consentimento para oferta direta de serviços da sociedade da informação, não a uma autorização geral para todos os tratamentos de menores. [R1; R2]

## Fluxograma 6  Dietas e instruções alimentares

Proteger os dados e assegurar que a refeição correta chega à pessoa certa.




**Quem atua.** Operação recebe e entrega; Nutrição valida; gestor do contrato articula com o cliente e os representantes.

**Aplicação.** Não expor listas de alergias nem exigir o processo clínico completo. O artigo 9.º aplica-se quando há categorias especiais. A condição de familiar não confere acesso automático; erros com dados seguem também o fluxo 3.

**Registos e referências.** Anexos 9, 10 e 15. Manual, secções 3.3 e 28. RGPD, artigos 5.º, 6.º e 9.º.

## 29 Relações laborais, vigilância e situações reservadas

| Situação | Regra operacional |
|---|---|
| Saúde ocupacional e incapacidade | Separar o circuito clínico dos RH e da chefia. Comunicar conclusões de aptidão e adaptações necessárias nos termos legais; diagnósticos e exames não são disponibilizados à chefia por rotina. Documentos para benefícios legais têm destinatários e acessos próprios. |
| Biometria | No contexto laboral, limitar ao controlo de assiduidade e de acessos às instalações, nos termos do artigo 28.º, n.º 6, da Lei n.º 58/2019. Demonstrar necessidade e proporcionalidade, usar representações não reversíveis e avaliar AIPD. O consentimento não afasta estes limites. [R1; R2] |
| CCTV | Delimitar áreas, ângulos, finalidades e acessos; informar antes da entrada; impedir captação de espaços de reserva e controlo de desempenho. Áudio é desativado salvo situação legalmente admissível fundamentada. Aplicar regime específico e prazo do Anexo 8. [R2; R3; R11] |
| Correio eletrónico, Internet e teletrabalho | Definir usos permitidos, continuidade e acessos excecionais, respeitando a reserva das comunicações pessoais. Não monitorizar permanentemente ecrã, teclado, câmara ou atividade doméstica. Investigação requer necessidade, escopo e análise jurídica. |
| Recrutamento e referências | Recolher só dados relevantes para a função; documentar testes, referências e fontes. Registo criminal só quando exista enquadramento legal. Diferenciar a obrigação de conservar o registo de recrutamento da retenção integral de todos os currículos. |
| Cessação e transição de prestador | Revogar acessos, devolver equipamentos e remover acessos a clientes. Transferir dados de trabalhadores apenas quando a regra laboral aplicável e a finalidade o permitam; não entregar o processo pessoal completo por defeito. |

A utilização de dados obtidos por vigilância em matéria disciplinar obedece aos limites legais; o manual não cria uma autorização de prova. O acórdão do Tribunal da Relação de Lisboa de 18 de junho de 2025, processo 2286/24.6T8FNC.L1-4, reafirma os limites do controlo de desempenho e da utilização de dados de GPS. É uma decisão relativa ao seu caso concreto, que reforça a necessidade de avaliação jurídica antes da reutilização. [R13]

## 30 Denúncias, auditorias e comunicações externas

O canal de denúncias mantém gestão e arquivo reservados, com pessoas autorizadas identificadas, proteção da identidade do denunciante, reserva dos visados e prevenção de retaliação. A aplicabilidade da Lei n.º 93/2021 é documentada. Nas denúncias internas abrangidas, comunica-se a receção até sete dias e as medidas previstas ou adotadas até três meses da receção; a informação sobre o resultado, quando requerida, segue o regime do artigo 11.º. Não confundir estes prazos com os dos direitos RGPD ou de notificação de violações. [R10]

Pedidos de acesso que envolvam denúncias, investigações ou terceiros são analisados individualmente. Protege-se a identidade e os direitos legalmente tutelados com expurgo proporcional; não existe dispensa geral de transparência ou acesso por chamar «confidencial» ao processo. Dados manifestamente irrelevantes para a denúncia são apagados sem demora nos termos legais. O registo segue o prazo específico do Anexo 8.

Auditores e clientes recebem evidência suficiente, preferindo amostras expurgadas, dados agregados e consulta controlada. Seguradoras, advogados, autoridades e bancos recebem apenas a parte necessária para a sua função. Qualquer pedido não previsto passa pelo Anexo 11: identidade e competência, finalidade, base jurídica, dados mínimos, canal, conservação e decisão. A urgência não legitima divulgação indiscriminada.

Na venda de ativos, reorganização, parceria ou alteração de operador, a diligência começa por informação anonimizada. Acesso nominativo requer fundamento, âmbito, compromissos, controlo de destinatários e avaliação da informação aos titulares. Incidentes alimentares ou de privacidade comunicados à imprensa são tratados por porta-voz autorizado, evitando identificar utentes, trabalhadores ou denunciantes sem necessidade e fundamento.

# E Anexos operacionais

Os instrumentos seguintes permitem transformar a política em decisões e evidências. Cada modelo é preenchido por tratamento ou ocorrência, com identificação do responsável, data e ligação aos documentos relevantes. Guardar os registos em acesso controlado; os formulários podem conter informação sensível.

| Quando utilizar | Instrumentos a articular |
|---|---|
| Iniciar ou alterar um tratamento | Anexos 1, 2, 7 e 9; AIPD no Anexo 13 e interesse legítimo no Anexo 3 quando necessários. |
| Contratar ou transmitir dados | Anexos 11 e 12; atualizar registo, avisos e transferências. |
| Informar e recolher escolhas | Anexos 10 e 16; não confundir informação com consentimento. |
| Responder a um pedido | Anexo 5; identificar responsável, dados, sistemas e prazo. |
| Gerir um incidente | Anexos 4 e 14; conter, avaliar, decidir e documentar. |
| Usar localização ou vigilância | Anexos 2, 6, 7 e 8; verificar regras laborais e testes antes da ativação. |
| Gerir dietas e representação | Anexo 15, fichas do Anexo 9 e regras da secção 28. |
| Acolher diferenças e resolver queixas | Secção 3.6 e Anexo 19; apoio acessível, decisão objetiva e proteção contra retaliação. |
| Encerrar e verificar | Anexos 8, 17 e 18; eliminação, cobertura e evidência de eficácia. |

## Regras de preenchimento

Substituir campos entre parênteses retos por dados verificados. Se não se aplicar, escrever «não aplicável» e o fundamento. Não deixar uma caixa vazia significar aprovação. Distinguir quem prepara, quem aconselha e quem decide; uma assinatura sem evidência não encerra a ação.

Num pedido urgente de direitos, incidente ou segurança alimentar, utilizar desde logo o canal operacional previsto. O preenchimento formal não pode atrasar a contenção, a resposta ou uma notificação legalmente devida.

## Anexo 1 Estrutura do registo de atividades de tratamento

| Campo | Preenchimento |
|---|---|
| Código e processo | [PREENCHER] |
| Responsável interno | [PREENCHER] |
| Finalidades | [PREENCHER] |
| Bases jurídicas | [PREENCHER] |
| Titulares | [PREENCHER] |
| Categorias de dados | [PREENCHER] |
| Origem | [PREENCHER] |
| Destinatários | [PREENCHER] |
| Sistemas e locais | [PREENCHER] |
| Transferências internacionais | [PREENCHER] |
| Conservação e eliminação | [PREENCHER] |
| Medidas de segurança | [PREENCHER] |
| Subcontratantes | [PREENCHER] |
| AIPD e teste de interesse legítimo | [PREENCHER] |
| Identificação e contactos das entidades | [RESPONSÁVEL, CORRESPONSÁVEIS, REPRESENTANTE E EPD QUANDO APLICÁVEL] |
| Registo como subcontratante | [CLIENTE RESPONSÁVEL, CATEGORIAS DE ATIVIDADES, CONTACTOS, TRANSFERÊNCIAS E SEGURANÇA] |
| Aviso / versão / canal | [IDENTIFICAÇÃO E PROVA DE DISPONIBILIZAÇÃO] |
| Última verificação | [DATA, RESPONSÁVEL E ALTERAÇÕES] |

## Anexo 2 Triagem de AIPD

Assinalar sim ou não e justificar. A presença de vários critérios, a intensidade do tratamento ou a vulnerabilidade dos titulares pode determinar uma AIPD mesmo sem regra numérica automática.

| Critério | Sim ou não | Justificação |
|---|---|---|
| Avaliação ou classificação de pessoas | [PREENCHER] | [PREENCHER] |
| Decisão automatizada com efeito significativo | [PREENCHER] | [PREENCHER] |
| Monitorização sistemática | [PREENCHER] | [PREENCHER] |
| Categorias especiais ou dados muito pessoais | [PREENCHER] | [PREENCHER] |
| Grande escala | [PREENCHER] | [PREENCHER] |
| Cruzamento de conjuntos | [PREENCHER] | [PREENCHER] |
| Pessoas vulneráveis ou trabalhadores | [PREENCHER] | [PREENCHER] |
| Nova tecnologia ou uso inovador | [PREENCHER] | [PREENCHER] |
| Impedimento do exercício de direito ou serviço | [PREENCHER] | [PREENCHER] |
| Localização precisa, contínua ou histórica | [PREENCHER] | [PREENCHER] |
| Lista obrigatória nacional / artigo 35.º, n.º 3 | [SIM/NÃO] | [FUNDAMENTO] |
| Decisão e parecer do EPD | [AIPD SIM/NÃO] | [DECISOR, DATA E FUNDAMENTO] |

## Anexo 3 Teste de interesse legítimo

Teste da finalidade: qual é o interesse legítimo, real, atual e lícito?

**[REGISTAR FUNDAMENTAÇÃO E EVIDÊNCIAS]**

Teste da necessidade: o tratamento é necessário ou existe alternativa menos intrusiva?

**[REGISTAR FUNDAMENTAÇÃO E EVIDÊNCIAS]**

Teste de ponderação: quais são as expectativas, impactos, vulnerabilidades e salvaguardas?

**[REGISTAR FUNDAMENTAÇÃO E EVIDÊNCIAS]**

Conclusão: o interesse prevalece, com que condições, revisão e possibilidade de oposição?

**[REGISTAR FUNDAMENTAÇÃO E EVIDÊNCIAS]**

## Anexo 4  Registo de violação de dados

| Campo | Registo |
|---|---|
| Data e hora da deteção | [PREENCHER] |
| Descrição factual | [PREENCHER] |
| Sistemas e dados | [PREENCHER] |
| Titulares e volume | [PREENCHER] |
| Causa provável | [PREENCHER] |
| Medidas de contenção | [PREENCHER] |
| Avaliação de risco | [PREENCHER] |
| Decisão de notificação | [PREENCHER] |
| Comunicações efetuadas | [PREENCHER] |
| Ações corretivas | [PREENCHER] |

### Prazos e decisão

Conhecimento pelo responsável: [DATA E HORA]  Limite de 72 horas: [DATA E HORA]
Fundamento de não notificação ou de atraso: [PREENCHER]
Decisor e comunicações aos titulares: [PREENCHER]

## Anexo 5  Pedido de exercício de direitos

| Campo | Registo |
|---|---|
| Titular e contacto | [PREENCHER] |
| Data e canal | [PREENCHER] |
| Direito exercido | [PREENCHER] |
| Verificação de identidade | [PREENCHER] |
| Sistemas consultados | [PREENCHER] |
| Responsáveis envolvidos | [PREENCHER] |
| Decisão e fundamento | [PREENCHER] |
| Data e conteúdo da resposta | [PREENCHER] |

### Controlo do prazo

Limite de resposta: [DATA]  Prorrogação comunicada em: [DATA]
Motivo e novo prazo: [PREENCHER]

## Anexo 6  Ficha de geolocalização

| Campo | Decisão documentada |
|---|---|
| Ativo, pessoa ou serviço | [PREENCHER] |
| Tecnologia e fornecedor | [PREENCHER] |
| Precisão e frequência | [PREENCHER] |
| Período de funcionamento | [PREENCHER] |
| Finalidade e base jurídica | [PREENCHER] |
| Alternativas avaliadas | [PREENCHER] |
| Perfis autorizados | [PREENCHER] |
| Prazo e método de eliminação | [PREENCHER] |
| Informação ao titular | [PREENCHER] |
| Modo privado ou mecanismo equivalente | [PREENCHER] |
| AIPD e parecer do EPD | [PREENCHER] |
| Data de revisão | [PREENCHER] |

## Anexo 7 Matriz de aprovação de novos tratamentos

| Tema | Responsável | Consulta | Evidência |
|---|---|---|---|
| Finalidade e necessidade | Responsável do processo | EPD | Ficha de projeto |
| Base jurídica | Jurídico ou Privacidade | EPD | Análise documentada |
| Segurança | TI e Segurança | EPD | Avaliação técnica |
| Fornecedor | Compras | Jurídico, TI e EPD | Diligência e contrato |
| AIPD | Responsável do processo | EPD | Relatório e plano |
| Aceitação de risco | Gestão competente | EPD e Segurança | Decisão formal |

### Decisão sobre o tratamento

Tratamento e referência do projeto: [PREENCHER]
Decisão e fundamento: [PREENCHER]
Condições a cumprir antes da entrada em produção: [PREENCHER]
Responsáveis e datas de conclusão: [PREENCHER]
Evidências verificadas: [PREENCHER]
Aprovação e data de revisão: [PREENCHER]

## Anexo 8 Matriz de conservação

Preencher uma ficha por conjunto de dados. O prazo só é aplicado após validação do fundamento e configuração nos sistemas e arquivos abrangidos.

| Campo | Decisão |
|---|---|
| Conjunto de dados e sistema | [PREENCHER] |
| Finalidade e base jurídica | [PREENCHER] |
| Prazo concreto | [DURAÇÃO E UNIDADE] |
| Início da contagem | [EVENTO OU DATA] |
| Fundamento do prazo | [NORMA OU NECESSIDADE DOCUMENTADA] |
| Destino após o prazo | [ELIMINAÇÃO OU ANONIMIZAÇÃO EFETIVA] |
| Cópias de segurança | [CICLO DE EXPIRAÇÃO E RESTRIÇÃO DE UTILIZAÇÃO] |
| Preservação excecional | [MOTIVO, ÂMBITO, DECISOR E REVISÃO] |
| Responsável e evidência | [FUNÇÃO E REGISTO DE EXECUÇÃO] |
| Aprovação e revisão | [NOME, DATA E PRÓXIMA REVISÃO] |

### 8.1 Regras legais e propostas de conservação

Distinguir prazos legais, regras setoriais e propostas internas. A tabela orienta a parametrização; a ficha anterior regista prazo, início da contagem, fundamento, exceções e eliminação de cada conjunto. Não copiar automaticamente a mesma duração para todos os dados de uma pessoa.

| Conjunto | Regra / prazo | Natureza e fundamento |
|---|---|---|
| Fiscal e contabilístico | 10 anos, salvo regra especial ou prolongamento legal aplicável. Financeira regista o período fiscal e início de contagem exatos. | Exigência legal: DL n.º 28/2019, artigo 19.º; verificar também o regime fiscal específico. [R15] |
| Registo dos processos de recrutamento | 5 anos; limitar ao conteúdo do artigo 32.º do Código do Trabalho. | Exigência legal. Não determina, por si só, a guarda integral de todos os currículos. [R3] |
| Currículos / seleção encerrada | Proposta: eliminar dados excedentários até 6 meses após o fecho, salvaguardado o registo legal e defesa concretamente necessária. | Proposta interna sujeita a validação. Bolsa futura separada: 12 meses de referência, mediante fundamento e informação próprios. |
| Imagens CCTV | Regra indicada pela CNPD: 30 dias; eliminação até 48 horas depois, salvo regime específico ou preservação em processo criminal. | Enquadramento a confirmar por instalação e regime. Relatório técnico comprova configuração. [R11] |
| Denúncias abrangidas pela Lei n.º 93/2021 | Pelo menos 5 anos e, independentemente desse prazo, durante processo judicial/administrativo referente à denúncia. | Exigência legal. Registar receção, fundamento do prolongamento e reavaliar a necessidade após o mínimo. [R10, artigo 20.º] |

| Conjunto | Regra / prazo | Natureza e fundamento |
|---|---|---|
| Listas ativas de dietas | Apenas enquanto a instrução/serviço estiverem ativos; substituir de imediato a lista operacional quando validada alteração. | Arquivo probatório separado: prazo por finalidade, regime e risco, aprovado antes do serviço; não guardar processo clínico por rotina. |
| Posição GPS em tempo real | Sem histórico por defeito quando só é necessária a posição atual. | Para percursos: fixar prazo concreto e necessidade no Anexo 6 antes da ativação; não adotar prazo universal. |
| Visitantes / acessos não abrangidos por regra específica | Proposta: 30 dias desde a visita ou evento, com preservação apenas de incidente concreto. | Proposta interna sujeita a teste de necessidade; CCTV e registos legais mantêm regras próprias. |
| Registos técnicos de segurança | Proposta: 90 dias, conforme capacidade e necessidade de deteção; extensões específicas fundamentadas. | Proposta interna; avaliar regimes especiais, risco, precisão e segregação de logs. |
| Processos laborais, SST e saúde | Dividir por documento, finalidade e regime; não estabelecer um único prazo para o processo inteiro. | RH/SST/Jurídico preenchem a ficha antes da aplicação; regras setoriais podem impor conservação prolongada. |
| Consentimentos, direitos e incidentes | Guardar a evidência mínima pelo período de prestação de contas/defesa demonstrado, com revisão e data final aprovadas. | O RGPD não fixa um prazo universal para estas provas. Não confundir prova do consentimento com autorização para continuar o tratamento. |
| Cópias de segurança | Ciclo concreto aprovado por sistema, com limite máximo e procedimento de reaplicação de supressões. | A indisponibilidade de eliminação granular não autoriza recuperação para uso normal de dados já apagados. |

## Anexo 9 Registo de partes interessadas por tratamento

Preencher uma ficha por relação e tratamento relevante. O registo orienta a consulta e a prestação de contas; não substitui o registo de atividades, o contrato com subcontratante nem a avaliação de impacto.

| Campo | Preenchimento |
|---|---|
| Tratamento e responsável interno | [CÓDIGO, PROCESSO E FUNÇÃO] |
| Parte interessada e condição | [GRUPO, ENTIDADE OU REPRESENTANTE; TITULAR, RESPONSÁVEL, SUBCONTRATANTE OU OUTRA] |
| Dados, fluxo e impacto | [DADOS, ORIGEM, DESTINO E CONSEQUÊNCIA PARA AS PESSOAS] |
| Requisito ou expectativa | [NORMA, CONTRATO, DIREITO OU EXPECTATIVA COM FUNDAMENTO] |
| Prioridade e resposta | [RISCO / IMPACTO; AÇÃO, CONTROLO E PRAZO] |
| Interação e responsável | [INFORMAÇÃO, CONSULTA OU ACORDO; CANAL E FUNÇÃO] |
| Evidência e estado | [LINK PARA AVISO, PARECER, CONTRATO, ATA OU REGISTO; PENDENTE / CONCLUÍDO] |
| Revisão | [DATA, MOTIVO DA ALTERAÇÃO E DECISOR] |

Rever na aprovação de novos tratamentos ou contratos, após incidentes ou alterações significativas e, no mínimo, na revisão anual do manual. A consulta de uma parte interessada não equivale a consentimento nem substitui uma obrigação legal de informação ou consulta.

### 9.1 Plano de aplicação por grupo e tratamento

As fichas seguintes estabelecem ações a aplicar quando o tratamento exista no contrato ou serviço. A inclusão de um cenário não confirma a sua existência nem a execução dos controlos. Estado inicial de todas as fichas: por validar pelo responsável do processo. O fecho exige identificação da unidade, responsável nominal, data e evidências.

### PI 01 Refeições para utentes com alergias e dietas específicas

| Partes interessadas | Utentes, representantes autorizados, entidade cliente, Nutrição e Operação. |
|---|---|
| Tratamento e riscos | Receção de instruções alimentares e identificação para preparação e entrega. Riscos: troca de dieta, informação desatualizada e exposição de dados de saúde. |
| Ações e controlos | Validar origem e atualização da instrução; limitar dados clínicos; separar listas operacionais de documentação clínica; restringir acessos e confirmar entrega. |
| Responsabilidade | Responsável de Operação, com Nutrição e gestor do contrato; Jurídico/Privacidade valida os fundamentos e papéis. |
| Momento de execução | Antes do início do serviço ou alteração da dieta; revisão nas mudanças relevantes. |
| Evidência de fecho | Fluxo validado, perfis de acesso, instruções vigentes, evidência de informação e verificação da entrega. |

PI 02 Crianças em contexto escolar

| **Partes interessadas** | **Crianças, encarregados de educação, escola ou entidade contratante e equipa de alimentação.** |
|---|---|
| Tratamento e riscos | Inscrição no serviço, contactos e necessidades alimentares. Riscos: divulgação a terceiros, representação incorreta e exclusão indevida. |
| Ações e controlos | Definir quem recebe e confirma alterações; verificar representação; disponibilizar informação compreensível; evitar listas nominativas com condições de saúde em locais públicos. |
| Responsabilidade | Gestor do contrato e Operação, com Nutrição e Privacidade. |
| Momento de execução | Antes da recolha; rever no início de cada período contratual e na alteração de interlocutores. |
| Evidência de fecho | Aviso, canal de comunicação acordado, registo da verificação de poderes e instruções operacionais. |

PI 03 Idosos e utentes com necessidades de apoio

| **Partes interessadas** | **Utentes, representantes legitimados, cuidadores autorizados e instituição cliente.** |
|---|---|
| Tratamento e riscos | Gestão de necessidades alimentares e apoio à comunicação. Riscos: exposição de saúde, comunicação a pessoa não autorizada e desconsideração da autonomia. |
| Ações e controlos | Adaptar informação e atendimento; confirmar legitimidade do interlocutor; não presumir incapacidade; comunicar apenas os dados necessários ao cuidado ou serviço. |
| Responsabilidade | Operação e gestor do contrato, com Nutrição e Privacidade. |
| Momento de execução | Antes da primeira comunicação e sempre que mude o representante ou a autorização. |
| Evidência de fecho | Informação acessível, verificação de representação, destinatários e decisão de acesso. |

PI 04 Trabalhadores e geolocalização

| **Partes interessadas** | **Condutores, outros trabalhadores abrangidos, representantes, Logística, RH e fornecedor.** |
|---|---|
| Tratamento e riscos | Posições, trajetos e eventos de viatura. Riscos: vigilância desproporcionada, recolha fora do serviço e reutilização indevida. |
| Ações e controlos | Demonstrar necessidade e alternativas; configurar horários e modo privado quando aplicável; limitar acessos e conservação; informar titulares e cumprir consultas devidas. |
| Responsabilidade | Logística e RH, com TI, Jurídico e aconselhamento do EPD quando exista. |
| Momento de execução | Antes da ativação; repetir avaliação na alteração da finalidade ou configuração. |
| Evidência de fecho | Ficha de geolocalização, triagem/AIPD, avisos, consultas aplicáveis, testes e decisão de ativação. |

### PI 05 Clientes institucionais e pedidos de informação

| Partes interessadas | Entidades contratantes, gestores de contrato e titulares abrangidos pelo serviço. |
|---|---|
| Tratamento e riscos | Relatórios de execução e pedidos de dados individuais. Riscos: comunicação excessiva e confusão de responsabilidades. |
| Ações e controlos | Mapear fluxos e papéis; privilegiar indicadores agregados; verificar finalidade, fundamento e destinatário de pedidos individuais; formalizar o instrumento contratual aplicável. |
| Responsabilidade | Gestor do contrato e Jurídico, com Operação e Privacidade. |
| Momento de execução | Antes da assinatura ou alteração contratual e de cada comunicação não prevista. |
| Evidência de fecho | Mapa de fluxos, cláusulas ou acordo aplicável, pedido, decisão e registo de comunicação. |

### PI 06 Fornecedores de tecnologia e subcontratantes

| Partes interessadas | Fornecedores, cadeia de subcontratação, TI, Compras e titulares dos dados. |
|---|---|
| Tratamento e riscos | Alojamento, aplicações, manutenção e suporte. Riscos: acesso indevido, perda de dados e transferências não avaliadas. |
| Ações e controlos | Avaliar garantias e localização dos dados; formalizar instruções e assistência; controlar acessos de suporte; definir devolução e eliminação; rever alterações da cadeia. |
| Responsabilidade | Compras e TI, com Jurídico e Privacidade. |
| Momento de execução | Antes da contratação ou acesso; rever em alterações e no termo do serviço. |
| Evidência de fecho | Diligência, contrato, medidas de segurança, avaliação de transferências quando aplicável e comprovativos de fecho. |

### PI 07 Direitos, reclamações e autoridades

| Partes interessadas | Titulares, representantes verificados, CNPD e outras autoridades competentes. |
|---|---|
| Tratamento e riscos | Pedidos, reclamações e incidentes. Riscos: resposta tardia, divulgação ao destinatário errado e incumprimento de deveres de cooperação. |
| Ações e controlos | Centralizar receção; verificar legitimidade proporcionalmente; registar prazo e decisor; preservar evidências; comunicar através de canal seguro e acompanhar medidas corretivas. |
| Responsabilidade | Privacidade coordena; responsável pelo tratamento decide; EPD coopera quando designado. |
| Momento de execução | Imediatamente após receção ou conhecimento; observar os prazos legais aplicáveis. |
| Evidência de fecho | Registo cronológico, avaliação, resposta, comprovativo de envio e verificação do encerramento. |

PI 08 Recrutamento, estágio e trabalho temporário

| Partes / dados | Candidatos, estagiários, agências e instituições: contactos, percurso e avaliações relevantes. |
|---|---|
| Decisão e controlos | Identificar responsável por cada fase; informar sobre fontes; restringir testes; separar bolsa futura e registo legal de recrutamento. |
| Responsável / evidência | RH com Jurídico: aviso, critérios de seleção, contrato com agência, matriz de conservação e prova de eliminação. |

PI 09 Antigos trabalhadores, dependentes e emergência

| Partes / dados | Antigos trabalhadores, familiares, dependentes e contactos: arquivo laboral, benefícios e contactos delimitados. |
|---|---|
| Decisão e controlos | Segmentar conservação; atualizar contactos; informar pessoas cujos dados foram fornecidos por terceiro quando devido; revogar acessos na saída. |
| Responsável / evidência | RH e TI: lista de saída concluída, registo de acessos revogados, aviso e fundamento por classe documental. |

PI 10 Saúde ocupacional e análises individualizadas

| Partes / dados | Trabalhadores, médico do trabalho, laboratórios e equipa de segurança: dados de saúde e conclusões funcionais. |
|---|---|
| Decisão e controlos | Qualificar papéis reais e sigilo; restringir resultados clínicos; usar códigos nas amostras quando possível; relatórios a clientes sem nomes desnecessários. |
| Responsável / evidência | SST com RH/Qualidade/Jurídico: circuito clínico separado, perfis autorizados, contratos e instruções de comunicação. |

PI 11 Visitantes, CCTV e segurança física

| Partes / dados | Visitantes, motoristas, trabalhadores externos e pessoas captadas: acesso, imagem e incidente. |
|---|---|
| Decisão e controlos | Aviso visível; zonas de captação delimitadas; sem cópia de identificação por rotina; exportação de imagens só por motivo e destinatário legitimados. |
| Responsável / evidência | Segurança: planta de câmaras, fundamento, sinalética, prazo configurado e registo de consultas/extrações. |

PI 12 Denunciantes, visados e testemunhas

| Partes / dados | Identidade, factos, contactos e evidências da denúncia; risco de retaliação ou imputação indevida. |
|---|---|
| Decisão e controlos | Canal segregado; acesso nominal; verificação de conflitos; confidencialidade e limites dos direitos analisados caso a caso. |
| Responsável / evidência | Gestor do canal com Jurídico: cronologia, decisões, comunicações, registo de acesso e prazo de conservação. |

PI 13 Marketing, eventos e utilizadores digitais

| Partes / dados | Contactos, escolhas, identificadores digitais, fotografia e voz quando efetivamente tratados. |
|---|---|

| Partes / dados | Contactos, escolhas, identificadores digitais, fotografia e voz quando efetivamente tratados. |
|---|---|
| Decisão e controlos | Consentimentos separados quando exigidos; prova da origem das listas; recusa simples; não ativar cookies opcionais antes da escolha. |
| Responsável / evidência | Comunicação/TI: inventário de tecnologias, avisos, consentimentos, teste de bloqueio e lista de supressão. |

PI 14 Auditorias, seguros e relações institucionais

| Partes / dados | Auditores, consultores, seguradoras, bancos e autoridades; dados de terceiros incluídos nas evidências. |
|---|---|
| Decisão e controlos | Necessidade, papel e base por comunicação; minimizar e expurgar; não enviar pastas completas; proteger segredo profissional quando aplicável. |
| Responsável / evidência | Qualidade/Jurídico/Financeira: pedido autenticado, decisão, inventário do enviado, canal e prova de receção. |

PI 15 Representação e pessoas falecidas

| Partes / dados | Titular, representante designado, acompanhante ou herdeiros; poderes e dados protegidos por lei. |
|---|---|
| Decisão e controlos | Verificar âmbito dos poderes e eventuais limites; não presumir acesso por parentesco; ponderar minimização de documentos de prova. |
| Responsável / evidência | Privacidade/Jurídico: método de verificação, norma aplicável, decisão motivada e dados efetivamente comunicados. |

## 9.2 Verificação da execução

Na revisão anual, Privacidade apresenta à gestão: proporção de tratamentos relevantes com partes interessadas identificadas; ações concluídas com evidência face às ações vencidas; pedidos respondidos dentro do prazo; e desvios recorrentes em avisos, representação ou acessos. Registar numerador, denominador, período, causa dos desvios, ação, responsável e prazo. A revisão deve considerar também reclamações e a adequação da informação aos grupos vulneráveis.

## Anexo 10 Avisos de privacidade por público

Modelo de trabalho. Completar e disponibilizar antes de recolher dados; retirar opções que não se apliquem. Um aviso com alternativas jurídicas não resolvidas não está pronto para divulgação.

| Elemento obrigatório | Texto-base a completar |
|---|---|
| Responsável e contacto | [DENOMINAÇÃO, MORADA E CONTACTO] é responsável pelo tratamento descrito neste aviso. Contacto de privacidade: [CONTACTO]. EPD, quando designado: [CONTACTO]. |
| Dados, finalidade e base | Tratamos [DADOS] para [FINALIDADE CONCRETA], com fundamento em [ARTIGO/BASE APLICÁVEL]. Para categorias especiais: [CONDIÇÃO DO ARTIGO 9.º]. Identificar o interesse prosseguido se se usar interesse legítimo. |
| Origem e obrigatoriedade | Os dados são recolhidos [JUNTO DO TITULAR / FONTE]. [CAMPOS] são necessários por [OBRIGAÇÃO/CONTRATO]; sem eles [CONSEQUÊNCIA REAL]. Os restantes são opcionais. |
| Destinatários e transferências | Acesso por [FUNÇÕES]; comunicação a [DESTINATÁRIOS/CATEGORIAS]. Transferências: [INEXISTENTES OU PAÍSES, MECANISMO E MODO DE OBTER AS GARANTIAS]. |
| Conservação | Conservamos [CONJUNTO] por [PRAZO CONCRETO OU CRITÉRIO EXPLICÁVEL], contado de [EVENTO]. Após esse período [DESTINO], ressalvadas obrigações de preservação aplicáveis. |
| Direitos e reclamação | Pode exercer os direitos aplicáveis junto de [CANAL], incluindo acesso, retificação, apagamento, limitação, oposição e portabilidade; retirar consentimento quando seja a base. Pode reclamar junto da CNPD: www.cnpd.pt. |
| Automatização | [NÃO EXISTEM DECISÕES DO ARTIGO 22.º / DESCREVER EXISTÊNCIA, LÓGICA RELEVANTE, IMPORTÂNCIA, CONSEQUÊNCIAS E SALVAGUARDAS]. |
| Versão e acesso | Aviso versão [N.º], de [DATA]; disponível em [LOCAL/CANAL]. Alterações relevantes são comunicadas antes da nova finalidade. |

| Público / módulo | Informação específica que não pode faltar |
|---|---|
| Trabalhadores e candidatos | Fases da relação; destinatários públicos; dados de saúde separados; monitorização; origem de referências e prazos da seleção/bolsa. |
| Utentes e representantes | Entidades responsáveis, circuito de dietas, atualização, representação e informação adaptada; não anexar a lista de utentes ao aviso. |
| Contactos e fornecedores | Gestão da relação profissional, pagamentos, avaliações e eventual marketing em finalidade separada. |
| Visitantes e CCTV | Aviso curto visível e acesso à informação completa; responsável, finalidade e contactos; zonas e prazo do sistema. |
| Geolocalização | Equipamento, precisão, frequência, horários, modo privado, destinatários, prazo e finalidades excluídas. |
| Digital e marketing | Cookies por finalidade, fornecedores, duração, transferências, escolhas e retirada; consentimento não pré-selecionado. |
| Denúncias | Canal reservado, responsáveis, confidencialidade, destinatários, prazos próprios e condições de exercício de direitos. |

## Anexo 11 Qualificação de papéis e comunicação de dados

| Pergunta de decisão | Registo obrigatório |
|---|---|
| Quem decide a finalidade e os meios essenciais? | [ENTIDADE E DECISÕES EFETIVAS]. Distinguir decisão própria, conjunta e execução por instruções. |
| Qual é o papel de cada entidade neste fluxo? | [RESPONSÁVEL / CORRESPONSÁVEL / SUBCONTRATANTE / DESTINATÁRIO COM FINALIDADE PRÓPRIA]. Fundamentar. |
| Qual o instrumento necessário? | [ARTIGO 26.º / ARTIGO 28.º / ACORDO DE COMUNICAÇÃO ENTRE RESPONSÁVEIS / OUTRO]. Não aplicar rótulo por conveniência. |
| Quem informa e responde aos titulares? | [ENTIDADE, CANAL E PRAZO DE ENCAMINHAMENTO]. Acordos entre entidades não eliminam direitos do titular. |
| O pedido de dados foi autenticado? | [IDENTIDADE, PODERES, REFERÊNCIA E CONTACTO CONFIRMADO]. |
| Qual a finalidade e o fundamento? | [ARTIGO 6.º; ARTIGO 9.º/10.º QUANDO APLICÁVEL; OBRIGAÇÃO SETORIAL]. |
| É possível reduzir ou agregar? | [DADOS MÍNIMOS, OCULTAÇÕES E JUSTIFICAÇÃO DO QUE SE MANTÉM]. |
| Há transferência, risco ou nova finalidade? | [AVALIAÇÃO E CONDIÇÕES ANTES DO ENVIO]. |
| Como e a quem foi enviado? | [CANAL, DESTINATÁRIO, DATA, INVENTÁRIO E COMPROVATIVO]. |
| Decisão e revisão | [AUTORIZAR / LIMITAR / RECUSAR FUNDAMENTADAMENTE; DECISOR E DATA]. |

Exemplo de aplicação: um cliente pede trajetos nominativos para confirmar entregas. O gestor verifica se um comprovativo de entrega ou indicador agregado satisfaz a finalidade; não abre acesso à plataforma de GPS apenas porque o contrato exige relatórios de execução.

## Anexo 12  Diligência e contrato de subcontratação

| Ponto a verificar | Evidência / decisão |
|---|---|
| Objeto, duração e instruções | [SERVIÇO, FINALIDADES, DADOS, TITULARES E CONTACTOS DO RESPONSÁVEL]. |
| Garantias de segurança | [ACESSOS, CIFRAGEM, CORREÇÕES, REGISTOS, CONTINUIDADE E TESTES]. |
| Pessoas e confidencialidade | [COMPROMISSOS E LIMITAÇÃO DE ACESSO]. |
| Cadeia de subcontratação | [LISTA, PAÍSES, AUTORIZAÇÃO E PROCESSO DE ALTERAÇÃO/OPOSIÇÃO]. |
| Localização e transferências | [ALOJAMENTO, SUPORTE, CÓPIAS E MECANISMOS DO CAPÍTULO V]. |
| Incidentes | [CANAL 24/7 QUANDO NECESSÁRIO; COMUNICAÇÃO SEM DEMORA INJUSTIFICADA; META CONTRATUAL E CONTEÚDO INICIAL]. |
| Direitos, AIPD e consulta | [CONTACTO, ASSISTÊNCIA, TEMPOS DE ENCAMINHAMENTO E EXTRAÇÃO/ELIMINAÇÃO]. |
| Auditoria e evidência | [INFORMAÇÃO DISPONÍVEL, AUDITORIAS/INSPEÇÕES E TRATAMENTO DE DESVIOS]. |
| Final do serviço | [DEVOLUÇÃO OU ELIMINAÇÃO, CÓPIAS, PRAZOS, EXCEÇÕES LEGAIS E CERTIFICADO]. |
| Instrução ilegal | [DEVER DE INFORMAR IMEDIATAMENTE E ESCALAR ANTES DE EXECUTAR]. |
| Conclusão | [APROVADO / CONDICIONADO / RECUSADO; AÇÕES, DONOS E DATAS]. |

Nos contratos em que a ICA é subcontratante, o guião aplica-se às obrigações assumidas perante o cliente e à cadeia que a ICA utiliza. O responsável deve ter informação suficiente para avaliar as garantias; segredos comerciais não justificam ausência total de evidência.

## Anexo 13 AIPD e matriz de riscos para as pessoas

A triagem do Anexo 2 decide a necessidade; este guião estrutura a avaliação completa. Descrever tratamento, finalidade, fluxos, intervenientes, necessidade, proporcionalidade, riscos, medidas, parecer do EPD e consulta aos titulares quando adequada. A análise considera o dano para as pessoas, não apenas multas ou reputação da empresa.

| Escala interna proposta | Critério |
|---|---|
| Probabilidade 1 / 2 / 3 / 4 | Remota / possível / provável / muito provável, atendendo ao cenário e aos controlos efetivos. |
| Gravidade 1 / 2 / 3 / 4 | Impacto limitado / significativo reversível / grave ou de difícil reversão / muito grave, incluindo risco físico ou discriminação severa. |
| Classificação P × G | 1–3 baixo; 4–7 moderado; 8–11 elevado; 12–16 muito elevado. A gravidade extrema exige escalada mesmo com resultado inferior. |
| Limite do método | Escala de gestão interna. Não substitui os critérios legais de AIPD, de notificação ou de consulta prévia. |

| Cenário ilustrativo | Dano / medida a testar |
|---|---|
| Lista de alergias exposta | Estigma e divulgação de saúde / identificação reservada, acessos e verificação no ponto de entrega. |
| Instrução de dieta alterada | Refeição insegura e dano físico / origem autenticada, dupla validação e controlo de versões. |
| GPS fora do serviço | Exposição da vida privada / modo privado eficaz, horário técnico e teste independente. |
| Envio de folha salarial errada | Exposição financeira e fraude / validação de destinatário, canal seguro e revisão antes do envio. |
| Fornecedor sem saída verificável | Persistência de dados e perda de controlo / teste de exportação, eliminação e prazo para cópias. |

| Ficha por risco | Preenchimento |
|---|---|
| Tratamento / partes afetadas | [CÓDIGO, PESSOAS, DADOS, DIREITOS E VULNERABILIDADES]. |
| Cenário e causas | [AMEAÇA, VULNERABILIDADE, EVENTO E CONSEQUÊNCIAS]. |
| Avaliação inicial | [P, G, RESULTADO E JUSTIFICAÇÃO]. |
| Medidas e evidência | [CONTROLO, RESPONSÁVEL, PRAZO E TESTE DE EFICÁCIA]. |
| Risco residual | [P, G, RESULTADO E LIMITAÇÕES APÓS CONTROLAR]. |
| Decisão | [REFORMULAR / APROVAR SE LÍCITO / CONSULTAR CNPD ANTES DE TRATAR SE PERSISTIR RISCO ELEVADO]. |
| Parecer e revisão | [EPD, CONSULTA A TITULARES OU JUSTIFICAÇÃO, DECISOR E DATA]. |

## Anexo 14  Resposta a incidentes e modelos de comunicação

| Janela operacional proposta | Ação |
|---|---|
| Imediatamente | Reportar, conter, preservar evidência e acionar suplente; registar hora de conhecimento do responsável. |
| Primeiras horas | Identificar dados/titulares e efeitos; verificar se ICA é responsável ou subcontratante; avisar o responsável quando subcontratante. |
| Até 24 horas — meta interna | Reunir factos suficientes, avaliar risco, preparar decisão e comunicação; não esperar por certeza absoluta. |
| Antes do limite legal | Notificar CNPD até 72 horas do conhecimento, sempre que possível e quando devido; justificar atraso e usar fases se necessário. |
| Sem demora injustificada | Comunicar aos titulares se provável risco elevado, salvo exceção legal fundamentada. |
| Fecho | Concluir causa raiz, eficácia das medidas, evidências e lições; rever AIPD, formação e contratos. |

### Modelo de comunicação ao titular

Em [DATA] identificámos [DESCRIÇÃO CLARA]. A situação poderá ter afetado [DADOS] e ter como consequências [RISCO CONCRETO]. Adotámos [MEDIDAS] e recomendamos [AÇÕES ÚTEIS AO TITULAR]. Para esclarecimentos e exercício de direitos, contacte [CONTACTO / EPD]. Prestaremos nova informação quando [COMPROMISSO ADEQUADO].

### Modelo de decisão de não notificar

Incidente [REFERÊNCIA]. Factos conhecidos em [DATA/HORA]. Categorias e volume: [DADOS]. Avaliação documentada: [PROBABILIDADE, GRAVIDADE E SALVAGUARDAS EFETIVAS]. Conclui-se [FUNDAMENTO LEGAL E FACTUAL]. Decisor: [FUNÇÃO]. A decisão será reavaliada perante [NOVOS FACTOS]. Não usar apenas «dados cifrados» sem verificar eficácia da cifragem e proteção das chaves.

## Anexo 15 Instrução alimentar e representação

| Campo operacional | Registo mínimo |
|---|---|
| Serviço e utente | [UNIDADE, IDENTIFICADOR SEGURO E DADOS ESTRITAMENTE NECESSÁRIOS]. |
| Entidades e papéis | [CLIENTE / ICA / OUTROS; QUEM DECIDE E QUEM EXECUTA]. |
| Fonte autorizada | [ENTIDADE/PESSOA, CANAL, DATA E LEGITIMIDADE]. |
| Instrução alimentar | [RESTRIÇÕES E ORIENTAÇÕES NECESSÁRIAS; EVITAR DIAGNÓSTICOS NÃO NECESSÁRIOS]. |
| Fundamentos e informação | [ARTIGO 6.º + CONDIÇÃO DO ARTIGO 9.º, QUANDO APLICÁVEL; AVISO ENTREGUE]. |
| Validação e vigência | [FUNÇÃO COMPETENTE, DATA, INÍCIO E REVISÃO]. |
| Preparação / entrega | [FUNÇÕES COM ACESSO E MÉTODO DE CONFIRMAÇÃO]. |
| Alteração | [PEDIDO, AUTORIZAÇÃO, VERSÃO SUBSTITUÍDA E COMUNICAÇÃO À EQUIPA]. |
| Arquivo / eliminação | [PRAZO E EVENTO; RESPONSÁVEL; RETIRADA DA LISTA ATIVA]. |

### Verificação de representação

Registar titular, interlocutor, natureza dos poderes, ato em causa, meio de verificação, validade e decisão. Conservar a evidência mínima da verificação; exigir cópia integral de documento apenas quando necessária e fundamentada. Em caso de poderes limitados, comunicação parcial ou conflito, encaminhar para Jurídico/Privacidade sem desconsiderar o titular. A urgência alimentar é tratada pelo circuito de segurança e contacto competente, sem presumir autorização geral de acesso.

## Anexo 16  Consentimento, oposição e prova de informação

Utilizar apenas quando o consentimento seja a base adequada. Separar finalidades e não pré-assinalar opções. A recusa não prejudica serviços que não dependam desse tratamento. Consentimento para dados de saúde exige as condições de consentimento explícito e uma escolha efetivamente livre.

| Elemento | Modelo |
|---|---|
| Finalidade opcional | Aceito [ATO CONCRETO] para [FINALIDADE], por [RESPONSÁVEL], envolvendo [DADOS]. |
| Escolha separada | [SIM / NÃO] para cada finalidade e canal; não agrupar marketing, imagem e dados de saúde numa única opção. |
| Informação prévia | Aviso [VERSÃO/DATA] disponibilizado em [CANAL]. |
| Retirada | Posso retirar através de [CANAL SIMPLES], sem afetar a licitude anterior. |
| Prova mínima | [TITULAR/IDENTIFICADOR, FINALIDADE, TEXTO/VERSÃO, DATA, ATO AFIRMATIVO E EVENTUAL REPRESENTAÇÃO]. |
| Oposição / supressão | [DATA, ÂMBITO, SISTEMAS, DESTINATÁRIOS ATUALIZADOS E CONFIRMAÇÃO DE EXECUÇÃO]. |

A prova de entrega de um aviso usa registo separado: «Foi disponibilizada a informação de privacidade [VERSÃO], em [DATA/CANAL]». Não acrescentar «autorizo todos os tratamentos» nem condicionar direitos à assinatura. A assinatura de receção de aviso de GPS não sana uma utilização proibida.

## Anexo 17  Saída, eliminação e preservação excecional

| Etapa | Verificação e prova |
|---|---|
| Desencadeador | [FIM DO PRAZO, FIM DO SERVIÇO, SAÍDA DE PESSOA OU PEDIDO VÁLIDO]. |
| Inventário | [SISTEMAS, FICHEIROS, PAPEL, CÓPIAS LOCAIS, DESTINATÁRIOS E FORNECEDORES]. |
| Preservação legal | [SE APLICÁVEL: MOTIVO, NORMA/PROCESSO, DADOS LIMITADOS, DECISOR, ACESSOS E DATA DE REVISÃO]. |
| Execução | [ELIMINAÇÃO SEGURA, DESTRUIÇÃO OU ANONIMIZAÇÃO VALIDADA; DATA E OPERADOR]. |
| Cópias e restauro | [EXPIRAÇÃO, LIMITAÇÃO DE USO E REGISTO A REAPLICAR APÓS RESTAURO]. |
| Fornecedor | [DEVOLUÇÃO/ELIMINAÇÃO, SUBCONTRATANTES, CÓPIAS E CERTIFICADO]. |
| Verificação independente | [AMOSTRA, RESULTADO E CORREÇÕES]. |
| Encerramento | [RESPONSÁVEL, EVIDÊNCIA E DATA]. |

A preservação para litígio suspende apenas a eliminação dos dados pertinentes. Não converte todos os arquivos numa conservação indefinida. O Jurídico revê o motivo e determina o levantamento quando termine a necessidade; a TI executa a eliminação remanescente e regista o resultado.

## Anexo 18 Plano de implementação e verificação da cobertura

Prazos abaixo são metas internas propostas a contar da aprovação, não períodos de tolerância legal. Um tratamento novo com requisito crítico por cumprir não começa; uma situação existente ilícita é contida e corrigida sem aguardar a meta.

| Prioridade / meta | Entrega e critério de fecho |
|---|---|
| Imediata | Confirmar entidade e contactos; identificar dados de saúde, GPS, CCTV e denúncias; conter acessos ou divulgações sem fundamento. |
| Até 15 dias | Designar responsáveis; classificar os 24 grupos por unidade/contrato; inventariar fluxos e papéis; decidir obrigatoriedade do EPD. |
| Até 30 dias | Completar RAT, avisos, conservação, contratos e triagens; testar direitos, acessos e modo privado dos sistemas existentes. |
| Até 60 dias | Concluir ações técnicas e AIPD necessárias antes de novos tratamentos; executar testes de eliminação, restauro e resposta a incidentes. |
| Até 90 dias | Auditoria por amostra, resolução de desvios e revisão da gestão com evidências; manter ações residuais com dono e data. |

| Verificação por grupo / tratamento | Registo |
|---|---|
| Aplicabilidade | [APLICÁVEL / NÃO APLICÁVEL E FUNDAMENTO / POR CONFIRMAR]. |
| Cobertura | [RAT, AVISO, BASES, ACESSOS, CONSERVAÇÃO, CONTRATO E AIPD QUANDO EXIGIDA]. |
| Teste | [AMOSTRA OU CENÁRIO, DATA E RESULTADO]. |
| Lacuna | [REQUISITO EM FALTA, RISCO PARA AS PESSOAS E MEDIDA DE CONTENÇÃO]. |
| Ação | [RESPONSÁVEL NOMINAL, PRAZO E EVIDÊNCIA ESPERADA]. |
| Validação de fecho | [VERIFICADOR, DATA E DOCUMENTO/LIGAÇÃO DA PROVA]. |

Indicadores: tratamentos inventariados face aos identificados; grupos aplicáveis com cobertura comprovada; pedidos no prazo; ações vencidas; fornecedores críticos com diligência; eliminações executadas/testadas; acessos revistos; percentagem de trabalhadores formados; incidentes repetidos. Para cada indicador indicar período, numerador, denominador, meta aprovada, resultado e ação. Um valor percentual sem universo conhecido não demonstra cobertura. Acrescentar os indicadores de cibersegurança da secção 13.8.

## Anexo 19 Respeito pelas diferenças e não discriminação

Aplicar em pedidos de adaptação cultural ou religiosa e em alegações de discriminação relacionadas com raça, etnia, cor da pele, tradições, cultura ou religião. Separar a gestão de um pedido operacional do processo reservado de uma eventual reclamação.

| Etapa | Registo e controlo |
|---|---|
| Ouvir sem presumir | [NECESSIDADE DESCRITA PELA PESSOA; APOIO DE COMUNICAÇÃO, SE NECESSÁRIO]. Não atribuir crença ou origem pela aparência. |
| Minimizar | [INFORMAÇÃO FUNCIONAL SUFICIENTE]. Não pedir raça, etnia ou religião se a necessidade puder ser atendida sem esses dados. |
| Verificar licitude | [FINALIDADE, BASE DO ARTIGO 6.º E, SE NECESSÁRIO, CONDIÇÃO DO ARTIGO 9.º; AVISO E ACESSOS]. |
| Analisar solução | [ALTERNATIVAS, SEGURANÇA ALIMENTAR, DIREITOS DE TERCEIROS, CONDIÇÕES LEGAIS/CONTRATUAIS E LIMITAÇÕES REAIS]. |
| Decidir sem discriminar | [CRITÉRIO OBJETIVO, MEDIDA, RESPONSÁVEL, PRAZO E EXPLICAÇÃO À PESSOA]. Reavaliar efeitos indiretos de regras gerais. |
| Proteger a reclamação | [CANAL RESERVADO, GESTOR SEM CONFLITO, EVIDÊNCIAS, CONFIDENCIALIDADE E PREVENÇÃO DE RETALIAÇÃO]. |
| Corrigir e verificar | [AÇÃO, COMUNICAÇÃO ADEQUADA, RESULTADO, FORMAÇÃO E VERIFICAÇÃO DE NÃO RECORRÊNCIA]. |
| Conservar apenas o necessário | [PRAZO, FUNDAMENTO, ACESSOS E ELIMINAÇÃO]. Não incluir dados sensíveis em relatórios gerais. |

| Exemplo de aplicação | Resposta esperada |
|---|---|
| Pedido de refeição sem determinado ingrediente por motivo cultural/religioso | Confirmar a restrição e condições reais da preparação; procurar solução; registar instrução mínima e evitar rótulos sobre a crença. |
| Aviso incompreensível para o destinatário | Disponibilizar explicação ou apoio linguístico adequado, sem recorrer automaticamente a familiar não autorizado. |
| Comentário racista ou depreciativo num registo de utente | Preservar evidência mínima em processo reservado, corrigir o registo operacional, apurar responsabilidade e prevenir repetição. |
| Critério de recrutamento com efeito desvantajoso não justificado | Suspender a sua aplicação quando necessário, rever pertinência para a função e documentar a correção e os casos afetados. |
| Pedido de relatório que agrupe utentes por etnia ou religião | Não produzir sem finalidade necessária, fundamento específico e avaliação; propor informação operacional ou efetivamente anonimizada quando suficiente. |

A diversidade não é tratada como fator de risco da pessoa. O risco avaliado é o de exposição, discriminação ou tratamento injusto causado pelo processo, pela informação ou pela decisão da organização.

## Anexo 20  Avaliação de aplicabilidade e calendário NIS2

Preencher por entidade jurídica. Estado inicial: por confirmar. Não classificar a ICA como entidade essencial ou importante sem análise e qualificação aplicáveis.

| Campo | Registo e evidência |
|---|---|
| Identificação | [DENOMINAÇÃO, NIF, ESTABELECIMENTOS, RESPONSÁVEL E DATA]. |
| Atividades e território | [ATIVIDADES EFETIVAS, SERVIÇOS, CAE AUXILIAR, CLIENTES, LOCAIS E JUSTIFICAÇÃO FACE AOS ANEXOS I E II]. |
| Dimensão e grupo | [EFETIVOS, VOLUME DE NEGÓCIOS, BALANÇO, EXERCÍCIO E EMPRESAS ASSOCIADAS OU COLIGADAS; CRITÉRIO DO ANEXO III]. |
| Critérios especiais | [CRITÉRIOS DO ARTIGO 3.º, IDENTIFICAÇÃO COMO ENTIDADE CRÍTICA, EXCLUSÕES E EVENTUAIS REGIMES SETORIAIS]. |
| Conclusão interna | [ABRANGIMENTO INDICIADO / NÃO ABRANGIDA COM FUNDAMENTO / POR CONFIRMAR; PARECER E DECISOR]. |
| Autoridade e qualificação | [AUTORIDADE, AUTOIDENTIFICAÇÃO, DATA, RECIBO, QUALIFICAÇÃO COMUNICADA E EVENTUAIS ESCLARECIMENTOS]. |
| Responsáveis e contactos | [FUNÇÃO DE CIBERSEGURANÇA, CONTACTO PERMANENTE, SUPLENTES, PODERES DE REPRESENTAÇÃO E COMUNICAÇÕES DEVIDAS]. |
| Revisão | [DATA, EVENTOS DE REVISÃO E RESPONSÁVEL; MUDANÇA DE ATIVIDADE, DIMENSÃO, GRUPO OU NORMA]. |

### Calendário por obrigação

| Obrigação e norma | Prazo e estado | Responsável e prova |
|---|---|---|
| [AUTOIDENTIFICAÇÃO / CONTACTOS / INVENTÁRIO / MEDIDAS / REPORTE / INCIDENTES] | [EVENTO INICIAL, PRODUÇÃO DE EFEITOS, DATA EXIGÍVEL E ESTADO] | [NOME, SUPLENTE, COMPROVATIVO E PRÓXIMA AÇÃO] |

Repetir uma linha por obrigação. Identificar disposições já exigíveis, diferidas e dependentes de instruções técnicas. Registar cada instrução consultada e a respetiva versão. A incerteza não suspende os deveres RGPD nem as medidas urgentes de contenção. [R19; R20]

## Anexo 21 Ativos riscos e controlos de cibersegurança

Usar uma ficha por ativo ou serviço. Articular com RAT, Anexo 13 e avaliação de continuidade, mantendo separados o risco para as pessoas e o risco operacional.

| Campo | Preenchimento |
|---|---|
| Ativo e dependências | [SISTEMA, SERVIÇO, DONO, FORNECEDOR, LOCALIZAÇÃO, VERSÃO, REDES E DEPENDÊNCIAS]. |
| Informação e utilizadores | [DADOS, TITULARES, VOLUME, FUNÇÕES, PRIVILÉGIOS E ACESSOS REMOTOS]. |
| Cenário | [AMEAÇA, VULNERABILIDADE, EVENTO, IMPACTO NO SERVIÇO E CONSEQUÊNCIAS PARA AS PESSOAS]. |
| Avaliação inicial | [MÉTODO, PROBABILIDADE, IMPACTO E JUSTIFICAÇÃO COM EVIDÊNCIA]. |
| Requisito | [LEGAL / CONTRATUAL / INTERNO; NORMA OU CLÁUSULA; QNRCS E NÍVEL APLICÁVEL]. |
| Controlo e teste | [MEDIDA, CONFIGURAÇÃO, RESPONSÁVEL, PRAZO, CRITÉRIO E RESULTADO DO TESTE]. |
| Risco residual | [AVALIAÇÃO APÓS MEDIDAS, LIMITAÇÕES E DECISÃO COMPETENTE]. |
| Exceção | [MOTIVO, CONTROLO COMPENSATÓRIO, APROVAÇÃO E DATA DE EXPIRAÇÃO]. |
| Evidência e revisão | [LOCAL RESTRITO DA PROVA, VERIFICADOR, DATA E PRÓXIMA REVISÃO]. |

### Exemplos para iniciar a avaliação

| Cenário | Medida a comprovar |
|---|---|
| Conta de fornecedor comprometida | MFA, acesso autorizado por tempo limitado e rastreabilidade. |
| Instrução alimentar adulterada | Origem autenticada, controlo de versões e dupla validação. |
| Cópias cifradas pelo atacante | Separação, proteção contra alteração e ensaio de recuperação. |
| Registos de segurança excessivos | Minimização, acesso restrito, prazo e proibição de reutilização laboral indevida. |

## Anexo 22  Registo integrado de incidente

Complementa os Anexos 4 e 14. Usar o mesmo identificador de ocorrência, evitando duplicar listas nominativas. A tabela deve permitir reconstruir quem sabia o quê e em que momento.

| Elemento | Registo |
|---|---|
| Identificação e coordenação | [REFERÊNCIA, UNIDADES, COORDENADOR, EQUIPA, SUPLENTES E CANAL ALTERNATIVO]. |
| Cronologia | [INÍCIO OU ESTIMATIVA; DETEÇÃO; CONHECIMENTO RGPD; VERIFICAÇÃO DE IMPACTO SIGNIFICATIVO; FIM DO IMPACTO; RESOLUÇÃO]. |
| Impacto | [ATIVOS, SERVIÇOS, UTILIZADORES, DURAÇÃO, GEOGRAFIA, DADOS, TITULARES E POSSÍVEL DANO FÍSICO]. |
| Avaliação RGPD | [PAPEL DA ICA, VIOLAÇÃO, RISCO, RISCO ELEVADO, FUNDAMENTOS, DECISOR E PARECER EPD]. |
| Avaliação cibersegurança | [APLICABILIDADE, SIGNIFICÂNCIA, CRITÉRIOS E LIMIARES USADOS, AUTORIDADE E DECISOR]. |
| Contenção e continuidade | [ISOLAMENTO, EVIDÊNCIAS, FONTE ALTERNATIVA VALIDADA, DECISÕES SOBRE REFEIÇÕES E RESPONSÁVEIS]. |
| Comunicações | [DESTINATÁRIO, OBRIGAÇÃO, PRAZO, DATA/HORA EFETIVA, CONTEÚDO, RECIBO E ATUALIZAÇÕES]. |
| Não notificação ou exceção | [FACTOS, FUNDAMENTO LEGAL, APROVAÇÃO, HORA E EVENTO DE REAVALIAÇÃO]. |
| Recuperação e fecho | [TESTES, RECONCILIAÇÃO, CAUSA, RISCO RESIDUAL, AÇÕES, RESPONSÁVEIS E VERIFICAÇÃO]. |

### Modelo de registo de decisão

Às [HORA/DATA], com base em [FACTOS E EVIDÊNCIAS], [DECISOR] concluiu [CLASSIFICAÇÃO RGPD] e [CLASSIFICAÇÃO DE CIBERSEGURANÇA]. São devidas [COMUNICAÇÕES], até [DATAS/HORAS]. A decisão de não notificar [DESTINATÁRIO] assenta em [FUNDAMENTO]. Reavaliar perante [NOVOS FACTOS] ou em [MOMENTO].

## Anexo 23  Continuidade ensaio e retoma

| Campo | Registo e critério de aprovação |
|---|---|
| Serviço e dependências | [PROCESSO CRÍTICO, UNIDADES, CLIENTES, SISTEMAS, FORNECEDORES, PESSOAS E ENERGIA/COMUNICAÇÕES]. |
| Objetivos aprovados | [INTERRUPÇÃO MÁXIMA TOLERÁVEL, TEMPO DE RECUPERAÇÃO, PERDA DE DADOS TOLERÁVEL E FUNDAMENTO]. |
| Ativação | [SINAL DE ATIVAÇÃO, DECISOR, SUPLENTE E CANAL ALTERNATIVO]. |
| Alternativa segura | [MEIOS, CÓPIA CONTROLADA, FONTE AUTORIZADA, VERSÃO E ÚLTIMA ATUALIZAÇÃO]. |
| Proteção dos utentes | [CONFIRMAÇÃO DE DIETA, ALERGÉNIOS, IDENTIDADE E ALTERAÇÕES; DECISÃO QUANDO FALTE INFORMAÇÃO FIÁVEL]. |
| Execução | [AÇÕES, RESPONSÁVEIS, HORAS, SERVIÇOS SUSPENSOS OU MANTIDOS E COMUNICAÇÃO A CLIENTES]. |
| Retoma | [CONTENÇÃO CONFIRMADA, RESTAURO E INTEGRIDADE TESTADOS, RECONCILIAÇÃO E AUTORIZAÇÕES TI/OPERAÇÃO/DQAS]. |
| Dados e documentos | [REAPLICAÇÃO DE ELIMINAÇÕES, RETIRADA DE CÓPIAS OBSOLETAS E PROTEÇÃO DOS REGISTOS DO INCIDENTE]. |
| Ensaio | [CENÁRIO, DATA, PARTICIPANTES, RESULTADOS, TEMPOS REAIS E COMPARAÇÃO COM OBJETIVOS]. |
| Melhoria | [FALHAS, AÇÕES, DONOS, PRAZOS, NOVO TESTE E APROVAÇÃO DO FECHO]. |

Critério de segurança. Não autorizar a entrega de uma refeição cuja adequação ao utente não possa ser confirmada. Nutrição e Operação articulam com a fonte autorizada e o cliente a alternativa segura; a reposição do sistema informático, por si só, não autoriza a retoma.

# Referenciais legais e técnicos

Fontes oficiais consultadas na revisão de 25 de setembro de 2026. As remissões R1–R20 identificam os referenciais usados. Confirmar a versão em vigor e os regimes setoriais de cada tratamento na aprovação e nas revisões. Orientações anteriores ao RGPD não reintroduzem automaticamente regimes de autorização revogados.

R1 RGPD — Regulamento (UE) 2016/679

Princípios, bases, categorias especiais, direitos, governação, segurança e transferências. Fonte oficial

R2 Lei n.º 58/2019, de 8 de agosto

Execução nacional: menores, pessoas falecidas, relações laborais, saúde e vigilância. Interpretar em conformidade com o RGPD. Fonte oficial

R3 Código do Trabalho — Lei n.º 7/2009, texto consolidado

Reserva da vida privada e vigilância, igualdade/não discriminação, registos de recrutamento; artigos 16.º–22.º, 24.º–32.º. Fonte oficial

R4 CNPD — Direitos dos titulares

Exercício dos direitos, prazos e condições. Fonte oficial

R5 CNPD — Violação de dados pessoais

Notificação, avaliação e documentação dos incidentes. Fonte oficial

R6 CNPD — Avaliação de impacto

AIPD e consulta prévia. Fonte oficial

R7 Regulamento n.º 798/2018 da CNPD

Publicita o Regulamento n.º 1/2018: lista nacional de tratamentos sujeitos a AIPD. Fonte oficial

R8 CEPD — Orientações 07/2020, versão final

Conceitos de responsável, corresponsáveis e subcontratante. Fonte oficial

R9 CNPD — Deliberação n.º 7680/2014

Geolocalização laboral; referência anterior ao RGPD, a ler com o direito vigente. Fonte oficial

R10 Lei n.º 93/2021, de 20 de dezembro

Denunciantes: seguimento, confidencialidade, dados e conservação; artigos 11.º, 18.º–20.º. Fonte oficial

R11 CNPD — Videovigilância

Condições de instalação e conservação de imagens; verificar o regime específico da instalação. Fonte oficial

R12 CNPD — Diretriz/2022/1

Comunicações eletrónicas de marketing direto; articulação com a Lei n.º 41/2004. Fonte oficial

R13 Tribunal da Relação de Lisboa — 18 de junho de 2025

Processo 2286/24.6T8FNC.L1-4: vigilância, GPS e utilização disciplinar. Fonte oficial

R14 CEPD — Recomendações 01/2020, versão final

Medidas complementares em transferências internacionais. Fonte oficial

R15 Decreto-Lei n.º 28/2019, texto consolidado

Artigo 19.º: conservação de livros, registos e documentos de suporte; verificar normas especiais e período abrangido. Fonte oficial

R16 Constituição da República Portuguesa

Artigos 13.º e 41.º: igualdade e liberdade de consciência, religião e culto. Fonte oficial

R17 Lei n.º 93/2017, texto consolidado

Prevenção e combate à discriminação racial e étnica, cor, nacionalidade, ascendência e território de origem; alterada, designadamente, pela Lei n.º 3/2024. Fonte oficial

R18 Diretiva UE 2022 2555 sobre cibersegurança

NIS2: âmbito, governação, gestão de riscos e incidentes; artigos 2.º, 20.º, 21.º e 23.º e anexo II.

https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pt

R19 Decreto Lei 125 2025 de 4 de dezembro

Transposição nacional. Consultar o diploma e o regime anexo, incluindo âmbito, qualificação, medidas, notificações e produção de efeitos.

https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

R20 Regulamento 756 2026 de 22 de junho

Execução do regime nacional, plataforma, comunicações, QNRCS, matriz de risco, níveis de conformidade e produção de efeitos.

https://diariodarepublica.pt/dr/detalhe/regulamento/756-2026-1134399056

## Articulação com outras obrigações

Os usos de inteligência artificial são também sujeitos ao Regulamento (UE) 2024/1689 e ao respetivo regime de aplicação, quando pertinente. O cumprimento do RGPD não prova, por si só, conformidade com o regime de IA. A revisão jurídica acompanha ainda legislação de segurança privada, saúde ocupacional, segurança alimentar, comunicações eletrónicas, contratação e outras normas setoriais aplicáveis.

# Revisão e aprovação

A Gestão aprova após validação jurídica e operacional e aconselhamento do EPD quando designado. A revisão ocorre pelo menos anualmente e em alterações legais, de tecnologia, fornecedor, contrato, finalidade, incidentes relevantes ou conclusões de auditoria. O responsável de processo atualiza os documentos afetados e comprova a execução.

| Condição de aprovação | Evidência exigida |
|---|---|
| Identidade e contactos | Denominação, contactos de direitos/incidentes, suplentes e decisão sobre EPD. |
| Partes interessadas | 24 grupos avaliados por processo; grupos adicionais identificados; responsáveis e ações definidos. |
| Licitude e transparência | RAT, bases, condições especiais, avisos e prova de informação; direitos testados. |
| Conservação e segurança | Prazos concretos por conjunto, acessos, eliminação e continuidade verificados. |
| Terceiros e transferências | Papéis reais, instrumentos contratuais, países, mecanismos e garantias documentados. |
| Maior risco | AIPD, pareceres, consultas e medidas concluídos quando exigidos; nenhum tratamento novo ilícito autorizado. |
| Geolocalização e vigilância | Finalidade, proporcionalidade, configuração, informação, consultas e modo privado testados. |
| Diversidade e respeito | Secção 3.6 divulgada; canais acessíveis; formação, necessidades culturais/religiosas e não discriminação incluídas nos controlos. |
| Operacionalização | Anexos aplicáveis preenchidos; ações com responsáveis, prazos e evidências; ausência de lacunas críticas para os tratamentos aprovados. |
| Cibersegurança e NIS2 | Enquadramento e calendário documentados; responsáveis, controlos, fornecedores, incidentes e continuidade verificados; Anexos 20 a 23 preenchidos quando aplicáveis. |

| Intervenção | Nome / função | Data | Assinatura |
|---|---|---|---|
| Elaboração | [PREENCHER] | [DATA] | |
| Parecer EPD, se designado | [PREENCHER] | [DATA] | |
| Validação jurídica | [PREENCHER] | [DATA] | |
| Aprovação pela Gestão | [PREENCHER] | [DATA] | |

## Registo de divulgação e alterações

Versão divulgada: [VERSÃO] · data: [DATA] · destinatários e canal: [PREENCHER]. Responsável pela divulgação, formação e arquivo: [PREENCHER]. Substituir cópias obsoletas e conservar o histórico de versões em acesso controlado.

| Versão | Alteração principal |
|---|---|
| 1.3 · 25/09/2026 | Princípios, procedimentos, geolocalização e registo inicial de partes interessadas. |

| Versão | Alteração principal |
|---|---|
| 2.0 · 25/09/2026 | 24 grupos, 19 anexos, aprofundamento operacional, igualdade e respeito pela diversidade. |
| 2.1 · 25/09/2026 | Fecho documental, precisão dos limites da biometria, reforço da igualdade e revisão da apresentação e navegação. |
| 2.2 · 25/09/2026 | Integração de oito árvores de decisão nas secções correspondentes; atualização dos índices e da paginação. |
| 2.3 · 25/09/2026 | Layout ICA conforme modelo; articulação NIS2 e regime português; dois novos fluxogramas; quatro anexos e ligações aos procedimentos existentes. |