

TESTE DE BALANCEAMENTO

TESTE DE BALANCEAMENTO				Importância	Conformidade	
Critério / Princípio	Justificativa	Evidência	Observação	Peso (1-5)	Nota (1-5)	Peso x Nota
Finalidade (Art. 6, I)	O tratamento possui finalidade legítima, específica e informada ao titular.	Documentos de Política de Privacidade, Termos de Uso, contratos, NDA	Verificar se a finalidade é compatível com a atividade-fim da empresa.	5	3	15
Adequação (Art. 6, II)	Os dados tratados são compatíveis com a finalidade declarada.	Mapeamento de dados, inventário de tratamento.	Evita desvios de uso ou finalidade oculta. / Maquina esta isolada	5	3	15
Necessidade (Art. 6, III)	Apenas os dados estritamente necessários são coletados.	Formulários, sistemas de CRM/ERP.	Avaliar a exclusão de dados desnecessários. Evita coleta excessiva e riscos desnecessários. / Data; Equipamento; Crachá; Nome do usuário; Usuário; Status; Origem; Mensagem; Descrição Motivo Bloqueio	5	3	15
Livre Acesso (Art. 6, IV)	O titular pode consultar seus dados de forma fácil e gratuita.	Canais de atendimento, portal do titular.	Importante para autodeterminação informativa. / Validar se será via Talievi ou Controlador (Operador ou Controlador) - Controlador mais seguro e correto / Ttular não pode exercer todos os direitos com o Operador	4	3	12
Qualidade dos Dados (Art. 6, V)	Os dados são atualizados, exatos e pertinentes.	Registro de atualizações, logs, auditorias.	Prever rotinas de revisão e retificação de dados. / Retenção somente durante contrato ou a pedido da Controlador / Quanto mais tempo menos Qualidade	4	3	12
Transparência (Art. 6, VI)	Informações claras, precisas e acessíveis ao titular.	Políticas e avisos de privacidade publicados.	Linguagem simples e acessível. Verificar se o Controlador fez algum comunicado	4	3	12
Segurança (Art. 6, VII)	Medidas técnicas e administrativas para proteger os dados.	Plano de Segurança da Informação, ISO 27701 29100 29134 16167 31000 I.N 01062016	Inclui criptografia, controle de acesso, backups. / Muitos controles pertencem ao Controlador	3	3	9
Prevenção (Art. 6, VIII)	Ações para evitar danos decorrentes do tratamento.	RIPD, treinamentos, testes de invasão.	Proatividade na segurança e privacidade. / Sendo Feito	4	2	8
Não Discriminação (Art. 6, IX)	O tratamento não é realizado com propósitos discriminatórios ou abusivos.	Políticas internas de equidade e ética.	Reavaliar dados sensíveis e critérios de seleção.	4	3	12
Responsabilização e Prestação de Contas (Art. 6, X)	O controlador demonstra conformidade com a LGPD.	Relatórios de auditoria, nomeação de DPO, registros de tratamento.	Manter evidências de governança e conformidade.	4	4	16
Segurança Organizacional	Controles administrativos internos e externos eficazes.	Política de segurança da informação, treinamento periódico.	Complementa segurança técnica com governança robusta.	5	4	20
Minimização de Dados	Tratamento limitado ao mínimo necessário.	Configuração de formulários, coleta por padrão mínima.	Conceito essencial para compliance e eficiência. / Existem compos que não estão sendo usados -Eliminar até mesmo o campo - Risco de alguém coletar	4	3	12
Direitos do Titular	Observância aos direitos previstos nos artigos 9º e 18º e seguintes da LGPD.	Registros de solicitações, SLAs de atendimento.	Engloba acesso, correção, eliminação, oposição, entre outros. / Acionar Controlador - Titular não exerce direitos com o Operador	3	5	15
Avaliação de Riscos	Identificação e classificação de riscos à privacidade.	Relatórios de RIPD, metodologias de risco (ex. ISO 31000).	Base para priorização de medidas mitigadoras.	3	4	12
Medidas Mitigadoras	Adoção de controles técnicos e administrativos que reduzem riscos.	Plano de ação, logs de monitoramento, firewall, DLP.	Devem ser documentadas e auditáveis.	5	3	15
Riscos Potenciais	Consequências possíveis de falhas no tratamento.	Impacto avaliado por categoria de risco e tipo de dado.	Fundamento para decisões de continuidade ou revisão.	3	5	15
Retenção e Exclusão de Dados	Política clara de prazos e critérios de descarte.	Registro de logs, cronogramas de retenção, automação de exclusão.	Evita armazenamento indefinido e risco legal.	4	4	16
Impacto em Caso de Violação	Estimativa do impacto potencial sobre o titular em caso de incidente.	BIA, plano de resposta a incidentes, plano de notificação.	Mede gravidade e necessidade de mitigação adicional.	5	4	20
Conformidade Legal e Regulamentar	Atendimento às obrigações legais e regulamentares setoriais.	Normas ANPD, normas setoriais, parecer jurídico.	Complementa a base legal da LGPD com outras obrigações legais.	4	5	20
Natureza dos Dados Tratados	Classificação dos dados tratados (simples, sensíveis, biométricos etc.).	Inventário classificado, mapeamento sensível.	Critérios mais exigentes para dados sensíveis.	5	5	25
Alternativas Menos Invasivas	Análise de opções menos intrusivas para atingir a mesma finalidade.	Estudo de viabilidade, testes A/B de abordagem.	Apenas seguir com a opção mais invasiva se devidamente justificado.	2	4	8

Interesse Legítimo do Controlador	O interesse do controlador é real, legítimo, atual e relevante.	Documento de fundamentação jurídica e comercial.	Necessário demonstrar equilíbrio entre interesses.	5	5	25
Direitos e Liberdades do Titular	O tratamento não interfere desproporcionalmente nos direitos do titular.	Análise de impacto à privacidade (RIPD).	Essencial para sustentar o legítimo interesse.	4	5	20
Interesse Legítimo	Interesse real e justificado do controlador, com impacto mínimo aos titulares.	Documento de fundamentação legal e comercial.	Comparar com direitos e expectativas dos titulares.	5	5	25
Direitos e Liberdades do Titular (Art. 7, IX)	Não há violação de direitos fundamentais.	Avaliação de impacto à privacidade (RIPD).	Equilíbrio entre o interesse do controlador e o direito do titular.	3	4	12
Alternativas Menos Invasivas (Art. 7, IX)	Não existem formas menos intrusivas de atingir a finalidade.	Análise de viabilidade de outras abordagens.	Documentar decisão. - RIPD	4	3	12
Proporcionalidade (Art. 7, IX)	O tratamento é proporcional aos objetivos e riscos.	Matriz de risco/benefício.	Evitar excessos. - RIPD	4	3	12
Avaliação de Riscos (Art. 7, IX)	Identificação dos riscos potenciais à privacidade.	RIPD, relatórios de risco.	Atualização periódica recomendada.	4	3	12
Medidas Mitigadoras (Art. 7, IX)	Soluções para reduzir riscos identificados.	Implementação de controles e procedimentos.	Verificar eficiência dos controles.	4	3	12
Retenção e Exclusão de Dados (Art. 7, IX)	Existem regras claras de retenção e descarte.	Políticas de retenção, logs de exclusão.	Evitar armazenamento indefinido.	4	4	16
Natureza dos Dados (Art. 7, IX)	Tipo de dado tratado (simples/sensível/alto risco).	Classificação da informação.	Dados sensíveis exigem proteção reforçada. - ROPA	3	5	15
				390	116	319
				82%		
		Bom	Conforme esperado, aceitável / Conformidade adequada — poucas lacunas			

Percentual (%)	Avaliação	Significado	Ação Recomendada
90% a 100%	Excelente	Muito bom, alto nível de conformidade / Conformidade elevada — tratamento seguro e proporcional	Prosseguir com segurança
75% a 89%	Bom	Conforme esperado, aceitável / Conformidade adequada — poucas lacunas	Pode prosseguir com ajustes pontuais
50% a 74%	Regular	Precisa melhorar, atenção necessária /Conformidade parcial — riscos relevantes	Não recomendado sem mudanças significativas
25% a 49%	Ruim	Baixa conformidade, risco alto / Tratamento arriscado ou desproporcional	
0% a 24%	Muito Ruim	Não conforme, alto risco, ação urgente / Tratamento arriscado ou desproporcional	

Bases Legais Reconhecimento Facial/Digital/Senha - Código de Acesso -Token (LGPD)

Método	Bases Legais Possíveis	Observações	Justificativa	Riscos e Mitigações
Reconhecimento Facial	Consentimento (Art. 7º, I)	Consentimento deve ser informado e específico, podendo ser revogado.	Caso de visitantes ou terceiros onde o reconhecimento facial seja facultativo.	Consentimento pode ser revogado, exigindo métodos alternativos de acesso. / Senha ou liberação na Catraca / Falsos positivos/negativos
	Execução de contrato (Art. 7º, V)	Legítimo interesse deve ser ponderado e documentado com análise de impacto à privacidade. - Higienização maior	Aplicável para colaboradores que possuem vínculo formal. Controle de acesso necessário para execução do contrato de trabalho.	Revogação do acesso em desligamento imediato. / Controle e intereção maior com o Controlador / Falsos positivos/negativos
	Legítimo interesse (Art. 7º, IX)	Usado em segurança e controle de acesso.	Garantir segurança física de pacientes e colaboradores. O interesse do hospital prevalece sobre riscos, desde que haja medidas técnicas e organizacionais para proteção dos dados.	Risco de vazamento ou uso indevido de dados biométricos. / / Falsos positivos/negativos
	Obrigaç�o legal ou regulat�ria (Art. 7º, II)	Obriga�o legal		Mitiga�o: criptografia, controle restrito de acesso, monitoramento. / Maquina somente para acesso sem acesso a internet ou a rede / / Falsos positivos/negativos
Impress�o Digital (Biometria)	Mesmas bases do reconhecimento facial:	Dado biom�trico � sens�vel, requer cuidados redobrados.	Mesmo racional para dados biom�tricos sens�veis. -Algo que voc� �.	Mesmas mitiga�o que reconhecimento facial.
	Consentimento	Consentimento claro ou outra base legal s�lida � obrigat�rio.		
	Execu�o de contrato	Execu�o de contrato		
	Leg�timo interesse	Usado em seguran�a e controle de acesso.		
	Obriga�o legal	Obriga�o legal		
Senha / C�digo de Acesso / Token	Execu�o de contrato (Art. 7º, V)	Senha � dado pessoal comum, geralmente menos sens�vel.	Necess�ria para colaboradores como meio de identifica�o segura para acesso.	Risco de compartilhamento ou esquecimento. Mitiga�o: pol�ticas de troca per�dica e treinamentos.
	Leg�timo interesse (Art. 7º, IX)	Necess�rio para execu�o de contrato (ex: v�nculo empregat�cio).	Para acessos tempor�rios (ex: visitantes), visando prote�o do ambiente hospitalar.	Controle de validade limitada e monitoramento de acessos. / Pode ser perdido
	Obriga�o legal (Art. 7º, II)	N�o depende de consentimento.	Senha - Algo que voc� sabe / Token (f�sico ou digital) - Algo que voc� tem	- Algo que voc�s conhece. / Pode ser adivinhada ou vazada

Base - Legítimo Interesse

Critério	Descrição / Avaliação
Finalidade do tratamento	Controle de acesso seguro a áreas restritas do hospital (ex: UTI, farmácia, almoxarifado, centro cirúrgico, restaurante) com o objetivo de proteger pacientes, profissionais e visitantes.
	O objetivo é específico para o tratamento dos dados.
Tipo de dado tratado	Dado pessoal sensível – biometria facial (Art. 5º, II da LGPD).
Base legal	Legítimo Interesse do controlador (Art. 7º, IX da LGPD) e exceção para dados sensíveis (Art. 11, II, “f”).
Interesse legítimo do controlador	Garantir a segurança física de pacientes, profissionais e instalações hospitalares. Prevenir acessos não autorizados.
	Existe relação prévia e direta com os titulares (funcionários, pacientes, prestadores, etc.)
	O tratamento garante a prevenção à fraude e à segurança do titular,
Necessidade do tratamento	O reconhecimento facial é mais seguro, higiênico (sem toque) e menos sujeito a fraudes do que senhas ou crachás.
	Profissionais, pacientes e terceiros compreendem que o hospital deve garantir um ambiente seguro.
Alternativas menos invasivas?	Sim (senhas, cartões), mas menos eficazes e mais suscetíveis a compartilhamento ou perda. O método biométrico é mais robusto.
Expectativa do titular	Alta: em hospitais, espera-se controle rígido de acesso. A visibilidade do sistema e avisos reforçam essa expectativa.
Proporcionalidade	O tratamento é proporcional à finalidade não sendo reutilizado para outras finalidade. Apenas dados necessários são tratados. O uso é restrito ao controle de acesso.
Riscos à privacidade	Vazamento, uso indevido, acesso não autorizado, ausência de controle sobre retenção e descarte.
Medidas de mitigação adotadas	- Criptografia dos dados
	- Acesso restrito
	- Registros de auditoria
	- Prazos claros de retenção e descarte
	- Alternativa para quem não aceitar biometria
Transparência com o titular	Política de privacidade acessível; avisos de uso; canal de atendimento para dúvidas e direitos.
Benefício para o Controlador	Prevenção de acessos não autorizados, redução de fraudes.
	Ambiente hospitalar mais seguro.
Conclusão do balanceamento	O tratamento é legítimo, necessário e proporcional. Os direitos dos titulares são respeitados e protegidos com medidas adequadas de segurança e transparência. / Ágil (evita filas e atrasos no atendimento); / Seguro (menos suscetível a fraudes do que cartões ou senhas); / Higiênico (sem contato físico, essencial em ambiente hospitalar). / Alternativas como crachás e senhas apresentam riscos maiores de uso indevido, perda ou compartilhamento indevido.

IMPACTO BIOMETRIA

Aspecto	Descrição	Avaliação / Impacto	Justificativa e Considerações
Interesse do Controlador - LGPD	Garantir a segurança física e patrimonial no ambiente	Alto	Segurança do hospital e proteção de pacientes, colaboradores e visitantes é fundamental - Mais higiênico em ambiente hospitalar
Direitos e Liberdades do Titular - LGPD	Proteção da privacidade e dados pessoais sensíveis	Alto	Dados biométricos são sensíveis e demandam cuidados rigorosos na coleta, armazenamento e uso
Finalidade Específica e Transparente - LGPD	Dados coletados apenas para controle de acesso e segurança	Essencial	Transparência e comunicação clara para titulares são obrigatórias
Minimização de Dados	Coleta limitada ao necessário para atingir o objetivo	Adequada	Apenas dados faciais biométricos, sem coleta de dados adicionais irrelevantes
Segurança Técnica	Proteção dos dados contra acessos não autorizados, vazamentos	Rigorosa	Uso de criptografia, autenticação forte, monitoramento e auditorias regulares
Segurança Organizacional	Políticas internas, treinamentos e controles de acesso	Rigorosa	Garantia de uso ético e responsável da tecnologia
Avaliação de Riscos	Identificação e mitigação de riscos à privacidade e segurança	Obrigatória	DPIA (Análise de Impacto à Proteção de Dados) recomendada para mapear riscos e definir controles
Direitos do Titular	Garantia de acesso, correção, exclusão e revogação do consentimento	Fundamental	Procedimentos claros para atendimento a solicitações dos titulares
Alternativas para Titulares	Disponibilização de outros métodos para quem não deseja biometria	Necessário	Alternativas como senha, cartão ou outros métodos de autenticação devem ser oferecidas
Proporcionalidade e Necessidade	Uso da biometria é proporcional ao objetivo e imprescindível para segurança	Deve ser justificado	Justificar que métodos tradicionais não oferecem o mesmo nível de segurança ou praticidade
Transparência e Comunicação	Informação clara e acessível sobre o tratamento de dados	Obrigatória	Política de privacidade atualizada e canais de comunicação eficientes
Retenção e Exclusão de Dados	Tempo limitado para armazenamento e procedimentos para exclusão	Essencial	Dados mantidos pelo tempo necessário e removidos ao término da necessidade ou pedido do titular - Usar Picotadora
Impacto em Caso de Violação	Consequências para titulares em eventual vazamento ou uso indevido	Elevado	Dados biométricos comprometidos podem causar danos graves à privacidade e segurança pessoal / Possível exposição e discriminação se dados vazarem
Conformidade Legal e Regulamentar	Atendimento às disposições da LGPD e demais normas aplicáveis	Obrigatório	Auditorias periódicas e revisões para garantir conformidade contínua
Natureza dos Dados	Tipo de dado tratado (biometria facial, considerado sensível)	Sensível	Biometria tem alto risco se vazada ou mal utilizada
Riscos Potenciais	Vazamento, uso indevido, discriminação, falhas técnicas	Moderado a Alto	Risco elevado devido à sensibilidade do dado
Medidas Mitigadoras	Procedimentos para minimizar riscos	Implementadas	Controles técnicos e organizacionais robustos
Alternativas Disponíveis	Opções para titulares que não desejam usar biometria	Sim	Senha, cartão, reconhecimento manual
Necessidade e Proporcionalidade	Uso da biometria é necessário e proporcional ao fim	Adequada	Tecnologia justificada pela criticidade da segurança hospitalar

Nota (1–5)									
Item	Total	Total	Impacto	Risco	Frequência	Conformidade	Pontuação Total	Prioridade	Ponderada %
Facilita o acesso de forma fluida e rápida.	15		5	4	3	4	16	Emergência	84%
Integrável a CRMs, sistemas de RH, catracas eletrônicas e ERPs.	15		3	2	4	2	11	Urgente	56%
Automatiza processos de identificação e autenticação.	15		2	2	3	3	10	Urgente	46%
Permite integração com sistemas de vigilância, registro de ponto e BI (business intelligence).	15		4	4	3	3	14	Urgente	74%
Elimina o contato físico com superfícies (comparado a digitais, cartões ou teclados).	15		5	5	4	5	19	Emergência	96%
Possibilita cruzamento com outras bases (ex: listas de bloqueio, visitantes agendados).	15		4	3	3	4	14	Urgente	70%
Suporta políticas de segurança corporativa com mais precisão.	15		5	4	3	4	16	Emergência	84%
Reduz filas e necessidade de pessoal para checagem manual.	15		3	3	3	3	12	Urgente	60%
Facilita a rastreabilidade de eventos e pessoas (quem entrou, quando e onde).	15		3	2	2	3	10	Urgente	50%
Reduz necessidade de vigilância humana constante.	15		3	2	4	2	11	Urgente	56%
Controla acesso a salas limpas, UTI, centros cirúrgicos, laboratórios.	17		3	3	3	2	11	Urgente	58%
Restringe entrada de terceiros a ambientes de risco biológico.	17		3	3	4	2	12	Urgente	62%
Gera relatórios de acesso, horários de entrada e saída, e padrões de comportamento.	18		5	5	4	5	19	Emergência	96%
Pode ser combinado com sistemas de IA, machine learning e reconhecimento de comportamento.	18		5	5	3	5	18	Emergência	92%
Ideal para ambientes sensíveis como hospitais, laboratórios e cozinhas industriais.	18		4	3	3	3	13	Urgente	68%
Aumenta a velocidade do controle de entrada/saída (sem contato físico).	18		3	3	2	3	11	Urgente	56%
Menor custo com fraudes ou acessos indevidos.	18		4	4	3	3	14	Urgente	74%
Evita a necessidade de portar crachá, senha ou chave física.	18		2	2	3	2	9	Importante	44%
Diminui despesas com reposição de crachás, senhas e chaves.	18		2	2	4	2	10	Urgente	48%
Ajuda no cumprimento de normas regulatórias (ex: segurança do trabalho, ANVISA, LGPD com cuidados).	18		4	5	3	4	16	Emergência	82%
Reduz fraudes de identidade (não pode ser facilmente replicado como crachás ou senhas).	18		5	5	4	5	19	Emergência	96%
Pode ser combinado com alertas em tempo real (ex: tentativa de acesso por pessoa não autorizada).	18		3	3	4	2	12	Urgente	62%
Gera menos atrito no dia a dia de colaboradores e visitantes.	18		5	4	2	5	16	Emergência	82%
Controla rigorosamente o acesso a áreas restritas e sensíveis.	19		3	2	4	2	11	Urgente	56%
Permite auditoria e rastreamento de acessos com precisão.	21		5	4	2	4	15	Emergência	80%
Garante que apenas profissionais autorizados tenham acesso a medicamentos controlados.	21		5	5	2	5	17	Emergência	88%

ITEM	VANTAGEM	Segurança (1-3)	Eficiência (1-3)	Conformidade (1-3)	Experiência (1-3)	Total
Segurança Reforçada	Reduz fraudes de identidade (não pode ser facilmente replicado como crachás ou senhas).	2	3	2	2	18
	Controla rigorosamente o acesso a áreas restritas e sensíveis.	2	3	3	1	19
	Permite auditoria e rastreamento de acessos com precisão.	2	3	3	3	21
	Pode ser combinado com alertas em tempo real (ex: tentativa de acesso por pessoa não autorizada).	3	2	2	1	18
Eficiência Operacional	Automatiza processos de identificação e autenticação.	2	3	1	1	15
	Aumenta a velocidade do controle de entrada/saída (sem contato físico).	3	2	2	1	18
	Reduz filas e necessidade de pessoal para checagem manual.	2	3	1	1	15
Experiência do Usuário	Evita a necessidade de portar crachá, senha ou chave física.	3	2	2	1	18
	Facilita o acesso de forma fluida e rápida.	2	3	1	1	15
	Gera menos atrito no dia a dia de colaboradores e visitantes.	3	2	2	1	18
Higiene e Segurança Sanitária	Elimina o contato físico com superfícies (comparado a digitais, cartões ou teclados).	2	3	1	1	15
	Ideal para ambientes sensíveis como hospitais, laboratórios e cozinhas industriais.	3	2	2	1	18
Monitoramento e Análise Inteligente	Permite integração com sistemas de vigilância, registro de ponto e BI (business intelligence).	2	3	1	1	15
	Gera relatórios de acesso, horários de entrada e saída, e padrões de comportamento.	3	2	2	1	18
	Possibilita cruzamento com outras bases (ex: listas de bloqueio, visitantes agendados).	2	3	1	1	15
Redução de Custos a Longo Prazo	Diminui despesas com reposição de crachás, senhas e chaves.	3	2	2	1	18
	Reduz necessidade de vigilância humana constante.	2	3	1	1	15
	Menor custo com fraudes ou acessos indevidos.	3	2	2	1	18
	Facilita a rastreabilidade de eventos e pessoas (quem entrou, quando e onde).	2	3	1	1	15

Conformidade e Auditoria	Ajuda no cumprimento de normas regulatórias (ex: segurança do trabalho, ANVISA, LGPD com cuidados).	3	2	2	1	18
	Suporta políticas de segurança corporativa com mais precisão.	2	3	1	1	15
Integração com outras tecnologias	Pode ser combinado com sistemas de IA, machine learning e reconhecimento de comportamento.	3	2	2	1	18
	Integrável a CRMs, sistemas de RH, catracas eletrônicas e ERPs.	2	3	1	1	15
Aplicações específicas para saúde	Controla acesso a salas limpas, UTI, centros cirúrgicos, laboratórios.	2	3	1	3	17
	Restringe entrada de terceiros a ambientes de risco biológico.	2	3	1	3	17
	Garante que apenas profissionais autorizados tenham acesso a medicamentos controlados.	2	3	3	3	21

ITEM	VANTAGEM	Segurança (1-3)	Eficiência (1-3)	Conformidade (1-3)	Experiência (1-3)	Total
Segurança Reforçada	Reduz fraudes de identidade (não pode ser facilmente replicado como crachás ou senhas).	2	3	2	2	18
	Controla rigorosamente o acesso a áreas restritas e sensíveis.	2	3	3	1	19
	Permite auditoria e rastreamento de acessos com precisão.	2	3	3	3	21
	Pode ser combinado com alertas em tempo real (ex: tentativa de acesso por pessoa não autorizada).	3	2	2	1	18
Eficiência Operacional	Automatiza processos de identificação e autenticação.	2	3	1	1	15
	Aumenta a velocidade do controle de entrada/saída (sem contato físico).	3	2	2	1	18
	Reduz filas e necessidade de pessoal para checagem manual.	2	3	1	1	15
Experiência do Usuário	Evita a necessidade de portar crachá, senha ou chave física.	3	2	2	1	18
	Facilita o acesso de forma fluida e rápida.	2	3	1	1	15
	Gera menos atrito no dia a dia de colaboradores e visitantes.	3	2	2	1	18
Higiene e Segurança Sanitária	Elimina o contato físico com superfícies (comparado a digitais, cartões ou teclados).	2	3	1	1	15
	Ideal para ambientes sensíveis como hospitais, laboratórios e cozinhas industriais.	3	2	2	1	18
Monitoramento e Análise Inteligente	Permite integração com sistemas de vigilância, registro de ponto e BI (business intelligence).	2	3	1	1	15
	Gera relatórios de acesso, horários de entrada e saída, e padrões de comportamento.	3	2	2	1	18
	Possibilita cruzamento com outras bases (ex: listas de bloqueio, visitantes agendados).	2	3	1	1	15
Redução de Custos a Longo Prazo	Diminui despesas com reposição de crachás, senhas e chaves.	3	2	2	1	18
	Reduz necessidade de vigilância humana constante.	2	3	1	1	15
	Menor custo com fraudes ou acessos indevidos.	3	2	2	1	18
	Facilita a rastreabilidade de eventos e pessoas (quem entrou, quando e onde).	2	3	1	1	15

Conformidade e Auditoria	Ajuda no cumprimento de normas regulatórias (ex: segurança do trabalho, ANVISA, LGPD com cuidados).	3	2	2	1	18
	Suporta políticas de segurança corporativa com mais precisão.	2	3	1	1	15
Integração com outras tecnologias	Pode ser combinado com sistemas de IA, machine learning e reconhecimento de comportamento.	3	2	2	1	18
	Integrável a CRMs, sistemas de RH, catracas eletrônicas e ERPs.	2	3	1	1	15
Aplicações específicas para saúde	Controla acesso a salas limpas, UTI, centros cirúrgicos, laboratórios.	2	3	1	3	17
	Restringe entrada de terceiros a ambientes de risco biológico.	2	3	1	3	17
	Garante que apenas profissionais autorizados tenham acesso a medicamentos controlados.	2	3	3	3	21

Resumo:

Teste de Balanceamento e Legítimo Interesse na LGPD

O Teste de Balanceamento e a exigência da LGPD para uso do fundamento do Legítimo Interesse compará-los:

Interesses do controlador ou de terceiros



VS

Direitos e liberdades fundamentais dos titulares



Considerações para cada finalidade específica

- ✓ A legitimidade e necessidade do interesse
- ✓ Os riscos e impactos ao titular
- ✓ As legítimas expectativas do titular quanto ao uso de seus dados

Controlador responsável por:

- Elaborar o teste de balanceamento
- Manter registros da justificativa
- Aplicar medidas de mitigação de risco

Legítimo interesse só é válido quando:

- 1 Está em conformidade com a lei e princípios da LGPD
- 2 É baseado em situações concretas e atuais
- 3 Está vinculado a finalidades legítimas, específicas e explícitas



O titular deve ter acesso facilitado às informações sobre o tratamento realizado