



LISTA DE DOCUMENTOS E PROCESSOS RGPD

Tecnologias Imaginadas

Síntese

Resumo de todos os documentos e processos necessários e em conformidade com o disposto no Regulamento Geral de Dados Pessoais UE nº 2016/679 de 27 de Abril de 2016 (RGPD) sobre proteção de dados pessoais

CONTEÚDO

Políticas e termos	4
Termos e condições gerais	4
Direitos do Titular	5
Políticas de privacidade e confidencialidade da informação.....	8
A informação que coletamos nas nossas plataformas web.....	8
Utilização da informação por Tecnologias Imaginadas.....	9
Confidencialidade da informação.....	9
Nome de Utilizador.....	10
Senha Pessoal.....	10
Menores de idade.....	10
Uso da informação por outros Utilizadores.....	10
Ordem de autoridades competentes – Requerimentos Legais.....	11
Segurança e Armazenamento da informação.....	12
Política de Utilização Aceitável - PUA	13
Visão geral	13
Propósito	13
ÂMBITO.....	14
Política	14
Política de informação publicitária e processamento de dados com finalidades comerciais e de fidelização.....	20
Política de cookies.....	20
Política de segurança de dados: requisitos de funcionários.....	21
Usando esta política	21
Propósito	21
Âmbito	21
Política de resposta a violações de dados.....	22
Propósito	22
ÂMBITO.....	22

Funções e Responsabilidades.....	23
Enforcement.....	24
Histórico de Revisões.....	24
Política de passwords.....	24
Conformidade política.....	27
Histórico de Revisão.....	27
Comunicações e relatórios.....	28
Workflows de resposta aos titulares dos direitos.....	28
Plano de contingência.....	28
Workflow.....	28
Breach notification (notificação de violação de dados).....	29
Contratos, declarações e formulários.....	31
Contratos de subcontratação.....	31
Contratos de parceria.....	31
Declaração de consentimento.....	31
Sites.....	31
IoT.....	32
Formulário para solicitação de exercício de direito.....	32
Finalidades de tratamento.....	32
Local onde são guardados.....	33
Período em que serão utilizados.....	34
Pessoa/entidade que os forneceu.....	34
Pessoas que têm acesso aos dados.....	34
Alterações à política de privacidade.....	34
Lei e foro aplicáveis.....	34

POLÍTICAS E TERMOS

TERMOS E CONDIÇÕES GERAIS

Em conformidade com o disposto no Regulamento Geral de Dados Pessoais UE nº 2016/679 de 27 de Abril de 2016 (RGDP) sobre proteção de dados pessoais, os termos e condições gerais seguintes, regulam o tratamento realizado pela Tecnologias Imaginadas.

As restantes Políticas, Normas e Regulamentos da Tecnologias Imaginadas devem ser devidamente enquadradas e mediante a aceitação dos Termos e Condições Gerais, está implícito que o utilizador as aceita.

Em termos gerais, a **Tecnologias Imaginadas** utiliza os Dados do Titular para as seguintes finalidades:

1. A atividade associada a uma empresa de Sistemas de informação e comunicação/tecnologia;
2. Fornecimento aos intervenientes nos serviços solicitados pelo utilizador para concretização dos serviços contratados pelo Utilizador / Cliente;
3. Gestão, administração, prestação, ampliação e melhoria dos serviços em que o utilizador / cliente decida subscrever-se e registar-se ou utilizar a adequação desses serviços às preferências e gostos dos utilizadores;
4. Verificar cartões de crédito e outros tipos de cartões utilizados no pagamento e indicados pelo próprio Utilizador / Cliente;
5. O estudo da utilização dos serviços por parte dos utilizadores;
6. Verificar, manter e desenvolver sistemas e análises estatísticas, para uso da empresa com a finalidade de melhorar os serviços/produtos disponibilizados ao mercado.
7. Atividades de publicidade, promoção e prospeção se devidamente aceite pelo Utilizador;
8. Enviar formulários de inquéritos aos quais o utilizador não fica obrigado a responder;
9. Enviar mensagens SMS com fins de venda direta, publicitários ou relacionados com o serviço contratado.

O utilizador deve consentir, através de formulário próprio ou de documento suficientemente explícito, que a Tecnologias Imaginadas, trate os seus Dados Pessoais com a finalidade de determinar o seu perfil e oferecer-lhe produtos e serviços adequados. Estes serviços podem ser próprios ou de terceiros (Ex.: SAAS).

DIREITOS DO TITULAR

O Titular dos dados tem salvaguardados a todo o momento os direitos estabelecidos pelo RGPD, nomeadamente:

- DIREITO DE ACESSO AOS DADOS PESSOAIS

A **Tecnologias Imaginadas** garante os meios que permitam o acesso, pelo Titular, aos seus dados pessoais. Todo e qualquer acesso é apenas garantido após identificação inequívoca do titular dos dados, o que poderá implicar o pedido de comprovativo de identificação.

O Titular tem o direito de obter da **Tecnologias Imaginadas** a confirmação de que os dados pessoais que lhe dizem respeito são ou não objeto de tratamento.

O Titular pode a qualquer momento solicitar à **Tecnologias Imaginadas**, a título gratuito, uma cópia dos seus Dados Pessoais que a empresa tenha em sua posse. O fornecimento de outras cópias solicitadas pelo Titular poderá acarretar custos administrativos.

- DIREITO DE RETIFICAÇÃO DOS DADOS PESSOAIS

O Titular tem o direito de solicitar, a qualquer momento, a retificação dos seus dados pessoais e, bem assim, o direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

Em caso de retificação dos dados, a **Tecnologias Imaginadas** comunica a cada destinatário a quem os dados tenham sido transmitidos a respetiva retificação, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado para a **Tecnologias Imaginadas**.

- DIREITO AO APAGAMENTO DOS DADOS PESSOAIS ("DIREITO A SER ESQUECIDO")

O Titular tem o direito de obter, por parte da **Tecnologias Imaginadas**, o apagamento dos seus dados quando se aplique um dos seguintes motivos:

- Os Dados do Titular deixarem de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
- O Titular retirar o consentimento em que se baseia o tratamento dos dados e não existir outro fundamento jurídico para o referido tratamento;
- Caso os Dados do Titular sejam tratados ilicitamente;
- Caso os Dados do Titular tiverem de ser apagados para o cumprimento de uma obrigação jurídica a que a **Tecnologias Imaginadas** esteja sujeita.

Nos termos legais aplicáveis, a **Tecnologias Imaginadas** não tem a obrigação de apagar os Dados do Titular na medida em que o tratamento se revele necessário à execução de um contrato no qual o titular dos dados é parte ou ao cumprimento de uma obrigação legal a que a **Tecnologias Imaginadas** esteja sujeita ou para efeitos de declaração, exercício ou defesa de um direito da **Tecnologias Imaginadas** num processo judicial.

Em caso de apagamento dos dados, a **Tecnologias Imaginadas** comunica a cada destinatário/entidade a quem os dados tenham sido transmitidos o respetivo apagamento, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado para a **Tecnologias Imaginadas**.

Quando a **Tecnologias Imaginadas** tiver tornado públicos os Dados do Titular e for obrigada a apagá-los ao abrigo do direito ao apagamento, a **Tecnologias Imaginadas** compromete-se a assegurar as medidas que forem razoáveis, incluindo de carácter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o Titular lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

- DIREITO À LIMITAÇÃO DO TRATAMENTO DOS DADOS PESSOAIS

O Titular tem o direito de obter, por parte da **Tecnologias Imaginadas**, a limitação do tratamento dos Dados do Titular, se se aplicar uma das seguintes situações (a limitação consiste em inserir uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro):

- Se contestar a exatidão dos dados pessoais, durante um período que permita à **Tecnologias Imaginadas** verificar a exatidão;
- Se o tratamento for ilícito e o Titular se opuser ao apagamento dos dados, solicitando, em contrapartida, a limitação da sua utilização;
- Se a **Tecnologias Imaginadas** já não precisar dos Dados do Titular para fins de tratamento, mas esses dados sejam requeridos pelo Titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
- Caso o Titular se tenha oposto ao tratamento, até se verificar que os motivos legítimos
- da **Tecnologias Imaginadas** prevalecem sobre os do Titular.

Quando os Dados do Titular sejam objeto de limitação, só poderão, à exceção da conservação, ser tratados com o consentimento do Titular ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos de interesse público legalmente previstos. O Titular que tiver obtido a limitação do tratamento dos seus dados nos casos acima referidos será informado pela **Tecnologias Imaginadas** antes de ser anulada a limitação ao tratamento.

Em caso de limitação do tratamento dos dados, a **Tecnologias Imaginadas** comunicará a cada destinatário a quem os dados tenham sido transmitidos a respetiva limitação, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado para a **Tecnologias Imaginadas**.

- DIREITO DE PORTABILIDADE DOS DADOS PESSOAIS

O Titular tem o direito de receber os Dados Pessoais que lhe digam respeito e que tenha fornecido à **Tecnologias Imaginadas**, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento, se:

- O tratamento se basear no consentimento ou num contrato de que o Titular é parte;
- O tratamento for realizado por meios automatizados.

O direito de portabilidade não inclui dados inferidos nem dados derivados, i.e., dados pessoais que sejam gerados pela **Tecnologias Imaginadas** como consequência ou resultado da análise dos dados objeto de tratamento, mas apenas os dados pessoais que o Titular legalmente cedeu.

O Titular tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

- DIREITO DE OPOSIÇÃO AO TRATAMENTO

O Titular tem o direito de se opor ao tratamento dos dados pessoais a qualquer momento, por motivos relacionados com a sua situação particular, nos seguintes casos:

- Quando o tratamento for efetuado para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos, incluindo a definição de perfis;
- Quando os dados pessoais forem tratados para fins estatísticos.

A **Tecnologias Imaginadas** cessará o tratamento dos Dados do Titular, salvo se apresentar razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do Titular, ou para efeitos de declaração, exercício ou defesa de um direito da **Tecnologias Imaginadas** num processo judicial.

Caso o Titular se oponha ao tratamento dos seus dados para efeitos de comercialização direta, a **Tecnologias Imaginadas** cessa o tratamento dos dados para esse fim.

O Titular tem ainda o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, salvo se a decisão:

- For necessária para a celebração ou a execução de um contrato entre o Titular e a **Tecnologias Imaginadas**;
- For autorizada por legislação a que a **Tecnologias Imaginadas** estiver sujeita;
- For baseada no consentimento explícito do Titular.

POLÍTICAS DE PRIVACIDADE E CONFIDENCIALIDADE DA INFORMAÇÃO.

A privacidade dos dados dos seus clientes é muito importante para a **Tecnologias Imaginadas**. Por essa razão, tomamos as devidas precauções e cuidados para proteger sua informação, utilizando os mais completos e eficazes mecanismos de segurança cibernética para proteção de dados.

Este documento é parte integrante dos Termos e Condições Gerais da **Tecnologias Imaginadas**. Mediante a aceitação dos Termos e Condições Gerais, o utilizador aceita as políticas aqui contidas.

A INFORMAÇÃO QUE COLETAMOS NAS NOSSAS PLATAFORMAS WEB.

A primeira providência para desfrutar dos serviços web de **Tecnologias Imaginadas** é registar-se, introduzindo dados pessoais ("Informação Pessoal") completos e exatos. A

informação obtida será tratada de forma confidencial. Expressamente se acorda que a qualquer momento o utilizador registado em **CareTracker** poderá solicitar a remoção ou encerramento de seu registo e/ou o encerramento da sua conta, bem como a eliminação da sua conta e informações da(s) base(s) de dados. **Tecnologias imaginadas** recolhe e armazena automaticamente algumas informações sobre a atividade dos utilizadores e visitantes de seu site. Tais informações podem incluir ações realizadas, serviços escolhidos, avaliações e respostas enviadas, dentre outras informações que possam ser armazenadas.

UTILIZAÇÃO DA INFORMAÇÃO POR TECNOLOGIAS IMAGINADAS.

Para fornecer um serviço de qualidade e para que os Usuários possam realizar operações de forma ágil e segura, a **Tecnologias Imaginadas** requer certas informações de carácter pessoal, incluindo endereços de e-mail. A recolha dessas informações permite-nos oferecer aos Utilizadores serviços e funcionalidades que se possam adequar às suas necessidades e personalizar os nossos serviços para fazer com que suas experiências com **Tecnologias Imaginadas** sejam o mais cómodas possível.

CONFIDENCIALIDADE DA INFORMAÇÃO.

Uma vez registado em seu web site, **Tecnologias Imaginadas** não venderá ou compartilhará dados pessoais do Titular, exceto nas formas estabelecidas nestas políticas, e será feito tudo o que estiver ao alcance no sentido de proteger a privacidade da informação.

Pode ocorrer que, em virtude de ordens judiciais, ou de disposições legais, **Tecnologias Imaginadas** seja compelida a revelar informações às autoridades ou terceiras partes sob certas circunstâncias, ou em casos em que terceiros possam intercepar ou aceder certas informações ou transmissões de dados de forma ilícita, casos estes em que **Tecnologias Imaginadas** não responderá pela informação que seja revelada.

NOME DE UTILIZADOR

Para interagir dentro do Site, os Utilizadores devem utilizar um nome de Utilizador que os identifique. Os Utilizadores não terão acesso à informação pessoal de outros Utilizadores, salvo quando tenham realizado com ele alguma operação através de nossa plataforma, caso em que ambas as partes receberão os dados um do outro.

SENHA PESSOAL.

Para aceder aos nossos serviços reservados unicamente aos Utilizadores devidamente cadastrados, estes irão dispor de uma senha pessoal. Esta senha deve ser mantida sob absoluta confidencialidade e, em nenhum caso, deverá ser revelada ou compartilhada com outras pessoas. O Utilizador será responsável por todos os atos que sejam realizados com o uso de seu nome de Utilizador e senha, o que inclui responder pelo pagamento de tarifas que sejam eventualmente devidas ou a responsabilização por prejuízos que possam vir a sofrer de outros Utilizadores por tal motivo. Se por qualquer razão um Utilizador desconfiar que alguém pode conhecer sua senha, deverá modificá-la ingressando, pelo menu de navegação, á área pessoal.

MENORES DE IDADE.

Nossos serviços estão apenas disponíveis para aquelas pessoas que tenham capacidade legal para os contratar. Portanto, aqueles que não cumpram com tal requisito deverão abster-se de enviar suas informações pessoais para serem incluídas em nossas bases de dados. Contudo, podem fazê-lo por meio de seus pais ou responsáveis legais.

USO DA INFORMAÇÃO POR OUTROS UTILIZADORES.

Para facilitar a interação entre todos os membros da comunidade, o nosso serviço permite um acesso limitado a certos dados de contacto dos demais Utilizadores, tais como nome de utilizador, telefones, cidade e endereço de e-mail. Sob nenhuma circunstância, se deve comunicar informação pessoal ou endereço de e-mail de outro Utilizador a nenhum terceiro sem nosso consentimento e do Utilizador afetado. Não se deve adicionar à agenda de endereços (física ou eletrônica) os dados de nenhum Utilizador, nem sequer

os dados de aqueles que tenham adquirido algum serviço oferecido em <Nome do serviço>, sem o prévio e expresso consentimento de tal Usuário.

ORDEM DE AUTORIDADES COMPETENTES – REQUERIMENTOS LEGAIS.

A **Tecnologias Imaginadas** coopera com as autoridades competentes e com terceiros para garantir o cumprimento da lei, por exemplo, em matéria de proteção de direitos de propriedade industrial e intelectual, prevenção de fraudes e outros.

A **Tecnologias Imaginadas** poderá revelar a informação pessoal de seus Utilizadores sob requerimento de autoridades judiciais ou governamentais competentes para fins de investigações conduzidas por estas, mesmo que não exista uma ordem judicial, por exemplo (e sem limitar-se a), quando se trate de investigações de caráter penal ou relacionadas com pirataria informática ou a violação de direitos de autor. Nestas situações, a **Tecnologias Imaginadas** colaborará com as autoridades competentes com o fim de salvaguardar a integridade e a segurança da Comunidade e de seus Usuários.

A **Tecnologias Imaginadas** pode (e os Usuários desde já expressamente o autorizam) comunicar qualquer Informação Pessoal sobre seus Usuários com a finalidade de cumprir a legislação aplicável e cooperar com as autoridades competentes na medida em que discricionariamente entenda necessário e adequado em relação a qualquer investigação de um ilícito, infração de direitos de propriedade industrial ou intelectual, ou outra atividade que seja ilegal ou que possa expor A **Tecnologias Imaginadas** ou seus Utilizadores a qualquer responsabilidade legal. Este direito será exercido por **Tecnologias Imaginadas** a fim de cooperar com o cumprimento e execução da lei, independentemente de existir ou não uma ordem judicial ou administrativa para o efeito.

Além disso, a **Tecnologias Imaginadas** reserva o direito de (e os Usuários desde já expressamente o autorizam) comunicar informação sobre seus Usuários a outros Usuários, entidades ou terceiros quando haja motivos suficientes para considerar que a atividade de um utilizador seja suspeita de tentar ou de cometer um delito ou tentar prejudicar a outras pessoas. Este direito será utilizado por **Tecnologias Imaginadas** a seu inteiro dispor quando considere apropriado ou necessário para manter a integridade e a segurança da Comunidade e de seus Usuários, para fazer cumprir os Termos e Condições Gerais e demais políticas do Site e com o fim de cooperar com a execução e cumprimento da lei. Este direito será exercido pela **Tecnologias Imaginadas** independentemente de existir uma ordem judicial ou administrativa nesse sentido.

SEGURANÇA E ARMAZENAMENTO DA INFORMAÇÃO.

A **Tecnologias Imaginadas** está obrigada a observar todas as normas aplicáveis em matéria de medidas de segurança de informação pessoal. Além disso, emprega os padrões mais avançados da indústria em matéria de proteção da confidencialidade das informações pessoais, a incluir, entre outras medidas, firewalls, anti-ramnsonware, anti-malware, etc.

A **Tecnologias Imaginadas** considera os dados de seus Usuários como um bem precioso que deve ser protegido de qualquer perda ou acesso não autorizado. Empregamos, portanto, diversas técnicas de segurança para proteger tais dados de acessos não autorizados por Usuários de dentro ou fora da empresa. Ainda assim, é necessário considerar que a segurança perfeita não existe no que toca a sistemas de informação/comunicação. Portanto, A **Tecnologias Imaginadas** não será responsável por intercetações ilegais ou violação de seus sistemas ou bases de dados por parte de pessoas não autorizadas. A **Tecnologias Imaginadas**, também não se responsabilizará pela indevida utilização da informação obtida por esses meios. Todos os dados pessoais dos Usuários serão armazenados em um arquivo automatizado de dados pessoais.

O arquivo de Dados Pessoais dos Usuários da **Tecnologias Imaginadas** está localizado em Portugal. O Usuário, ao cadastrar-se em <Nome do serviço>, confirma que está informado da localização deste arquivo e autoriza caso se aplique esta transferência internacional de seus dados.

POLÍTICA DE UTILIZAÇÃO ACEITÁVEL - PUA

VISÃO GERAL

As intenções da **Tecnologias Imaginadas** de publicar uma Política de Uso Aceitável não são impor restrições que sejam contrárias à cultura estabelecida de abertura, confiança e integridade da equipa. A **Tecnologias Imaginadas** está comprometida em proteger os funcionários, parceiros e a própria empresa de ações ilegais ou prejudiciais de indivíduos, conscientes ou não.

Os sistemas relacionados à Internet / Intranet / Extranet, incluindo, entre outros, equipamentos de informática, software, sistemas operacionais, dispositivos de armazenamento, contas de rede que fornecem correio eletrônico, navegação WWW e FTP, são de propriedade da **Tecnologias Imaginadas**. Esses sistemas devem ser usados para fins comerciais, servindo os interesses da empresa e de nossos clientes e no decorrer das operações relacionadas com a normal operação.

A segurança efetiva é um esforço de equipa que envolve a participação e o suporte de todos os funcionários e afiliados da **Tecnologias Imaginadas** que lidam com informações e/ou sistemas de informação. É responsabilidade de cada funcionário conhecer essas diretrizes e conduzir suas atividades de acordo com as mesmas.

PROPÓSITO

O objetivo desta política é delinear o uso aceitável de equipamentos de informática da **Tecnologias Imaginadas**. Essas regras estão em vigor para proteger o funcionário e a da **Tecnologias Imaginadas**. O uso inadequado expõe a da **Tecnologias Imaginadas** a riscos, incluindo, mas não limitado a ataques de vírus, malware, ramsonware, o comprometimento de sistemas e serviços, e problemas legais.

ÂMBITO

Esta política aplica-se ao uso de informação, dispositivos eletrônicos e de computação e recursos de rede para conduzir negócios da **Tecnologias Imaginadas** ou interagir com redes internas e sistemas comerciais, sejam de propriedade ou alugados por **Tecnologias Imaginadas**, o funcionário ou um terceiro. Todos os funcionários, contratados, consultores, temporários e outros funcionários da **Tecnologias Imaginadas** e suas subsidiárias são responsáveis por utilizar de forma apropriada, com recurso a bom senso profissional e ético e de acordo com as políticas e padrões de **Tecnologias Imaginadas** bem como respeitando leis e regulamentos nacionais e/ou locais, as informações, dispositivos eletrônicos e recursos de rede necessários ao exercício da sua atividade.

Esta política aplica-se a funcionários, contratados, consultores, temporários e outros trabalhadores da **Tecnologias Imaginadas**, incluindo todo o pessoal afiliado a terceiros. Esta política aplica-se a todos os equipamentos que são de propriedade ou alugados por **Tecnologias Imaginadas**.

POLÍTICA

1. Uso Geral e Propriedade

- 1.1 Informações proprietárias da **Tecnologias Imaginadas**, armazenadas em dispositivos eletrônicos e de computação, sejam de propriedade ou alugadas por **Tecnologias Imaginadas**, o funcionário ou um terceiro, permanecem como propriedade exclusiva da desta. O utilizador deve garantir, por meios legais e/ou técnicos, que as informações proprietárias sejam protegidas de acordo com o *Padrão de proteção de dados* assegurado pelas políticas da Empresa.
- 1.2 O Utilizador tem a responsabilidade de denunciar imediatamente o roubo, a perda ou a divulgação não autorizada de informações proprietárias da **Tecnologias Imaginadas**.
- 1.3 O Utilizador pode aceder, usar ou compartilhar informações proprietárias da **Tecnologias Imaginadas** somente na medida em que for autorizado e necessário para cumprir as obrigações de trabalho que lhe forem designadas.
- 1.4 Os funcionários são responsáveis por exercer bom senso quanto à razoabilidade do uso para fins pessoais. Departamentos individuais são responsáveis por criar diretrizes sobre o uso pessoal de sistemas de Internet / Intranet / Extranet. Na ausência de tais políticas, os funcionários devem ser guiados por políticas

departamentais sobre uso pessoal e, se houver alguma incerteza, os funcionários devem consultar seu supervisor ou gerente.

- 1.5 Para fins de segurança e manutenção de rede, os indivíduos autorizados dentro da **Tecnologias Imaginadas** podem monitorar o equipamento, os sistemas e o tráfego da rede a qualquer momento.
- 1.6 **Tecnologias imaginadas** reserva-se o direito de auditar periodicamente redes e sistemas para garantir a conformidade com os necessários níveis de performance.

2. Segurança e Informação Proprietária

- 2.1 Todos os dispositivos móveis e de computação conectados à rede interna devem obedecer a uma lógica de minimização da informação, acedendo estritamente à informação necessária para o desempenho da sua função.
- 2.2 As senhas ao nível do sistema e ao nível do usuário devem estar em conformidade com a *Política de Passwords*. É proibido fornecer acesso a outro indivíduo, seja deliberadamente ou por meio de falha para garantir seu acesso.
- 2.3 Todos os dispositivos de computação devem ser protegidos com um protetor de tela protegido por senha com o recurso de ativação automática definido para 10 minutos ou menos. Você deve bloquear a tela ou fazer logoff quando o dispositivo estiver sem supervisão.
- 2.4 As postagens de funcionários de um endereço de e-mail de **Tecnologias Imaginadas** para grupos de notícias devem conter um aviso afirmando que as opiniões expressas são estritamente próprias e não necessariamente as de **Tecnologias Imaginadas**, a menos que o envio esteja no curso das obrigações laborais.
- 2.5 Os funcionários devem ter muito cuidado ao abrir anexos de email recebidos de remetentes desconhecidos, que podem conter malware.

3. Uso inaceitável

As atividades a seguir são, em geral, proibidas. Os funcionários podem ficar isentos dessas restrições durante o curso de suas responsabilidades legítimas (por exemplo, a equipa de administração de sistemas pode ter a necessidade de desativar o acesso à rede de um host se esse host estiver interrompendo algum dos serviços necessários à operação da empresa).

Sob nenhuma circunstância um funcionário da **Tecnologias Imaginadas** está autorizado a envolver-se em atividades ilegais segundo as leis locais, nacionais ou internacionais, ao utilizar recursos de <Nome da Empresa>.

As listas abaixo não são exaustivas, mas tentam fornecer uma estrutura para atividades que se enquadram na categoria de uso inaceitável.

4. Atividades de sistema e rede

As seguintes atividades são estritamente proibidas, sem exceções:

- 4.1 Violações dos direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredos comerciais, patentes ou outras propriedades intelectuais ou leis ou regulamentos similares, incluindo, mas não se limitando à instalação ou distribuição de produtos "pirateados" ou outros produtos de software que não sejam devidamente licenciados para uso da **Tecnologias Imaginadas**.
- 4.2 Cópia não autorizada de material protegido por direitos autorais incluindo, mas não limitado a digitalização e distribuição de fotografias de revistas, livros ou outras fontes com direitos autorais, música com direitos autorais e a instalação de qualquer software protegido por direitos autorais para o qual **Tecnologias Imaginadas** ou o usuário final não tenha uma licença ativa é estritamente proibida.
- 4.3 É proibido aceder a dados, servidores ou serviços para qualquer finalidade que não seja a de prosseguir com a atividade comercial da **Tecnologias Imaginadas**, mesmo se você tiver acesso autorizado a estas fontes.
- 4.4 A exportação de software, informações técnicas, software de criptografia ou tecnologia, em violação das leis de controle de exportação internacionais, nacionais ou locais, é ilegal. A gerência apropriada deve ser consultada antes da exportação de qualquer material que esteja em questão.
- 4.5 Introdução de programas maliciosos – Malware - na rede ou servidor (por exemplo, vírus, worms, cavalos de Tróia, bombas de e-mail, etc.).
- 4.6 Revelar uma password para outras pessoas ou permitir o uso de um acesso pessoal por outras pessoas. Isso inclui familiares e outros membros da família quando o trabalho está sendo feito em casa.
- 4.7 Fazer ofertas fraudulentas de produtos, itens ou serviços originados de qualquer conta da <Nome da Empresa>.
- 4.8 Efetuar violações de segurança ou interrupções da comunicação de rede. Violações de segurança incluem, mas não se limitam a aceder a dados dos quais o funcionário não é um destinatário pretendido ou entrar num servidor ou conta a que o funcionário não está expressamente autorizado a aceder, a menos que esses deveres estejam dentro do escopo dos deveres regulares. Para fins desta seção, "interrupção" inclui, mas não se limita a, *sniffing* de rede, falsificação de pacotes, negação de serviço e informações falsas de roteamento para fins maliciosos.

- 4.9 Executar qualquer forma de monitoramento de rede que intercete dados não destinados ao host do funcionário, a menos que essa atividade faça parte do trabalho / dever normal do funcionário.
- 4.10 Contornar a autenticação do usuário ou a segurança de qualquer host, rede ou conta.
- 4.11 Usar qualquer programa / script / comando, ou enviar mensagens de qualquer tipo, com a intenção de interferir ou desabilitar a sessão de terminal de um utilizador, por qualquer meio, localmente ou através da Internet / Intranet / Extranet.
- 4.12 Fornecer informações ou listas de funcionários, Clientes, fornecedores ou de qualquer outra entidade que se relacione com **Tecnologias Imaginadas** a terceiros.

5. E-mail e atividades de comunicação

Ao usar recursos da empresa para aceder e usar a Internet, os usuários devem perceber que representam a empresa. Sempre que os funcionários declaram uma afiliação à empresa, eles também devem indicar claramente que "as opiniões expressas são minhas e não necessariamente as da empresa". Perguntas podem ser dirigidas ao Departamento de TI.

As seguintes atividades são estritamente proibidas, sem exceções:

- 5.1 Envio de mensagens de e-mail não solicitadas, incluindo o envio de "lixo eletrônico" ou outro material publicitário para pessoas que não solicitaram especificamente esse tipo de material (spam de e-mail).
- 5.2 Qualquer forma de assédio via email, telefone ou pager, seja por meio de idioma, frequência ou tamanho de mensagens.
- 5.3 Uso não autorizado ou falsificação de informações de cabeçalho de email.
- 5.4 Solicitação de e-mail para qualquer outro endereço de e-mail, com exceção da conta do anunciante, com a intenção de assediar ou recolher respostas.
- 5.5 Criar ou encaminhar "correntes", "Ponzi" ou outros esquemas "pirâmide" de qualquer tipo.
- 5.6 Uso de e-mails não solicitados provenientes de redes da **Tecnologias Imaginadas** de outros provedores de serviços de Internet/Intranet/Extranet em nome de, ou para anunciar, qualquer serviço hospedado por **Tecnologias Imaginadas** ou conectado através da rede **Tecnologias Imaginadas**.

6. Blogging e Redes Sociais

- 6.1** O blog de funcionários, seja usando propriedade e sistemas da **Tecnologias Imaginadas** ou sistemas de computadores pessoais, também está sujeito aos termos e restrições estabelecidos nesta Política. O uso limitado e ocasional dos sistemas da **Tecnologias Imaginadas** para se envolver em blogs é aceitável, desde que seja feito de maneira profissional e responsável, sem violar a política da **Tecnologias Imaginadas**, nem prejudicando os melhores interesses, nem interferindo com as obrigações normais de trabalho do funcionário. Blogar a partir dos sistemas da **Tecnologias Imaginadas** também está sujeito a monitoramento.
- 6.2** A Política de Confidencialidade de **Tecnologias Imaginadas** também se aplica a blogs. Como tal, os Funcionários são proibidos de revelar qualquer informação confidencial ou proprietária da <Empresa>, segredos comerciais ou qualquer outro material coberto pela política de Informações Confidenciais da <Empresa> quando envolvidos em blogs.
- 6.3** Os funcionários não se devem envolver em nenhum blog que possa prejudicar ou manchar a imagem, reputação e/ou boa vontade da **Tecnologias Imaginadas** e/ou de qualquer um dos seus funcionários. Os funcionários também estão proibidos de fazer comentários discriminatórios, depreciativos, difamatórios ou de assédio quando blogam.
- 6.4** Os funcionários também não podem atribuir declarações pessoais, opiniões ou crenças a **Tecnologias Imaginadas** quando estiverem envolvidos em blogs. Se um funcionário está expressando suas crenças e / ou opiniões em blogs, o funcionário não pode, de forma expressa ou implícita, fazer-se representar como funcionário ou representante da **Tecnologias Imaginadas**. Os funcionários assumem todo e qualquer risco associado aos blogs.
- 6.5** Além de seguir todas as leis relacionadas ao manuseio e divulgação de materiais controlados por direitos autorais ou de exportação, as marcas comerciais, logotipos e qualquer outra propriedade intelectual da **Tecnologias Imaginadas** também não podem ser usadas em conexão com qualquer atividade de blogging, a não ser que tal seja realizado dentro da função comercial da empresa.

7. Conformidade política

7.1 Medição de Conformidade

7.1.1 A equipe da **Tecnologias Imaginadas** verificará a conformidade com esta política por meio de vários métodos, incluindo, entre outros, relatórios de ferramentas de negócios, auditorias internas e externas e feedback para o proprietário da política.

7.2 Exceções

7.2.1 Qualquer exceção à política deve ser aprovada pela equipe da **Tecnologias Imaginadas** antecipadamente.

7.3 Não Conformidade

7.3.1 Um funcionário que tenha violado esta política pode estar sujeito a ações disciplinares, incluindo até a rescisão do contrato de trabalho.

8. Histórico de Revisão

Data de mudança	Responsável	Resumo da mudança
Julho de 2018	Olívio Pereira	Criação – Versão 1
Novembro de 2021	Vinicius Silva	Alteração para CareTracker Versão 1.1

POLÍTICA DE INFORMAÇÃO PUBLICITÁRIA E PROCESSAMENTO DE DADOS COM FINALIDADES COMERCIAIS E DE FIDELIZAÇÃO

Se o UTILIZADOR / CLIENTE assim o manifestar mediante configuração da sua conta ou se consentir receber a nossa newsletter, os seus dados serão utilizados para o informar de forma personalizada, através de qualquer meio, inclusivamente eletrónicos ou telefónicos, sobre produtos ou serviços comercializados e relativos à atividade da empresa. Os seus dados serão igualmente recolhidos para a melhoria da qualidade dos serviços, de segmentação comercial e de fidelização dos clientes.

Se não desejar receber comunicações comerciais, pode enviar um e-mail a retirar o seu consentimento para o suporte@tecnologiasimaginadas.com.

POLÍTICA DE COOKIES

Devido ao modo como funcionam os standards de comunicação, o acesso aos websites da **Tecnologias Imaginadas** pode implicar a utilização de cookies. Os cookies são pequenos ficheiros que são gravados no computador do utilizador e que servem apenas para identificar o computador que está a aceder ao web site. Esses ficheiros não mantêm nenhuma informação pessoal. Os cookies têm, geralmente, uma duração limitada no tempo. Nenhum cookie extrai informação do disco rígido do computador do utilizador, acede ou retira informação pessoal ou lê os ficheiros cookies criados por outros fornecedores. Através da utilização de cookies é possível reconhecer os utilizadores devidamente registados, desde que utilizem o mesmo equipamento e navegador, sem que se tenham de registar em cada visita para aceder às áreas e serviços reservados exclusivos. O utilizador é livre para rejeitar cookies se o navegador o permitir, mas ao fazê-lo está a comprometer a plena funcionalidade dos websites da **Tecnologias Imaginadas**.

POLÍTICA DE SEGURANÇA DE DADOS: REQUISITOS DE FUNCIONÁRIOS

USANDO ESTA POLÍTICA

Esta política descreve os comportamentos esperados dos funcionários ao lidar com dados pessoais e fornece uma classificação dos tipos de dados com os quais eles devem se preocupar. Está ligada à *Política de Uso Aceitável* (PUA), e fornece aos usuários orientações sobre os comportamentos necessários.

PROPÓSITO

A **Tecnologias Imaginadas** deve proteger contra perdas dados restritos, confidenciais ou sensíveis para evitar danos à sua reputação e evitar impactos adversos nos seus clientes, fornecedores e outras entidades com as quais haja relação. A proteção de dados no âmbito da sua atuação é um requisito essencial para os negócios, mas a flexibilidade para aceder aos dados e trabalhar com eficiência é também uma necessidade.

Não é esperado que o controlo através das soluções tecnológicas implementadas possa lidar com o cenário de roubo malicioso de maneira infalível. O objetivo principal desta política é a conscientização do utilizador e evitar cenários de perda acidental, mas também de o alertar para procedimentos de risco que podem facilitar direta ou indiretamente o roubo malicioso.

ÂMBITO

1 - Qualquer funcionário, contratado ou indivíduo com acesso a sistemas ou dados da **Tecnologias Imaginadas**.

2 - Definição de dados a serem protegidos (devem ser identificados os tipos de dados e dar exemplos para que os colaboradores possam identificá-los quando encontrarem)

- Pessoais
- Financeiros
- Restrito / Sensível
- Confidencial
- Outros

POLÍTICA DE RESPOSTA A VIOLAÇÕES DE DADOS

PROPÓSITO

O objetivo da política é estabelecer as metas e a visão do processo de resposta a violações. Essa política definirá claramente a quem ela se aplica e sob quais circunstâncias, e incluirá a definição de uma violação, funções e responsabilidades da equipe, padrões e métricas (por exemplo, para permitir a priorização dos incidentes), bem como relatórios, correção, e mecanismos de feedback. A política deve ser bem divulgada e disponibilizada facilmente a todo o pessoal cujas funções envolvam privacidade de dados e proteção de segurança.

As intenções da **Tecnologias Imaginadas** de publicar uma Política de Resposta à Violação de Dados concentram a sua atenção em como a cultura de abertura, confiança e integridade de **Tecnologias Imaginadas** deve responder em caso de Violação de Dados. A **Tecnologias Imaginadas** está empenhada em proteger os funcionários, parceiros e a empresa contra ações ilegais ou prejudiciais de indivíduos, conscientes ou não.

ÂMBITO

Esta política exige que qualquer indivíduo que suspeite que ocorreu um roubo, violação ou exposição dos dados protegidos, deve fornecer imediatamente uma descrição do que ocorreu via e-mail para o suporte@tecnologiasimaginadas.com, ligando para **212 592 207** ou através do uso da página web de relatórios do help desk em <https://tecnologiasimaginadas.com/contactos/>. Esse endereço de e-mail, número de telefone e página Web são monitorados pelo administrador de segurança da informação da **Tecnologias Imaginadas**. Essa equipe investigará todos os roubos, violações de dados e exposições relatados para confirmar se ocorreu um roubo, violação ou exposição. Se um roubo, violação ou exposição ocorreu, o Administrador de Segurança da Informação seguirá o procedimento apropriado em vigor.

Esta política aplica-se a todos que coletam, acedem, mantêm, distribuem, processam, protegem, armazenam, usam, transmitem, descartam ou de outra forma manipulam informações de identificação pessoal ou PHI (Protected Health Information) de membros da **Tecnologias Imaginadas**.

Política Roubo, violação de dados ou exposição do cliente e Dados protegidos.

Assim que um roubo, violação de dados ou exposição de suporte contendo dados protegidos ou confidenciais for identificado, o processo de remoção de todos os acessos a esse recurso será iniciado.

O Diretor Executivo presidirá uma equipe de resposta a incidentes para lidar com a violação ou exposição.

A equipe incluirá membros de:

- Infraestrutura de TI
- Aplicativos de TI
- Finanças (se aplicável)
- Legal
- Comunicações
- A unidade ou departamento afetado que usa o sistema envolvida ou cujos dados podem ter sido violados ou expostos
- Departamentos adicionais com base no tipo de dados envolvido, indivíduos adicionais, conforme considerado necessário pelo Diretor Executivo

Confirmado roubo, violação ou exposição dos dados do **Tecnologias Imaginadas**

O Diretor Executivo será notificado sobre o roubo, violação ou exposição. A equipe de TI, juntamente com a equipe forense designada, analisará a violação ou exposição para determinar a causa raiz.

FUNÇÕES E RESPONSABILIDADES

- O Administrador de Segurança da Informação é o membro da **Tecnologias Imaginadas**, designado pelo Diretor Executivo ou Diretor, que fornece suporte administrativo para a implementação, supervisão e coordenação de procedimentos e sistemas de segurança preventivos e/ou responsivos.
- Os utilizadores incluem todos os colaboradores da **Tecnologias Imaginadas** na medida em que possuem acesso a dados pessoais, protegidos ou confidenciais. Podem incluir funcionários, curadores, contratados, consultores, estagiários, funcionários temporários e voluntários.

- A **Equipa de Resposta a Incidentes** será presidida pela Diretoria Executiva e deverá incluir, mas não se limitará aos seguintes departamentos ou seus representantes: Infraestrutura de TI, Segurança de Aplicativos de TI; Comunicações; Legal; Gestão; Serviços Financeiros, Serviços para Membros; Recursos humanos.

ENFORCEMENT

Qualquer colaborador da **Tecnologias Imaginadas** encontrado em violação desta política pode estar sujeito a ação disciplinar, até e incluindo a rescisão do contrato de trabalho. Qualquer empresa parceira encontrada em violação será sujeita às penalizações previstas por lei, e o contrato entre as partes poderá ser rescindido por justa causa.

HISTÓRICO DE REVISÕES

Versão	Data de revisão	Autor	Descrição das Alterações
1.0	Julho de 2018	Olívio Pereira	Versão inicial
1.1	Novembro de 2021	Vinícius Silva	Alterações para base CareTracker

POLÍTICA DE PASSWORDS

VISÃO GERAL

As senhas são um aspeto importante da segurança do computador. Uma senha mal escolhida pode resultar num acesso não autorizado e / ou exploração de nossos recursos. Todos os funcionários, incluindo contratados e fornecedores com acesso aos sistemas **Tecnologias Imaginadas**, são responsáveis por executar as etapas apropriadas, conforme descrito abaixo, para selecionar e proteger suas senhas.

OBJETIVO

O objetivo desta política é estabelecer um padrão para a criação de senhas atuais e a proteção dessas senhas.

ÂMBITO

O âmbito desta política inclui todo o pessoal que tem ou é responsável por uma conta (ou qualquer forma de acesso que suporte ou exija uma senha) em qualquer sistema que resida em qualquer instalação da **Tecnologias Imaginadas**, tenha acesso à rede ou armazena qualquer informação não pública da empresa.

POLÍTICA

1. Criação de Senha

a. Todas as senhas de nível de usuário e nível de sistema devem estar em conformidade com as ***Diretrizes de construção de senha:***

i. Senhas fortes são longas, quanto mais caracteres tiver, mais forte será a senha. Recomendamos um mínimo de 14 caracteres na sua senha. Além disso, incentivamos o uso de senhas-frase, senhas compostas de várias palavras. Os exemplos incluem "É hora de férias" ou "bloquear-folhas-curiosas". As senhas-frase são fáceis de lembrar e digitar, mas respeitam os requisitos de segurança. Senhas pobres ou fracas têm as seguintes características:

1. Contêm oito caracteres ou menos.
2. Contêm informações pessoais, como datas de nascimento, endereços, números de telefone ou nomes de membros da família, animais de estimação, amigos e personagens fantasiosos.
3. Contêm padrões numéricos, como aaabbb, qwerty, zyxwvuts ou 123321.
4. São versões do "Welcome123" "Password123" "Changeme123"

ii. Além disso, todas as contas devem ter uma senha diferente e exclusiva. Para permitir que os usuários mantenham várias senhas, recomendamos o uso do software "gerenciador de senhas" que é autorizado e fornecido pela organização. Sempre que possível, também ative o uso de autenticação multifator.

- b. Os usuários devem usar uma senha única e separada para cada uma de suas contas relacionadas ao trabalho. Os usuários não podem usar senhas relacionadas ao trabalho para suas próprias contas pessoais.
2. Mudança de senha
- a. As senhas devem ser alteradas apenas quando houver motivos para acreditar que uma senha foi comprometida.
 - b. Quebra de senha ou adivinhação podem ser realizadas periodicamente ou aleatoriamente pela Equipa da **Tecnologias Imaginadas** ou por seus representantes. Se uma senha for adivinhada ou quebrada durante uma dessas verificações, o utilizador deverá alterá-la para estar em conformidade com as Diretrizes de construção de senha.
3. Proteção de senha
- a. As senhas não devem ser compartilhadas com ninguém, incluindo supervisores e colegas de trabalho. Todas as senhas devem ser tratadas como confidenciais.
 - b. As senhas não devem ser inseridas em mensagens de e-mail, nem reveladas por telefone a ninguém.
 - c. As senhas podem ser armazenadas apenas em "gestores de senhas" autorizados pela organização.
 - d. Não use o recurso "Lembrar senha" dos aplicativos (por exemplo, navegadores da Web).
 - e. Qualquer usuário que suspeite que sua senha pode ter sido comprometida deve relatar o incidente e alterar todas as senhas.
4. Desenvolvimento de aplicações
- a. Os programadores devem garantir que seus programas contenham as seguintes precauções de segurança:
 - i. As Aplicações devem suportar autenticação de usuários individuais, não grupos.
 - ii. As Aplicações não devem armazenar senhas em texto simples ou de qualquer forma facilmente reversível.
 - iii. As Aplicações não devem transmitir senhas em texto não criptografado pela rede.
 - iv. As Aplicações devem fornecer algum tipo de gestor de perfis, de modo que um usuário possa assumir as funções de outro sem precisar de saber a senha deste.

CONFORMIDADE POLÍTICA

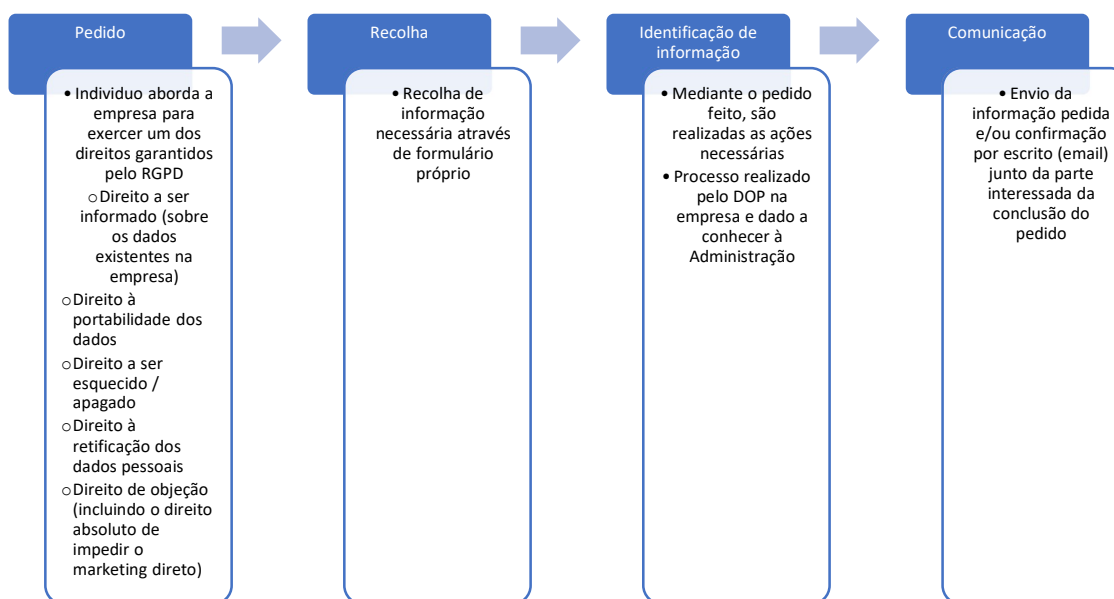
1. Medição de Conformidade
 - a. A equipe da **Tecnologias Imaginadas** verificará a conformidade desta política por meio de vários métodos, incluindo, entre outros, acompanhamento periódico, monitoramento de vídeo, relatórios de ferramentas de negócios, auditorias internas e externas e feedback ao proprietário da política.
2. Exceções
 - a. Qualquer exceção à política deve ser aprovada pela equipe da **Tecnologias Imaginadas** antecipadamente.
3. Não Conformidade
 - a. Um funcionário que tenha violado esta política pode estar sujeito a ações disciplinares, incluindo até a rescisão do contrato de trabalho.

HISTÓRICO DE REVISÃO

Versão	Data de revisão	Autor	Descrição das Alterações
1.0	Agosto de 2018	Olívio Pereira	Versão inicial
1.1	Novembro de 2021	Vinicius Silva	Alteração para base CareTracker

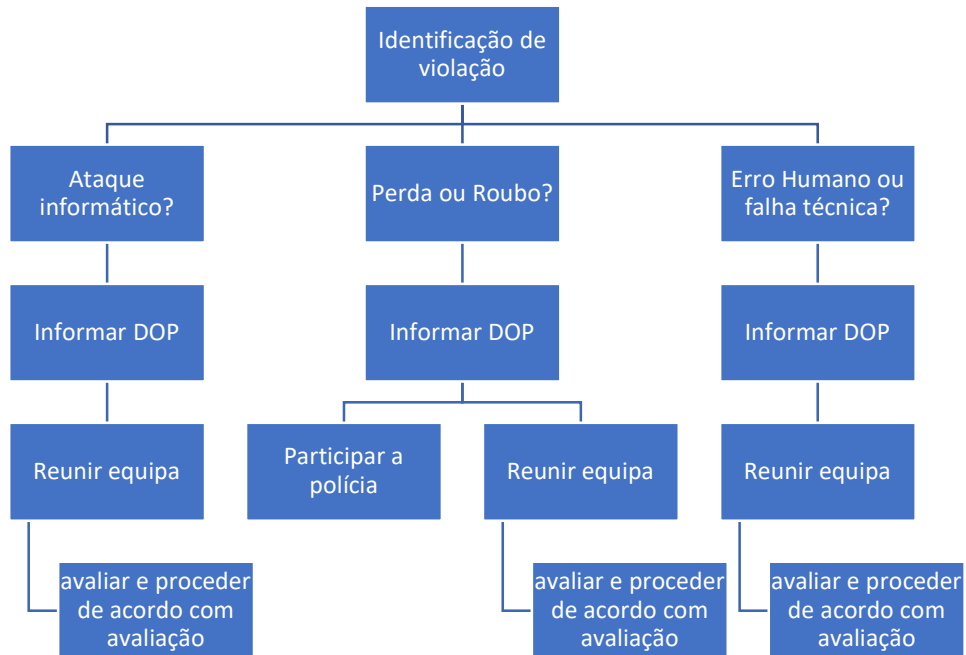
COMUNICAÇÕES E RELATÓRIOS

WORKFLOWS DE RESPOSTA AOS TITULARES DOS DIREITOS



PLANO DE CONTINGÊNCIA

WORKFLOW



BREACH NOTIFICATION (NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS)

Em caso de Violação de dados esta deve ser comunicada no âmbito do RGPD a diferentes entidades:

- a) Funcionários internos;
- b) CNPD através do site da Comissão Nacional de Proteção de dados é possível realizar a comunicação: <https://www.cnpd.pt/DataBreach/?AspxAutoDetectCookieSupport=1>
- c) Entidades diretamente afetadas, nomeadamente o(s) titolare(s)
- d) O público em geral

Com base no formulário da CNPD, na análise da violação e para possibilitar a devida comunicação deve ser recolhida a seguinte informação:

DADOS DA ENTIDADE

Nome da entidade

Empresa sediada em Portugal? (S/N)

Número de contribuinte (NIF)

Morada

Código postal -

Localidade

Setor de atividade

DADOS DE CONTACTO

Pessoa de contacto

Função

Telefone de contacto

Email de contacto

INFORMAÇÃO SOBRE A VIOLAÇÃO DE DADOS

Descrição da violação (*Descreva a violação de dados (o quê? quem? como?)*)

Data e hora fim | Data e hora inicio | Data e Hora Conhecimento

Forma como a violação foi identificada

Tipo de violação

Integridade | Confidencialidade | Disponibilidade

Natureza da violação

Equipamento perdido ou roubado | Documentos perdidos ou roubados
| Correio perdido ou acedido indevidamente | Hacking | Malware |
 Phishing | Outra

Causa da violação

Ato interno não malicioso | Ato interno malicioso | Ato externo não
malicioso | Ato externo malicioso | Outra

CONSEQUÊNCIAS DA VIOLAÇÃO DE DADOS

Confidencialidade

A utilização dos dados pode ter consequências para o titular dos dados?
(s/n)

Se sim, indique quais e qual o grau de impacto (baixo, médio, elevado):

DADOS PESSOAIS ENVOLVIDOS

Indique o(s) tipo(s) de dados pessoais envolvido(s)

Foi possível determinar o número de titulares afetados? Se sim quantifique.

TITULARES DOS DADOS

Tipo de titulares envolvidos (Trabalhadores, Utilizadores, Subscritores, Alunos,
Militares, Clientes, Pacientes, Menores, Indivíduos vulneráveis, Outros)

INFORMAÇÃO AOS TITULARES

Os titulares foram informados da violação?

Se sim indique:

a data
a forma/meio de comunicação
numero de titulares
mensagem enviada

MEDIDAS PREVENTIVAS/CORRETIVAS

Que mecanismos de segurança existiam ANTES da violação?

Que medidas foram aplicadas para corrigir/mitigar a violação?

TRATAMENTOS TRANSFRONTEIRIÇOS

Existe tratamento de dados transfronteiriço?

A violação vai ser notificada diretamente a outra autoridade de controlo da UE?

A violação vai ser notificada diretamente a outra autoridade de controlo da fora da UE?

A violação será notificada a outros reguladores europeus, por razões legais?

CONTRATOS, DECLARAÇÕES E FORMULÁRIOS

CONTRATOS DE SUBCONTRATAÇÃO

- Ver docs:
 - Minuta TI - Cláusula contratual a acrescentar em contratos de subcontratação.docx
 - Minuta TI – declaração terceiros.docx

CONTRATOS DE PARCERIA

- Ver docs :
 - Minuta TI - Protocolo de parceria_MINUTA.docx
 - Minuta TI - Non Disclosure Agreement.docx

DECLARAÇÃO DE CONSENTIMENTO

SITES

Declaro que para todos os efeitos, autorizo a **Tecnologias Imaginadas** e processar os dados por mim introduzidos, no âmbito do serviço **CareTracker**

Declaro também que tomei conhecimento dos **Termos e condições gerais**, dos meus **direitos como titular**, das **Políticas de privacidade e confidencialidade da informação** da Tecnologias Imaginadas, bem como da **Política de informação publicitária e processamento de dados com finalidades comerciais e de fidelização**, e da **Política de cookies**.

IOT

Declaro que para todos os efeitos, autorizo a **Tecnologias Imaginadas** e processar os dados por mim introduzidos, no âmbito do serviço **CareTracker**

Dada a natureza do serviço, autorizo também que a minha localização, associada ao dispositivo seja aferida no âmbito do serviço prestado, e que esta informação, bem como os restantes dados pessoais sejam acessíveis aos intervenientes nos serviços solicitados para sua concretização.

Declaro também que tomei conhecimento dos **Termos e condições gerais**, dos meus **direitos como titular**, das **Políticas de privacidade e confidencialidade da informação** da Tecnologias Imaginadas, bem como da **Política de informação publicitária e processamento de dados com finalidades comerciais e de fidelização**, e da **Política de cookies**.

FORMULÁRIO PARA SOLICITAÇÃO DE EXERCÍCIO DE DIREITO

- Ver docs:
 - Minuta TI - solicitação de exercício de direito – tratamento de dados pessoais.docx

FINALIDADES DE TRATAMENTO

Os Dados Pessoais são obtidos com a finalidade de:

- a) Própria atividade vinculada a uma empresa de Sistemas de informação e comunicação/tecnologia;
- b) Fornecimento aos intervenientes nos serviços solicitados pelo utilizador para concretização dos serviços contratados pelo Utilizador / Cliente;

- c) Gestão, administração, prestação, ampliação e melhoria dos serviços em que o utilizador / cliente decida subscrever-se e registar-se ou utilizar a adequação desses serviços às preferências e gostos dos utilizadores;
- d) Verificar cartões de crédito e outros tipos de cartões utilizados no pagamento e indicados pelo próprio Utilizador / Cliente;
- e) O estudo da utilização dos serviços por parte dos utilizadores;
- f) Verificar, manter e desenvolver sistemas e análises estatísticas, para uso da empresa com a finalidade de melhorar os serviços/produtos disponibilizados ao mercado.
- g) Atividades de publicidade, promoção e prospeção se devidamente aceite pelo Utilizador;
- h) Enviar formulários de inquéritos aos quais o utilizador não fica obrigado a responder;
- i) Enviar mensagens SMS com fins de venda direta, publicitários ou relacionados com o serviço contratado.

O utilizador poderá consentir, através de formulário próprio ou de documento suficientemente explícito, que a Tecnologias Imaginadas, trate os seus Dados Pessoais com a finalidade de determinar o seu perfil e oferecer-lhe produtos e serviços adequados. Estes serviços podem ser próprios ou de terceiros.

LOCAL ONDE SÃO GUARDADOS

- Sistemas Informáticos
 - ERP : PHC
 - CRM : CASgw
 - Sistema de Tickets: OTRS
 - Sites das empresas do Grupo
 - www.tecnologiasimaginadas.com
 - www.protocoltek.com
 - www.tasi.pt
 - www.tekcarta.pt
 - www.tekfrota.com
 - <http://www.mybluebee.pt/>
 - <https://locateit.tecnologiasimaginadas.com>
 -
- Arquivo Físico
 - Capas de contabilidade
 - Cartões de visita

PERÍODO EM QUE SERÃO UTILIZADOS

Caso não haja um pedido expresso por parte do proprietário dos dados, estes serão guardados sem limitação temporal. O motivo para tal está relacionado com a atividade da empresa e com o tipo de serviços prestados, muitas vezes cíclicos, mas sem um espaço temporal definido.

PESSOA/ENTIDADE QUE OS FORNECEU

Os dados pessoais a que a **Tecnologias Imaginadas** tem acesso, devem ser fornecidos pelo detentor dos mesmos ou por outra pessoa ou entidade devidamente autorizada a fazê-lo, por consentimento expresso, obrigatoriedade laboral, contratual ou legal.

PESSOAS QUE TÊM ACESSO AOS DADOS

O acesso aos dados está reservado aos elementos da equipa da **Tecnologias Imaginadas** que, pelas suas responsabilidades e obrigações profissionais, necessitam de aceder a esta informação. De notar que todos os elementos da equipa estão obrigados a obedecer às políticas internas de acesso e processamento de dados pessoais, bem como a toda a legislação em vigor.

ALTERAÇÕES À POLÍTICA DE PRIVACIDADE

A **Tecnologias Imaginadas** reserva-se o direito de alterar as presentes Políticas a todo o tempo. Em caso de modificação, a data da última alteração, disponível no topo desta página, é também atualizada.

LEI E FORO APLICÁVEIS

A Política de Privacidade, bem como a recolha, tratamento ou transmissão de Dados do Titular, são regidos pelo disposto no Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 e pela legislação e regulamentação aplicáveis em Portugal.

Quaisquer litígios decorrentes da validade, interpretação ou execução da Política de Privacidade, ou que estejam relacionados com a recolha, tratamento ou transmissão de Dados do Titular,

devem ser submetidos em exclusivo à jurisdição dos tribunais judiciais da comarca de Lisboa, sem prejuízo das normas legais imperativas aplicáveis.