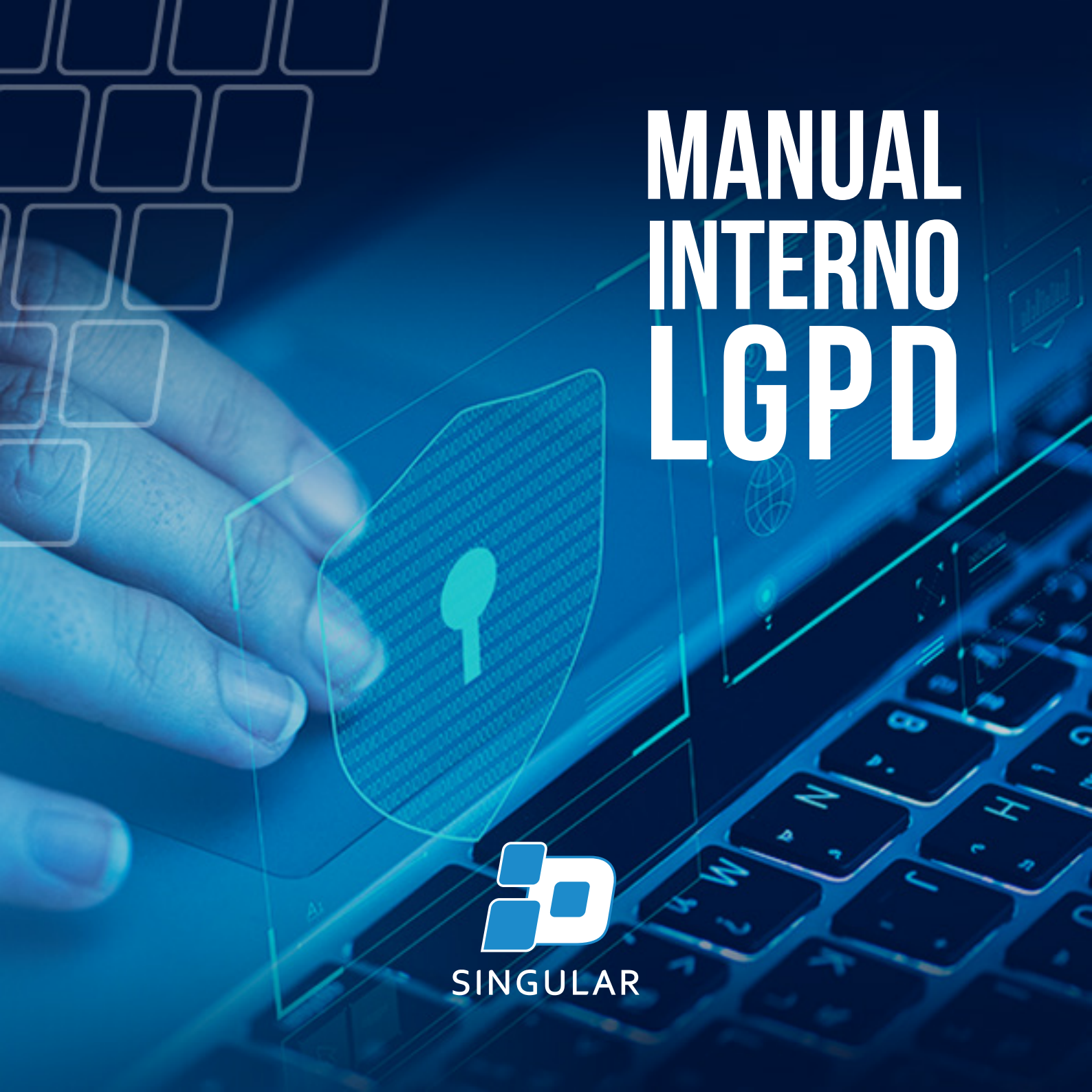
MANUAL INTERNO LGPD



SINGULAR

SEU MUNDO DO TAMANHO DO SEU CONHECIMENTO

SINGULAR

PRODUÇÃO EDITORIAL
ID Singular - LGPD
Versão 2025

SOMOS A ID SINGULAR

+50K PESSOAS IMPACTADAS

+250 EMPRESAS ATENDIDAS

MISSÃO

Promover a Singularidade integrando Humanização e Performance.

VISÃO

Ser a referência mundial em gestão humanizada e educação singular, transformando organizações em ecossistemas prósperos que valorizam e potencializam as pessoas.

VALORES

SINGULARIDADE - Reconhecer, respeitar e valorizar a diversidade.

PROSPERIDADE - Gerar e desfrutar de riqueza e abundância.

EXCELÊNCIA - Agregar valor impulsionando o potencial humano.

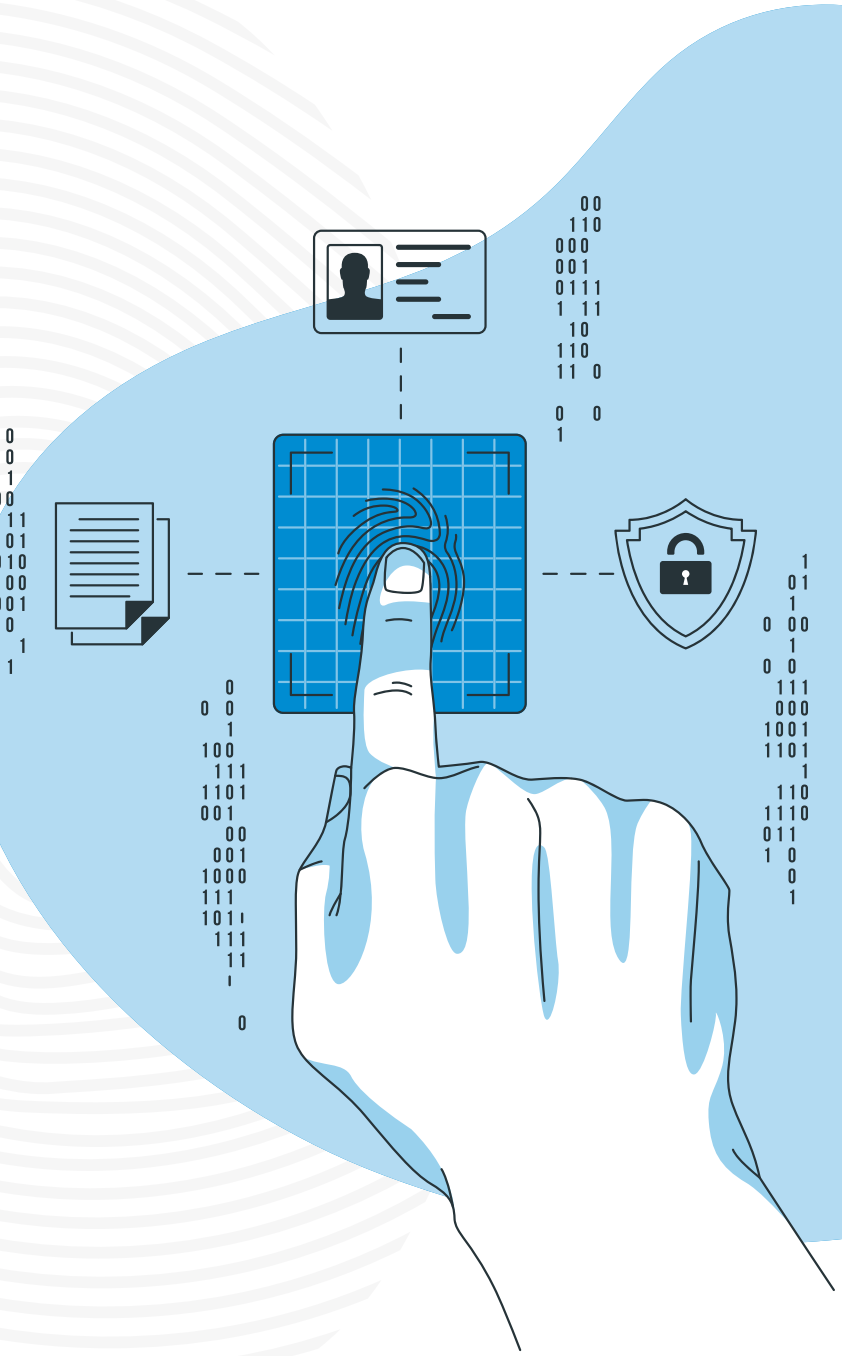
INTEGRALIDADE - Agir de forma integrada, harmônica e sistêmica.

SOLUÇÕES PERSONALIZADAS

- ***ACADEMIA DE LIDERANÇA***
- ***CONSULTORIA EM GESTÃO DE PESSOAS***
- ***ASSESSMENT***

Saiba Mais

SUMÁRIO



MANUAL INTERNO LGPD

SINGULAR

INTRODUÇÃO

Respeitar a sua privacidade é a nossa prioridade.

Na ID Singular, zelar pela privacidade e segurança das informações de nossos clientes, alunos e demais titulares de dados pessoais é um compromisso que levamos a sério. Este documento foi elaborado com o objetivo de oferecer transparência sobre como seus dados são coletados, tratados, armazenados e protegidos pela nossa organização, sempre em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Além de garantir o cumprimento das normas legais, este manual também tem o intuito de trazer esclarecimentos para os nossos clientes sobre as normas de segurança interna adotadas pela ID Singular. Aqui, você encontrará informações detalhadas sobre as medidas técnicas e organizacionais que implementamos para proteger os dados pessoais contra acessos não autorizados, vazamentos, perdas ou qualquer outra forma de tratamento inadequado.

Para facilitar a sua compreensão, apresentamos, de forma clara e organizada, as diretrizes, políticas internas e práticas adotadas pela ID Singular para mitigar riscos, proteger os direitos dos titulares e garantir a segurança das informações. Este manual também serve como um guia para orientar decisões rápidas e seguras, consolidando as melhores práticas no tratamento de dados pessoais e fortalecendo a cultura de proteção de dados em nossa organização.

Se você tiver alguma dúvida sobre esta Política de Privacidade e Proteção de Dados Pessoais, entre em

contato com nossa **Data Protection Officer** (DPO/Encarregada), Sabrina Alcici, pelo e-mail **lgpd@idsingular.com.br**. Estamos à disposição para esclarecer qualquer questão e garantir que seus direitos sejam respeitados.

Abaixo, você encontrará um quadro resumo dos termos abordados neste manual, organizado de forma clara e acessível para facilitar a sua consulta. Essas informações foram cuidadosamente preparadas para ajudá-lo a compreender não apenas os seus direitos, mas também as práticas e os procedimentos adotados pela ID Singular para garantir a segurança, a privacidade e a integridade das informações que nos são confiadas.

Aqui estão alguns dos principais termos abordados:

CONHEÇA UM POUCO MAIS

Adolescente: Pessoa física entre 12 e 18 anos de idade, conforme o Estatuto da Criança e do Adolescente (ECA).

Agentes de tratamento: Controlador e/ou operador, responsáveis pelo tratamento de dados.

Autoridade Nacional de Proteção de Dados (ANPD): Órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Anonimização: Uso de meios técnicos para garantir que um dado perca a possibilidade de associação, direta ou indireta, a um indivíduo.

Bloqueio: Suspensão temporária de qualquer operação de tratamento, mantendo o dado pessoal sob guarda.

Cliente: Pessoa física que utiliza os serviços da ID Singular.

Criança: Pessoa física com até 12 anos de idade incompletos, conforme o Estatuto da Criança e do Adolescente (ECA).

Compartilhamento: Transferência ou interconexão de dados pessoais com áreas internas ou terceiros.

Confidencialidade: Garantia de que os dados pessoais não serão divulgados para pessoas não autorizadas.

Controlador: Pessoa física ou jurídica responsável por decidir sobre o tratamento de dados pessoais. Consentimento: Manifestação livre, informada e inequívoca do titular, confirmando sua concordância com o tratamento de seus dados pessoais.

Cookies: Pequenos arquivos de texto armazenados no computador do usuário, utilizados para melhorar a experiência de navegação e personalizar serviços.

Dado Pessoal: Informação que permite identificar uma pessoa, direta ou indiretamente (ex.: nome, CPF, e-mail).

Dado Pessoal Sensível: Categoria de dado que requer proteção extra, como informações sobre saúde, origem racial, convicção religiosa, entre outros.

Direitos do titular: Incluem confirmação do tratamento, acesso, correção, eliminação, portabilidade de dados, revogação do consentimento e outras garantias previstas na LGPD.

Encarregado/DPO: Pessoa indicada para atuar como canal de comunicação entre a ID Singular, os titulares de dados e a ANPD.

Eliminação: Exclusão definitiva de dados pessoais armazenados.

LGPD: Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que regula o tratamento de dados pessoais no Brasil.

Operador: Pessoa ou entidade que realiza o tratamento de dados em nome do controlador.

Pseudonimização: Processo que descaracteriza dados pessoais, tornando-os pseudônimos, mas ainda passíveis de associação com informações adicionais.

Retenção de dados: Período em que os dados pessoais permanecem armazenados, mesmo após o término de sua finalidade.

Terceiros: Parceiros, prestadores de serviços ou fornecedores que atuam em conjunto com a ID Singular.
Titular: Pessoa física a quem se referem os dados pessoais tratados.

Tratamento de Dados: Todas as operações realizadas com dados pessoais, como coleta, armazenamento, uso, compartilhamento e eliminação.

Usuário: Pessoa física que navega no site da ID Singular, considerada titular de dados pessoais.
Vazamento: Divulgação ilícita ou acesso não autorizado a dados pessoais.

1. POLÍTICA DE ANÁLISE DE RISCOS E IMPACTOS

1.1. IDENTIFICAÇÃO DE RISCOS

A ID Singular adota medidas específicas para a identificação e mitigação dos riscos relacionados ao tratamento de dados pessoais, conforme as práticas estabelecidas abaixo:

✓ **Monitoramento Contínuo de Acessos e Manipulação de Dados**

A ID Singular utiliza softwares especializados, indicados no decorrer do manual, para monitoramento em tempo real e auditorias periódicas. Garante-se que o acesso aos dados seja restrito aos colaboradores autorizados. Relatórios diários são gerados e analisados pela equipe de segurança para identificar vulnerabilidades e adotar ações corretivas.

✓ **Backups Periódicos e Sistemas de Recuperação**

- **Frequência e Armazenamento:** Os backups são realizados diariamente para todos os dados críticos da ID Singular. Os backups são armazenados em locais físicos e na nuvem, garantindo que, em caso de falhas de hardware ou incidentes, os dados possam ser recuperados sem perda significativa de informações.
- **Testes de Recuperação:** Os testes de recuperação de dados são realizados periodicamente, simulando cenários de perda ou corrupção de dados. Isso assegura que os sistemas de recuperação estejam sempre operacionais e que o processo de restauração seja eficiente e rápido.

✔ Processos Internos para Atender Solicitações dos Titulares

Um canal exclusivo no site é disponibilizado para contato direto com o DPO (Data Protection Officer). Garantindo que os titulares de dados possam esclarecer suas dúvidas e receber atendimento ágil, com prazos especificados e eficácia direcionada por treinamentos específicos para a equipe, em relação ao tratamento de seus dados pessoais.

✔ Manutenções e Atualizações nos Sistemas

- O monitoramento contínuo dos logs de erro e de acesso das aplicações é realizado pela ID Singular, com investigação imediata de alertas e anomalias.
- A ID Singular adota a uma política de **Continuidade de Negócios e Recuperação de Desastres** de correção emergencial para erros críticos, com notificação automática ao desenvolvedor responsável e um prazo máximo de 24 horas para mitigação, detalhada no item 3 deste manual.
- As **atualizações nos servidores** são realizadas semanalmente, seguindo as recomendações de segurança da AWS, incluindo a aplicação de patches críticos divulgados pela Amazon EC2.
- A ID Singular **gerencia proativamente** pacotes e dependências, realizando atualizações semanais dos scripts Composer e Node (npm), priorizando a substituição de pacotes desatualizados ou vulneráveis em até 72 horas.

2. POLÍTICA DE RESPOSTA A INCIDENTES DE DADOS

2.1. DETECÇÃO E REGISTRO

A ID Singular adota as seguintes medidas para detectar e registrar incidentes relacionados a dados pessoais, assegurando a segurança e integridade das informações:

- **Ferramentas de Monitoramento:** Utilizamos ferramentas avançadas de monitoramento de segurança cibernética, como SIEM (Security Information and Event Management), para monitorar em tempo real os sistemas e redes da ID Singular. Essas ferramentas permitem identificar rapidamente atividades incomuns, como tentativas de acesso não autorizado ou alterações suspeitas em dados sensíveis.
- **Análise de Logs:** Todos os logs de acesso aos sistemas, transações e interações com dados pessoais são centralizados e analisados continuamente. Qualquer evento suspeito é imediatamente destacado para revisão detalhada. Além disso, são configurados alertas automáticos para notificar a equipe de segurança sobre possíveis incidentes.
- **Registro de Incidentes:** Para cada evento suspeito ou incidente confirmado, os registros são mantidos detalhados onde incluem a data, hora, descrição do evento, sistemas afetados, usuários envolvidos, e ações tomadas. Esses registros são mantidos em um repositório seguro e são usados para auditorias internas e investigações futuras.
- **Comunicação Imediata:** Quando um incidente é identificado, as equipes responsáveis, como segurança da informação, TI, e a gestão de riscos, são notificadas imediatamente por meio de sistemas automatizados de alerta. A comunicação rápida garante uma resposta ágil para minimizar os impactos do incidente.

2.2. AVALIAÇÃO E CONTENÇÃO

A ID Singular adota as seguintes práticas para avaliar e conter incidentes de dados pessoais:

- **Avaliação Inicial:** Imediatamente após detectar um incidente, é realizada uma avaliação inicial para identificar sua gravidade e impacto potencial.
- **Medidas de Contenção:** Quando necessário, o sistemas afetados é desconectado da rede e as senhas comprometidas alteradas para conter a propagação do incidente.
- **Isolamento de Sistemas Comprometidos:** Em caso de risco grave, isolamos fisicamente ou virtualmente os sistemas comprometidos para evitar a propagação do problema.

2.3. NOTIFICAÇÃO E COMUNICAÇÃO

A ID Singular segue as diretrizes abaixo para notificação e comunicação de incidentes relacionados a dados pessoais:

- **Notificação às Autoridades:** Em conformidade com a LGPD, as autoridades competentes são notificadas, como a Autoridade Nacional de Proteção de Dados (ANPD), quando um incidente envolve o vazamento ou exposição de dados pessoais sensíveis. A notificação é feita dentro do prazo estipulado pela legislação (geralmente até 72 horas após a detecção do incidente), incluindo informações sobre o incidente, dados afetados e medidas adotadas para mitigação.
- **Informação aos Titulares:** Quando o incidente envolve dados pessoais de titulares, e há risco relevante para seus direitos e liberdades, os titulares são notificados de forma transparente. A comunicação inclui uma descrição clara do incidente, os dados afetados, as ações que a ID Singular está tomando para resolver a situação e as medidas que os titulares podem tomar para proteger-se, caso necessário.
- **Comunicação com Stakeholders:** Os nossos stakeholders (clientes, parceiros, e outros envolvidos) são informados sobre os incidentes de forma clara e objetiva. As atualizações regulares são feitas para garantir que todos compreendam as ações tomadas para resolver o problema e as medidas preventivas que serão implementadas para evitar incidentes semelhantes no futuro. A transparência nesse processo ajuda a manter a confiança na ID Singular e reforça nosso compromisso com a segurança dos dados.

3. POLÍTICA DE CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

Garantir a continuidade das operações da ID Singular e a recuperação rápida de dados e sistemas essenciais em caso de incidentes, desastres ou falhas críticas. Este plano busca minimizar os impactos negativos, assegurando que as funções vitais sejam mantidas e que a ID Singular consiga se recuperar rapidamente.

3.1. IMPLEMENTAÇÃO DE MEDIDAS PREVENTIVAS

- **Backups Regulares:** São realizados backups diários, semanais e mensais dos dados críticos para garantir a recuperação rápida e eficiente.
- **Procedimentos Operacionais:** Os procedimentos operacionais específicos são definidos para priorizar sistemas críticos e manter funções essenciais durante um incidente.
- **Plano de Backup de Pessoal:** Os planos de backup de pessoal são estabelecidos para garantir que outras pessoas possam assumir responsabilidades em caso de ausência de colaboradores-chave.
- **Comunicação Interna Clara:** Os fluxos de comunicação foram criados para garantir que todos saibam o que fazer durante um incidente.
- A **equipe de TI** é responsável por conter e mitigar o impacto técnico do incidente.
- A **equipe de comunicação** lida com a notificação e a interação com stakeholders e autoridades.
- A **equipe jurídica** acompanha o cumprimento das regulamentações e garante que todas as obrigações legais, como a notificação à ANPD, sejam atendidas.
- **Reuniões periódicas** são realizadas para revisar e atualizar os papéis de acordo com mudanças organizacionais ou de processos.

3.2. TESTES E SIMULAÇÕES

• **Testes de Recuperação:**

Conduzimos testes periódicos para validar os processos de recuperação, simulando a perda de dados ou falhas críticas nos sistemas. Isso garante que a ID Singular esteja preparada para atuar rapidamente em caso de emergência,minimizando o tempo de inatividade e a perda de dados.

• **Treinamento Regular das Equipes:**

Os treinamentos periódicos são realizados com o objetivo de orientar nossa equipe sobre as melhores práticas de segurança da informação e a importância da proteção de dados pessoais, além de preparar todos para agir de maneira eficaz em incidentes.

• **Revisão Contínua do Plano:**

Nosso plano é revisado e atualizado com base em auditorias periódicas e feedback de simulações, garantindo que esteja sempre alinhado com as necessidades da ID Singular e com as mudanças no cenário de segurança.

4. POLÍTICA DE DESCARTE E DESTRUIÇÃO DE DADOS PESSOAIS

Esta política estabelece diretrizes claras e eficazes para o descarte e destruição de dados pessoais e documentos contendo informações sensíveis, garantindo a conformidade com a Lei Geral de Proteção de Dados (LGPD) e protegendo a segurança, a confidencialidade e a integridade das informações. O descarte e a destruição são realizados de forma irreversível, assegurando que os dados não possam ser recuperados ou reutilizados após a eliminação.

Abrangência

Esta política se aplica a todos os dados pessoais, sensíveis ou não, armazenados de forma digital ou física pela ID Singular, incluindo aqueles coletados de colaboradores, clientes, fornecedores e qualquer outra parte com quem a ID Singular mantenha relações.

4.1. DIRETRIZES PARA DESCARTE DE DADOS PESSOAIS

Dados Digitais

Todos os dados pessoais armazenados em sistemas digitais são eliminados de forma definitiva quando não são mais necessários para a finalidade original para a qual foram coletados.

O descarte de dados digitais é realizado utilizando softwares de sobrescrita segura, garantindo que os dados sejam irrecuperáveis.

Quando necessário, dispositivos de armazenamento (HDs, SSDs, pen drives, etc.) são destruídos fisicamente para garantir a irrecuperabilidade dos dados neles armazenados.

Documentos Físicos

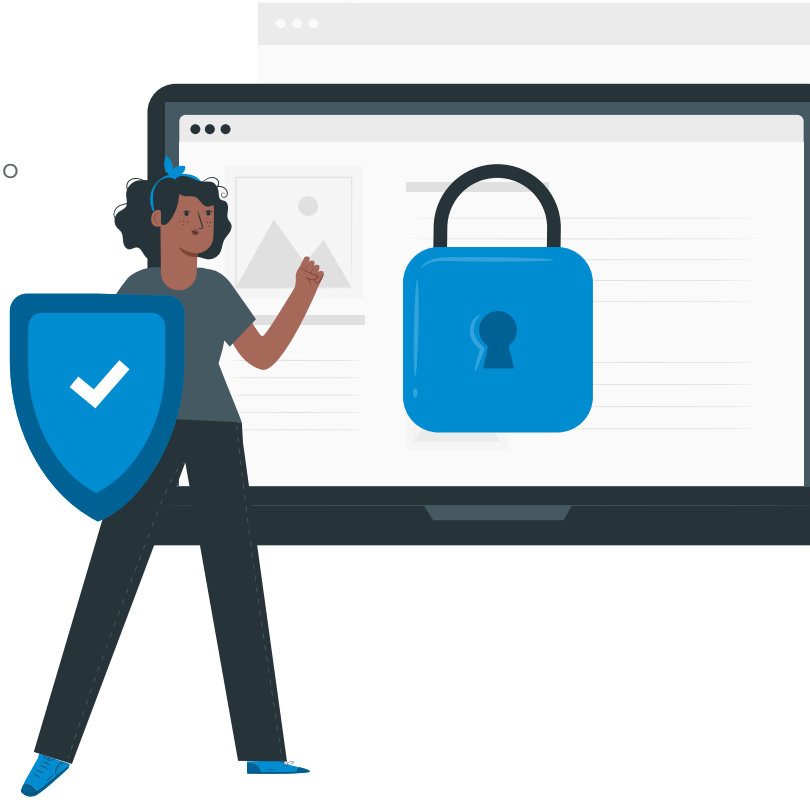
Documentos impressos que contêm dados pessoais são destruídos por meio de trituração ou outro método físico que garante a irreversibilidade da destruição.

4.2. PROCEDIMENTOS PARA DESCARTE E DESTRUIÇÃO

Mapeamento de Dados

Antes do descarte ou destruição, os dados ou documentos a serem eliminados são mapeados, incluindo:

- Tipo de dado
- Método de descarte/destruição
- Data da eliminação
- Responsável pela ação
- Justificativa para o descarte/destruição



Monitoramento e Supervisão

O DPO (Encarregado de Dados) supervisiona e monitora o cumprimento desta política, garantindo que os procedimentos de descarte e destruição sejam realizados de acordo com as diretrizes estabelecidas.

A área de TI e os setores responsáveis pelo armazenamento de dados garantem a execução adequada dos processos de eliminação, fornecendo relatórios periódicos ao DPO para garantir a rastreabilidade das ações.

Treinamento e Conscientização

Todos os colaboradores que lidam com dados pessoais recebem treinamento sobre os procedimentos de descarte e destruição de dados, a fim de garantir a execução correta e segura dessas atividades.

A conscientização sobre a importância da proteção e eliminação de dados é reforçada periodicamente, promovendo a cultura de segurança da informação na ID Singular.

Qualquer violação desta política é tratada de acordo com as normas internas da ID Singular, podendo resultar em ações disciplinares.

A política é revista periodicamente para garantir que continue atendendo aos requisitos legais e melhores práticas de segurança da informação.

5. POLÍTICA DE RETENÇÃO E BACKUP

A Política de Retenção e Backup tem como objetivo garantir a integridade, disponibilidade e segurança dos dados pessoais por meio de práticas consistentes de backup e recuperação de dados. A política assegura a proteção das informações armazenadas, permitindo a recuperação dos dados em caso de perda, falha ou incidente, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Abrangência:
Esta política se aplica a todos os dados pessoais e sensíveis armazenados pela ID Singular, tanto em ambientes digitais quanto físicos, que precisam ser protegidos por meio de backups periódicos, a fim de garantir a continuidade e segurança da informação.

5.1 . PROCEDIMENTOS DE BACKUP

5.1.1. Tipos de Backup

- **Mensal:**

Realizamos backups completos dos dados armazenados, com retenção de 2 meses. Esses backups garantem uma cópia completa de todos os dados necessários para a recuperação total em caso de falha ou perda de dados.

- **Semanal:**

São realizados backups incrementais semanalmente, com retenção de 3 semanas. Esses backups incluem apenas os dados modificados ou novos desde o último backup completo ou incremental.

- **Diário:**

Realizamos backups incrementais diários, com retenção de 5 dias. O objetivo é garantir que as alterações recentes nos dados sejam registradas de forma contínua e que, em caso de necessidade, seja possível recuperar os dados até o dia anterior ao incidente.

5.1.2. Criptografia dos Backups

- Todos os backups realizados, tanto completos quanto incrementais, são criptografados em trânsito (durante o envio) e em repouso (enquanto armazenados), garantindo que os dados estejam protegidos contra acessos não autorizados.

5.1.3. Armazenamento de Backups

- Os backups são armazenados em locais seguros, fisicamente separados, e em ambientes protegidos contra riscos de falhas ou incidentes, com acesso restrito e monitorado para garantir a integridade dos dados.

5.2. PLANO DE RECUPERAÇÃO

5.2.1 Ferramentas de Recuperação

- Ferramentas automatizadas são utilizadas para a recuperação de dados, que permitem restaurar rapidamente informações de diferentes pontos no tempo, começando pelos backups completos mensais. Essas ferramentas são configuradas para realizar a recuperação de dados de maneira eficiente e sem perda de integridade.

5.2.2 Procedimento de Recuperação

- A recuperação de dados segue a seguinte ordem de prioridade:

Backup Completo Mensal: caso seja necessário restaurar uma quantidade significativa de dados ou um período mais antigo, começa-se pelo backup completo mensal.

Backup Incremental Semanal: utilizado para restaurar dados alterados ou adicionados nas últimas semanas.

Backup Incremental Diário: usado para restaurar dados recentes, até 5 dias atrás, com a mínima perda de informações.

5.2.3 Testes de Recuperação

- A ID Singular Realiza periodicamente testes de recuperação para garantir a eficácia e funcionalidade do processo de recuperação de dados. Esses testes são realizados pela equipe de TI para assegurar que os backups podem ser restaurados de forma rápida e segura, atendendo aos padrões de continuidade e proteção de dados.

Todos os processos de backup são monitorados de forma contínua, e auditorias regulares são realizadas para garantir que os backups estão sendo executados conforme o cronograma e que os dados estão devidamente protegidos.

6. POLÍTICA DE SEGURANÇA DE REDE E CONTROLE DE ACESSO

Esta política estabelece as diretrizes e procedimentos para a gestão de acessos ao sistema ID System, visando garantir a segurança da informação, a confidencialidade dos dados e a integridade do sistema.

6.1. OBJETIVOS

- Definir os papéis e responsabilidades na gestão de acessos.
- Estabelecer os critérios para concessão, alteração e revogação de acessos.
- Garantir a conformidade com as normas e regulamentações apl'icáveis.
- Minimizar os riscos de acessos não autorizados e uso indevido do sistema.

6.2. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, parceiros, fornecedores e demais usuários que tenham acesso ao sistema ID System.

6.3. PAPÉIS E RESPONSABILIDADES

- **Gestor do Sistema:** Responsável por definir os perfis de acesso, conceder e revogar acessos, monitorar a atividade do sistema e garantir a conformidade com esta política.

- **Gestores de Área:** Responsáveis por solicitar a concessão de acessos para seus colaboradores e garantir que os acessos sejam utilizados de forma adequada.
- **Usuários:** Responsáveis por utilizar seus acessos de forma segura e responsável, cumprindo as normas e diretrizes estabelecidas.
- **Equipe de Segurança da Informação:** Responsável por definir os controles de segurança, monitorar a atividade do sistema, investigar incidentes de segurança e garantir a conformidade com as normas e regulamentações aplicáveis.

6.4. CRITÉRIOS PARA CONCESSÃO DE ACESSOS

- Os acessos serão concedidos com base no princípio do menor privilégio, ou seja, apenas os acessos necessários para o desempenho das funções do usuário serão concedidos.
- A concessão de acessos será solicitada pelo gestor de área, mediante justificativa e aprovação do gestor do sistema.
- Os acessos serão concedidos por meio de perfis de acesso, que definem as permissões e restrições de cada usuário.
- Os acessos serão revisados periodicamente para garantir que estejam adequados às necessidades do usuário.

6.5. PROCEDIMENTOS PARA CONCESSÃO, ALTERAÇÃO E REVOGAÇÃO DE ACESSOS

- A solicitação de concessão de acessos deverá ser feita por meio eletrônico, endereçado ao e-mail do gestor de área.
- A alteração de acessos deverá ser solicitada pelo gestor de área, mediante justificativa e aprovação do gestor do sistema.
- A revogação de acessos deverá ser solicitada pelo gestor de área ou realizada automaticamente em caso de desligamento do usuário, alteração de função ou violação desta política.
- Todas as concessões, alterações e revogações de acessos serão registradas em um log de auditoria.

6.6. SENHAS

- Os usuários deverão utilizar senhas fortes e complexas, com no mínimo 8 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais.

- As senhas deverão ser alteradas periodicamente, a cada 3 meses.
- As senhas não deverão ser compartilhadas com terceiros.
- Os usuários não deverão utilizar senhas padrão ou fáceis de serem adivinhadas.

6.7. MONITORAMENTO E AUDITORIA

- A atividade do sistema será monitorada continuamente para identificar acessos não autorizados e • uso indevido do sistema.
- erão realizadas auditorias periódicas para verificar a conformidade com esta política.
- Os logs de auditoria serão armazenados por um período de 5 anos.

6.8. INCIDENTES DE SEGURANÇA

- Qualquer incidente de segurança, como acesso não autorizado, uso indevido do sistema ou suspeita de violação desta política, deverá ser comunicado imediatamente à equipe de segurança da informação.
- A equipe de segurança da informação investigará o incidente e tomará as medidas cabíveis.

7. POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÕES

Os mecanismos de análise de privacidade e proteção de dados pessoais são adotados desde a concepção de nossos produtos, serviços e projetos, conforme o princípio do Privacy by Design. Nossa prioridade é garantir que a privacidade dos dados pessoais seja protegida em todas as fases do ciclo de vida da informação, alinhando nossas práticas às exigências da Lei Geral de Proteção de Dados (LGPD). Além disso, a ID Singular garante a segurança de sua infraestrutura de rede para proteger os sistemas e dados contra acessos maliciosos e vulnerabilidades externas.

Abrangência:
Esta política se aplica a todos os processos internos, produtos, serviços e projetos que envolvem o tratamento de dados pessoais e à segurança de rede da ID Singular.

7.1. PRÁTICAS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

7.1.1 Minimização de Dados

- A ID Singular coleta e processa apenas os dados pessoais estritamente necessários para a finalidade específica de cada serviço. Buscamos sempre a minimização da quantidade de dados coletados, evitando o tratamento de dados excessivos ou não pertinentes.

7.1.2 Controle de Acesso

- A ID Singular implementa restrições de acesso com base no princípio dos privilégios mínimos, garantindo que apenas usuários autorizados, e que realmente necessitam, possam acessar dados

sensíveis. O controle é rígido, e as permissões são revisadas periodicamente.

7.1.3 Criptografia e Proteção de Dados

- A ID Singular utiliza criptografia para proteger as informações tanto em trânsito quanto em repouso. Isso assegura que dados pessoais e sensíveis estejam protegidos contra acessos não autorizados durante a transmissão e quando armazenados.

7.2. ANÁLISE DE IMPACTO E TESTES DE SEGURANÇA

7.2.1 Revisão e Auditoria Contínua

- Antes da implementação de novos produtos ou funcionalidades, a ID Singular realiza avaliações de impacto à privacidade para identificar e mitigar riscos. Além disso, conduzimos testes de segurança regularmente para assegurar que as medidas de proteção estejam funcionando de forma eficaz.

Todas as revisões e aplicações de medidas de segurança são documentadas e armazenadas para auditoria. Os registros incluem:

- Logs de acessos e eventos registrados pelo GoAccess e Matomo.
- Logs de bloqueios automáticos de bots e ataques identificados pelo Apache Ultimate Bad Bot
- Blocker e Fail2Ban.
- Configurações e histórico de alterações no firewall (IPTables e Security Groups da AWS).
- Relatórios de aplicação de patches de segurança.

7.2.2 Avaliações de Segurança

- Avaliações de segurança contínuas são realizadas para detectar vulnerabilidades e adotar as correções necessárias, garantindo a integridade e a proteção dos dados pessoais tratados.

7.3. CONFORMIDADE REGULATÓRIA

7.3.1 Registro e Conformidade

- A ID Singular mantém documentação completa sobre as medidas adotadas para garantir conformidade com a LGPD e outras regulamentações aplicáveis. Isso inclui registros das práticas de privacidade implementadas, bem como a manutenção de auditorias de conformidade periódicas.

7.4 AVALIAÇÃO PERIÓDICA DE SEGURANÇA DE REDE

7.4.1. Procedimentos de Avaliação Periódica

Revisões semanais de segurança são realizadas, utilizando as seguintes ferramentas e métodos:

Monitoramento de Acessos

- **GoAccess:** Ferramenta utilizada para análise em tempo real dos logs de acesso (access_log) do servidor, permitindo a identificação de picos de acessos suspeitos e padrões anormais de tráfego.
- **Matomo Analytics:** Análise de acessos para identificação de origens suspeitas, incluindo acessos automatizados e comportamentos anômalos.

Bloqueio de Bots e Tráfego Malicioso

- **Apache Ultimate Bad Bot Blocker:** Implementação de bloqueio automático de bots maliciosos e acessos suspeitos ao servidor web.

7.4.2 Controle de Firewall e Bloqueio de IPs Suspeitos

- **IPTables e Security Groups (AWS EC2):** Configuração e revisão das regras de firewall para restringir acessos maliciosos e bloquear tráfego não autorizado.
- **Fail2Ban:** Ferramenta utilizada para detectar e bloquear IPs suspeitos com base em padrões de ataques identificados nos logs do sistema.

7.4.3 Atualizações de Patches de Segurança

- Aplicação semanal de patches de segurança conforme descrito no Documento de Procedimentos de Gerenciamento de Patches, garantindo que vulnerabilidades conhecidas sejam mitigadas rapidamente.

8. POLÍTICA DE AVALIAÇÕES PERIÓDICAS DE SEGURANÇA DE REDE

A ID Singular realiza avaliações periódicas de segurança de rede em nossa infraestrutura baseada em **Amazon Linux 2023**. O foco dessas avaliações está na detecção e mitigação de acessos maliciosos e na aplicação contínua de regras de firewall para proteger nossos sistemas e dados sensíveis.

Abrangência:
Esta política se aplica a todas as práticas de segurança de rede adotadas pela ID Singular, com foco na proteção contra ameaças externas e internas.

8.1. PRÁTICAS DE SEGURANÇA DE REDE

8.1.1 Monitoramento de Acessos

- Continuamente os acessos aos nossos sistemas são monitorados para detectar e mitigar ataques de força bruta, principalmente no SSH e no login da aplicação. Utilizamos o **GoAccess** para análise em tempo real dos logs de acesso do servidor, permitindo-nos identificar picos de acessos suspeitos e padrões anômalos de tráfego. Também realizamos uma análise detalhada dos acessos através do **Matomo Analytics**, o que nos ajuda a identificar origens suspeitas e comportamentos automatizados ou anômalos.

8.1.2 Análises de Vulnerabilidade

- A ID Singular conduz análises regulares de vulnerabilidades, revisando logs e alertas de segurança provenientes da AWS (Amazon Web Services). Essas análises são realizadas para identificar brechas de segurança em potencial, e tomamos ações proativas para corrigir qualquer vulnerabilidade identificada.

8.1.3 Gerenciamento de Firewall

- A ID Singular gerencia ativamente o firewall para bloquear tráfego suspeito e restringir acessos indevidos à nossa rede. Configuramos regras no **IPTables** e **Security Groups da AWS EC2** para permitir apenas o tráfego legítimo e eliminar riscos de intrusão. Também utilizamos o **Fail2Ban** para detectar e bloquear IPs suspeitos com base em padrões de ataques identificados nos logs.

8.1.4 Registro de Alterações

- A ID Singular mantém uma documentação detalhada de todas as alterações realizadas na nossa infraestrutura de TI. Antes de implementar qualquer mudança, uma revisão e aprovação é realizada para garantir que as alterações não comprometam a segurança da rede e que estejam em conformidade com as melhores práticas de segurança.

8.2. MONITORAMENTO E AUDITORIA

- **Monitoramento Contínuo:** Em tempo real monitoramos os acessos e o tráfego de rede, com alertas imediatos para qualquer atividade suspeita. As ferramentas **GoAccess** e **Matomo** são usadas para garantir que qualquer acesso anômalo seja identificado rapidamente e tratado de forma adequada.
- **Auditoria de Segurança:** Auditorias periódicas são realizadas para verificar se todas as práticas de segurança estão sendo seguidas corretamente e para identificar áreas que podem ser aprimoradas. Todos os logs e ações tomadas são documentados para auditoria e revisão contínua

9. RESPONSABILIDADES

DPO
(Encarregado de Dados)

Supervisiona as práticas de segurança para garantir que os dados pessoais sejam protegidos contra ameaças externas e internas, conforme exigido pela LGPD.

TI
(Tecnologia da Informação)

Responsável por implementar e monitorar as práticas de segurança de rede, realizando análises de vulnerabilidades, configurando firewalls, e garantindo que as alterações na infraestrutura sejam seguidas de revisão e aprovação.

COLABORADORES

Devem seguir as práticas de segurança definidas, reportando qualquer atividade suspeita e contribuindo para a proteção da rede.

10. CONCLUSÃO

Este Manual Interno de Proteção de Dados Pessoais (LGPD) da ID Singular foi elaborado com o objetivo de estabelecer diretrizes claras, políticas internas e procedimentos que garantam a conformidade com a Lei Geral de Proteção de Dados (LGPD) e a proteção dos direitos dos titulares de dados. O documento consolida as melhores práticas para o tratamento seguro de dados pessoais, a mitigação de riscos, a resposta eficaz a incidentes de segurança e a promoção de uma cultura organizacional voltada para a privacidade e a proteção de dados.

É importante destacar que este manual está sujeito a revisões e atualizações periódicas, conforme necessário, para acompanhar as mudanças nas diretrizes internas, nas regulamentações legais e nas melhores práticas do mercado. Qualquer atualização será comunicada de forma transparente, garantindo que todos os colaboradores e partes interessadas estejam alinhados com as novas práticas e procedimentos.

Ressalta-se que este manual não se sobrepõe à legislação vigente, servindo como um complemento às normas legais estabelecidas pela LGPD e outras regulamentações aplicáveis. A ID Singular reitera seu compromisso com a proteção de dados pessoais, a transparência em suas operações e a adoção de medidas proativas para garantir a segurança e a privacidade das informações sob sua responsabilidade.

SINGULAR

Whatsapp: 11 9 3450 2785

www.idsingular.com.br | contato@idsingular.com.br