

PROVIDER IT. | Caminhe por novos futuros

Política de Segurança da Informação

01 OBJETIVO

A nossa Política de Segurança da Informação (PSI) tem como principal objetivo proteger a Provider IT e todos os nossos colaboradores, garantindo um ambiente de trabalho seguro em relação ao uso de dados e da tecnologia, independentemente do modelo de trabalho adotado (presencial, híbrido ou remoto).

Esta política visa proteger nossos ativos de informação, garantindo a confidencialidade, integridade e disponibilidade dos dados, com o intuito de mitigar riscos de segurança, prevenir violações de dados, estar em conformidade com regulamentações e, assim, criar um ambiente seguro para todas as nossas operações.

Acreditamos que a segurança da informação é responsabilidade compartilhada de todos nós — não apenas uma obrigação técnica, mas um reflexo do respeito que temos pelas pessoas, pelos dados que nos foram confiados e pela confiança que nossos clientes depositam na Provider IT.

Este compromisso está diretamente alinhado com:

• Código de Conduta Ética (Seções 3.10 e 5.20);

• Política de Proteção de Dados (PPD);

• Política de Tratamento de Incidentes de Segurança da Informação (PTISI);

• Política de Inteligência Artificial;

• Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

• ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação.

02 ABRANGÊNCIA

As diretrizes desta Política destinamse a todos os diretores, gestores e a todos os nossos colaboradores diretos e indiretos da Provider IT, que são os responsáveis pela ciência e cumprimento das diretrizes aqui estabelecidas, em nível nacional.

A PSI aplicase a todos os modelos de trabalho, incluindo:

• Colaboradores de backoffice em modelo híbrido;

• Colaboradores técnicos alocados em clientes (modelo remoto ou híbrido);

• Prestadores de serviços e terceiros que utilizem o ambiente de processamento da Provider IT ou tenham acesso a informações pertencentes à empresa.

Todo e qualquer colaborador que utilize recursos computadorizados da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática, **independentemente do local em que esteja trabalhando**.

03 VIOLAÇÕES

A violação desta Política de Segurança é qualquer ato que:

• Exponha a Provider IT a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou de informações ou ainda da perda de equipamento;

• Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;

• Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental;

• Resulte no acesso, compartilhamento ou tratamento indevido de dados pessoais de colaboradores, clientes, candidatos ou qualquer outro titular, em desconformidade com a LGPD e com a Política de Proteção de Dados da Provider IT;

• Implique no uso de informações de um cliente para beneficiar outro, violando o princípio de confidencialidade multicliente.

04 CLASSIFICAÇÃO DAS INFORMAÇÕES

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área, de acordo com a tabela abaixo.

Essa classificação é o primeiro passo prático para que todos nós apliquemos o tratamento adequado às informações com as quais trabalhamos, conforme o Código de Conduta Ética (Seção 5.20) e a ISO/IEC 27001.

NÍVEL	DESCRIÇÃO
Pública	Acessível a todos
Interna	Restrita aos nossos colaboradores
Confidencial	Acessível a nossos colaboradores e parceiros autorizados
Restrita	Acessível apenas a colaboradores expressamente indicados

05 CONCEITOS

Informação Pública: É toda informação que pode ser acessada por nossos colaboradores, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por nossos colaboradores. São informações que possuem um grau de confidencialidade que pode comprometer nossa imagem.

Informação Confidencial: É toda informação que pode ser acessada por nossos colaboradores e por nossos parceiros. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao nosso negócio ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por colaboradores explicitamente indicados pelo nome ou pela área a que pertencem. A divulgação não autorizada dessa informação pode causar sérios danos ao nosso negócio e/ou comprometer nossa estratégia.

Todo Gerente/Supervisor deve orientar sua equipe a não circular informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa" ao terminar o trabalho, não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre as mesas.

06 PROGRAMAS ILEGAIS

Respeitamos os direitos autorais dos programas que usamos e reconhecemos que devemos pagar o justo valor por eles. É terminantemente proibido o uso de programas ilegais (sem licenciamento) na Provider IT. Nossos colaboradores não podem, em hipótese alguma, instalar este tipo de software nos equipamentos da companhia.

Somente nossa equipe de Informática tem autorização para instalação de programas previamente autorizados dentro desta Política. Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos colaboradores, visando garantir a correta aplicação desta diretriz.

Caso sejam encontrados programas não autorizados, estes deverão ser removidos imediatamente. Os colaboradores que instalarem programas não autorizados se responsabilizam perante a empresa por quaisquer problemas ou prejuízos oriundos desta ação, estando sujeitos às sanções previstas nesta Política e no Código de Conduta Ética.

07 CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOP

Não é política da Provider IT o armazenamento de dados em desktops individuais; entretanto, existem alguns programas que não permitem o armazenamento em rede. Nestes e em outros casos, nossa equipe de Informática deverá alertar o colaborador de que ele deve realizar backup dos dados de sua máquina periodicamente.

É responsabilidade dos próprios colaboradores a elaboração de cópias de segurança (backups) de dados e outros arquivos ou documentos desenvolvidos em suas estações de trabalho e que não sejam considerados de fundamental importância para a continuidade dos negócios.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios, o Setor de Informática disponibilizará um espaço nos servidores onde cada colaborador deverá manter estas informações, que serão incluídas na rotina diária de backup da área.

Colaboradores em regime remoto ou híbrido devem observar as mesmas diretrizes de backup, utilizando exclusivamente os repositórios corporativos aprovados pelo Setor de Informática. É vedado o armazenamento de dados de trabalho em serviços de nuvem pessoais (como contas pessoais de Google Drive, Dropbox, iCloud ou equivalentes).

08 DESCARTE DE MATERIAL DE INFORMÁTICA

Com o objetivo de atender às demandas socioambientais, mantemos parceria com uma empresa de descarte de materiais, e toda mídia descartada passa por processo de inventário e destruição de dados, conforme sua necessidade e complexidade.

Antes de qualquer descarte, doação ou retorno de equipamentos, é obrigatória a sanitização completa de dados pelo Setor de Informática, garantindo que nenhuma informação confidencial, restrita ou de clientes permaneça nos dispositivos. Esta diretriz está alinhada com a Política Ambiental da Provider IT (Seção 3.4) e com a Política de Proteção de Dados (PPD).

09 SEGURANÇA E INTEGRIDADE DO BANCO DE DADOS

Nosso Setor de Informática é o responsável exclusivo pelo gerenciamento dos nossos bancos de dados, assim como pela manutenção, alteração e atualização de equipamentos e programas, garantindo a integridade e a disponibilidade das informações fundamentais para nossas operações.

O acesso a bases de dados deve observar o princípio do privilégio mínimo: cada colaborador acessa apenas os dados estritamente necessários ao desempenho de suas funções, conforme autorização formal do seu gestor.

10 PROPRIEDADE INTELECTUAL

10.1. Criações no âmbito da Provider IT (backoffice e operações internas)
São de propriedade da Provider IT todos os designs, criações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício com a empresa, no exercício de suas funções internas.

10.2. Criações no âmbito de alocações em clientes

⚠️ Atenção – Regra específica para colaboradores alocados:

Trabalhos, desenvolvimentos, códigos, soluções e demais criações intelectuais produzidos por colaboradores durante a prestação de serviços em alocação pertencem ao CLIENTE, conforme definido no contrato de prestação de serviços firmado entre a Provider IT e o respectivo cliente. Esta regra prevalece sobre a disposição geral do item 10.1, por força contratual.

Os colaboradores alocados devem:

• Respeitar rigorosamente os acordos de Propriedade Intelectual estabelecidos entre a Provider IT e o cliente;

• Não reutilizar código, soluções, metodologias ou ativos desenvolvidos em um cliente em outro projeto, sem autorização expressa e documentada de ambas as partes;

• Documentar adequadamente contribuições que possam gerar dúvidas futuras sobre titularidade;

• Consultar o Departamento Jurídico da Provider IT antes do início do desenvolvimento, em caso de qualquer dúvida sobre titularidade.

Em casos de desenvolvimento conjunto Provider IT + cliente, ou quando houver dúvida sobre titularidade, os colaboradores devem consultar previamente o Departamento Jurídico (conforme Código de Conduta Ética, Seção 5.10, e Política de Ética Empresarial, Seção 9.1).

11 INTERNET

O acesso à Internet será autorizado aos colaboradores que necessitarem da mesma para o desempenho das suas atividades profissionais na Provider IT. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

O uso da Internet será monitorado pelo Setor de Informática, inclusive através de logs que informam qual colaborador está conectado, o tempo de uso e qual página acessou.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da Provider IT sem expressa anuência do Setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

Nossos colaboradores devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

De estações de rádio;
De conteúdo pornográfico ou relacionados a sexo;
De apostas e jogos online;
Que defendam atividades ilegais;
Que menosprezem, depreciem ou incitem qualquer tipo de preconceito;
Que promovam a participação em salas de discussão de assuntos não relacionados aos nossos negócios;
Que promovam discussão pública sobre os nossos negócios, a menos que autorizado pela nossa Diretoria;
Que possibilitem a distribuição de informações de nível "Confidencial"; Que permitam a transferência (downloads) de arquivos e/ou programas ilegais. 12

Portais de Inteligência Artificial públicos (acesso via Internet): o uso de ferramentas de IA publicamente acessíveis (como ChatGPT, Gemini e equivalentes) para fins corporativos é regido integralmente pela Política de Inteligência Artificial da Provider IT.
É vedado inserir, carregar, transmitir ou disponibilizar em ferramentas de IA públicas, abertas ou não aprovadas pela Provider IT informações não públicas da empresa, de clientes, fornecedores, parceiros, colaboradores ou terceiros.

A vedação inclui, sem se limitar a, contratos e anexos, e-mails e documentos internos, dados pessoais, informações financeiras, comerciais ou estratégicas, códigos-fonte, especificações técnicas, arquiteturas de sistemas, credenciais, senhas, chaves, tokens e informações protegidas por obrigação de confidencialidade.

Quando houver dúvida sobre a classificação ou autorização para uso do conteúdo, o usuário não deverá enviá-lo e deverá consultar seu gestor e as áreas competentes.

O uso de plataforma corporativa aprovada não autoriza, por si só, o envio irrestrito de informações. Devem ser observados os perfis de acesso, as finalidades permitidas, as configurações de privacidade e retenção, os controles de segurança, as instruções documentadas aplicáveis e as obrigações contratuais do cliente. Sempre que adequado, devem ser usados dados públicos, fictícios, anonimizados ou minimizados.

Colaboradores com acesso à plataforma corporativa aprovada devem utilizá-la exclusivamente para atividades de trabalho.

12 USO CORRETO DO CORREIO ELETRÔNICO (EMAIL)

O correio eletrônico fornecido pela Provider IT é um instrumento de comunicação interna e externa para a realização dos nossos negócios. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a nossa imagem e não podem ser contrárias à legislação vigente nem aos nossos princípios éticos.

O uso do correio eletrônico é pessoal, e o colaborador é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam relativas a "correntes", conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da Provider IT ou de outras empresas;
- Sejam incoerentes com as nossas políticas;

- Contenham dados pessoais de titulares compartilhados sem a devida base legal e sem as salvaguardas exigidas pela LGPD e pela Política de Proteção de Dados.

O envio de arquivos contendo dados pessoais ou informações confidenciais por email é admitido apenas em caráter excepcional e, nesse caso, os arquivos devem estar protegidos por senha, comunicada por canal separado — conforme Política de Proteção de Dados (Seção 8).

Para incluir um novo colaborador no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao nosso Setor de Informática, que providenciará a inclusão. A utilização do email deve ser criteriosa, evitando que o sistema fique congestionado.

Em caso de congestionamento no sistema de correio eletrônico, nosso Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos colaboradores, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de emails gratuitos (liberados em sites da web) nos computadores da Provider IT.
Nosso Setor de Informática poderá, visando evitar a entrada de vírus em nosso ambiente, bloquear o recebimento de emails provenientes de sites gratuitos.

13 NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

Nosso Setor de Informática é responsável pela aplicação da nossa Política em relação à definição de compra e substituição de software e hardware.

Qualquer necessidade de novos programas ou de novos equipamentos de informática deverá ser discutida com o responsável pelo Setor de Informática.

Não é permitida a compra ou o desenvolvimento de softwares ou hardwares diretamente pelos colaboradores.

A adoção de qualquer nova ferramenta tecnológica, incluindo plataformas de IA, aplicativos de colaboração, sistemas de nuvem ou ferramentas de automação, deve ser precedida de avaliação de impacto de privacidade (Privacy by Design), em conformidade com a Política de Proteção de Dados e com a Política de Inteligência Artificial, antes de qualquer implementação.

14 USO DE NOTEBOOKS NA EMPRESA

Os colaboradores que tiverem direito ao uso de computadores pessoais (laptop ou notebook) ou qualquer outro equipamento computacional de propriedade da Provider IT devem estar cientes de que:

- Os recursos de TI disponibilizados têm como objetivo exclusivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio colaborador;
- É responsabilidade de cada colaborador assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O colaborador não deve alterar a configuração do equipamento recebido.
- Cuidados fora do ambiente de trabalho:
- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, transporte por aplicativo etc.;
- Quando transportar o equipamento em automóvel, utilize sempre o portamalas ou lugar não visível;

- Jamais conecte o equipamento corporativo a redes WiFi públicas sem o uso de VPN corporativa aprovada pelo Setor de Informática.

Em caso de furto ou perda:

- Registre a ocorrência em uma delegacia de polícia;
- Comunique imediatamente ao seu superior imediato e ao Setor de Informática;
- Comunique também ao DPO (dpo@providerit.com.br), pois a perda de equipamento com dados pode configurar incidente de segurança sujeito às obrigações previstas na PTISI e na LGPD;
- Envie uma cópia da ocorrência policial ao Setor de Informática.

15 RESPONSABILIDADE DOS GESTORES

Nossos gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus colaboradores aos sistemas e informações da Provider IT, cabendo a eles verificar se os colaboradores estão acessando exatamente as rotinas compatíveis com as suas respectivas funções.

Nosso Setor de Informática fará auditorias periódicas do acesso dos colaboradores às informações, verificando:

- Que tipo de informação o colaborador pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o colaborador a ter permissão de acesso;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

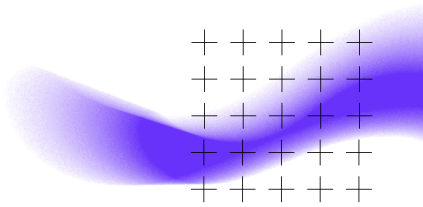
Gestores de equipes alocadas em clientes têm a responsabilidade adicional de assegurar que os colaboradores sob sua supervisão conheçam e cumpram simultaneamente as normas de segurança da Provider IT e, quando aplicável, as normas de segurança do cliente, reportando ao Setor de Informática qualquer conflito ou lacuna identificada.

16 SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições relacionadas aos meios de comunicação institucional, incluindo celulares corporativos, Microsoft Teams e quaisquer outras soluções de comunicação hospedadas ou em nuvem, são responsabilidade do Setor de Informática, em conformidade com as diretrizes definidas pela Diretoria.

Para fins de controle e transparência, ao final de cada mês o Setor de Informática enviará relatórios às gerências, indicando os custos associados a cada colaborador ou dispositivo de comunicação institucional.

17 USO DE ANTIVÍRUS



Todo arquivo em mídia proveniente de entidade externa à Provider IT deve ser verificado por programa antivírus.

Todo arquivo recebido/obtido através do ambiente Internet deve ser verificado por programa antivírus.

Todas as estações de trabalho devem ter um antivírus instalado, com atualização automática agendada pelo Setor de Informática via rede.

O colaborador não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

18 SEGURANÇA NO TRABALHO REMOTO E HÍBRIDO

Considerando que a Provider IT opera predominantemente em modelos de trabalho remoto e híbrido, tanto para colaboradores de backoffice, quanto para colaboradores técnicos alocados, as seguintes diretrizes de segurança se aplicam a todos os colaboradores fora das instalações físicas da empresa:

18.1. Ambiente e equipamento remoto

- Utilizar exclusivamente o equipamento corporativo fornecido pela Provider IT para o desempenho de atividades profissionais;
- Manter o ambiente de trabalho residencial com acesso restrito a pessoas não autorizadas enquanto sistemas corporativos estiverem em uso;
- Não realizar reuniões ou chamadas com informações confidenciais em locais públicos sem uso de fone de ouvido;
- Bloquear a tela do computador sempre que se ausentar, mesmo que por breve período.

18.2. Conexão e redes

- Utilizar exclusivamente redes de conexão seguras. Caso seja necessário utilizar redes externas (hotéis, cafés, coworkings), o uso de VPN corporativa é obrigatório;
- É vedada a conexão de equipamentos corporativos a redes sem senha ou redes públicas sem VPN ativa.

18.3. Videoconferências e reuniões virtuais

- Reuniões que envolvam conteúdo confidencial ou restrito não devem ser gravadas sem autorização prévia de todos os participantes;
- Links de reuniões corporativas não devem ser compartilhados publicamente ou em canais não autorizados;
- O uso de fundos virtuais é incentivado quando o colaborador estiver em ambiente doméstico, a fim de preservar a privacidade pessoal e a confidencialidade do ambiente.

18.4. Separação entre uso pessoal e profissional

- É vedado o uso dos equipamentos corporativos para atividades pessoais, bem como o uso de dispositivos pessoais para acesso a sistemas, dados ou comunicações corporativas sem autorização expressa do Setor de Informática (política de BYOD não está autorizada, salvo aprovação formal).

19 CONFIDENCIALIDADE MULTICLIENTE

Em razão do modelo de negócios da Provider IT, com alocação de recursos humanos em diferentes clientes, todos os colaboradores que atuem ou tenham atuado em projetos de diferentes clientes devem observar rigorosamente o princípio de separação de informações confidenciais ("chinese walls" informacionais), conforme estabelecido no Código de Conduta Ética (Seção 5.5).

É expressamente vedado:

- Utilizar conhecimentos, dados, códigos, metodologias ou qualquer informação confidencial obtida em uma alocação para beneficiar, orientar ou instrumentalizar outro cliente;
- Compartilhar, ainda que de forma genérica ou anonimizada, estratégias, arquiteturas, processos ou dados de um cliente com equipes de outro cliente;
- Aceitar alocação simultânea em clientes concorrentes sem aprovação prévia e documentada da Diretoria da Provider IT.

O descumprimento desta diretriz constitui violação grave desta Política e do Código de Conduta Ética, com potencial responsabilização civil e disciplinar.

20 USO RESPONSÁVEL DE INTELIGÊNCIA ARTIFICIAL

O uso de ferramentas de Inteligência Artificial no ambiente corporativo é regido integralmente pela Política de Inteligência Artificial da Provider IT. No contexto específico da segurança da informação, destacamse as seguintes diretrizes:

20.1. Vedações absolutas

- É proibida a inserção de dados pessoais, dados sensíveis, informações de clientes, dados financeiros ou qualquer informação classificada como Confidencial ou Restrita em plataformas de IA públicas (ChatGPT, Gemini, Copilot não corporativo ou equivalentes);
- Colaboradores com acesso à plataforma corporativa de IA aprovada pela Provider IT não podem utilizar, para fins de trabalho, qualquer outro portal de IA não autorizado.

20.2. Uso autorizado

- O uso de IA deve ser feito com supervisão humana obrigatória, especialmente em decisões críticas ou que envolvam dados de terceiros;

- Todo conteúdo gerado por IA e utilizado em entregas para clientes deve ser revisado e validado por profissional responsável antes do compartilhamento.

20.3. Incidentes relacionados a IA

- Qualquer incidente ético ou de segurança decorrente do uso de IA deve ser reportado imediatamente ao Comitê de Governança de IA pelo canal inteligencia.artificial@providerit.com.br e ao Setor de Informática para fins de gestão de incidente, conforme a PTISI.

21 GESTÃO DE ACESSOS E CREDENCIAIS

21.1. Princípio do privilégio mínimo

Todo acesso a sistemas, aplicações, ambientes de clientes e repositórios de dados deve ser concedido com base no princípio do menor privilégio necessário ao desempenho das funções do colaborador. Acessos ampliados devem ser formalmente justificados e aprovados pelo gestor responsável.

21.2. Gestão de senhas

- Senhas devem ser únicas por sistema e não podem ser compartilhadas com terceiros, nem mesmo com colegas ou superiores;

- É vedado o uso de senhas pessoais ou facilmente identificáveis (datas de nascimento, sequências numéricas simples);

- O Setor de Informática poderá implementar política de troca periódica de senhas e uso de autenticação multifator (MFA) nos sistemas críticos.

21.3. Desligamento e encerramento de acessos

- Ao término de qualquer contrato, alocação ou vínculo, os acessos concedidos ao colaborador ou prestador de serviço devem ser revogados imediatamente pelo Setor de Informática, mediante comunicação formal da área de Gestão de Pessoas ou do gestor responsável.

22 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todo colaborador ou prestador de serviço que identificar ou suspeitar de um incidente de segurança, incluindo acesso não autorizado, perda de equipamento, comportamento anômalo de sistema, suspeita de vazamento de dados ou qualquer evento que possa comprometer a segurança da informação, deve:

1. Reportar imediatamente ao Setor de Informática pelo canal suporte@providerit.com.br;
2. Comunicar seu gestor imediato em paralelo;
3. Não tentar remediar, ocultar ou investigar o incidente por conta própria;
4. Guardar sigilo sobre os detalhes do incidente durante e após a resposta.

O tratamento de incidentes de segurança obedece integralmente à Política de Tratamento de Incidentes de Segurança da Informação (PTISI) da Provider IT, que define papéis, responsabilidades, prazos de resposta, obrigações de notificação à ANPD e procedimentos de preservação forense.

Incidentes que envolvam dados pessoais serão comunicados ao Encarregado de Proteção de Dados (DPO) da Provider IT – Datablock Proteção de Dados Ltda., representada por Mariel Trabulse – pelo canal dpo@providerit.com.br, para avaliação do risco e eventual notificação à ANPD e aos titulares afetados, nos termos do Art. 48 da LGPD e da Resolução CD/ANPD nº 15/2024.

24 VIGÊNCIA E REVISÃO

A Provider IT cumprirá todas as leis e regulamentos aplicáveis à segurança da informação. Esta Política está sujeita a revisões e melhorias contínuas para garantir a eficácia das medidas de segurança.

A revisão desta Política ocorrerá, no mínimo, anualmente ou sempre que:

- Ocorrer incidente de segurança de nível Crítico ou Alto;
- Houver alteração relevante na legislação ou em normas técnicas de referência (LGPD, ISO 27001, resoluções da ANPD);
- Houver mudanças significativas na infraestrutura, nos serviços prestados ou no perfil de clientes da Provider IT;
- Uma auditoria interna ou externa identificar lacunas relevantes.

Canais de reporte de incidentes e dúvidas:

CANAL	FINALIDADE
suporte@providerit.com.br	Incidentes de segurança da informação (CSIRT/IRT)
dpo@providerit.com.br	Incidentes envolvendo dados pessoais (DPO)
inteligencia.artificial@providerit.com.br	Incidentes éticos ou de segurança relacionados ao uso de IA
eticaprovider@providerit.com.br	Violações éticas (Canal Interno – Comitê de Ética)

Documento: Política de Segurança da Informação | Provider IT
Periodicidade de Revisão: Anual
Versão: Setembro/2026
Documentos complementares: Política de Tratamento de Incidentes de Segurança da Informação (PTISI) | Política de Proteção de Dados (PPD) | Política de Inteligência Artificial | Código de Conduta Ética (Seções 3.10, 5.5, 5.19, 5.20)