Onfly Tecnologia Ltda

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EXTERNA

Versão 1.0
Data: 14/07/2025
Classificação: PÚBLICA

CRIADO POR:	REVISADO POR:	APROVADO POR:
Júlia Nunes Cyber Security Analyst julia@onfly.com.br	Fábio Samora Cyber Security Lead fabio@onfly.com.br	Christian Machado CTO christian@onfly.com.br

VERSÃO	DATA	ATUALIZAÇÃO	AUTOR
1.0	14/07/2025	Revisão	Fábio Samora - Cyber Security Lead

1. Objetivo

A presente Política de Segurança da Informação Externa tem como finalidade assegurar a transparência perante as partes interessadas quanto às práticas e controles de segurança da informação adotados pela Onfly.

Adicionalmente, estabelece diretrizes para que fornecedores e terceiros compreendam e atendam aos requisitos mínimos de segurança no tratamento de informações relacionadas à organização, em conformidade com os princípios do Sistema de Gestão de Segurança da Informação (SGSI).

2. Conceitos e Definições

Para fins de interpretação e aplicação desta política, são adotadas as seguintes definições:

- **Segurança da Informação:** Conjunto de práticas, processos e controles que visam preservar a confidencialidade, integridade, disponibilidade, rastreabilidade e, quando aplicável, a privacidade das informações, em todas as suas formas (física, digital, verbal).
- **Informação:** Todo e qualquer dado ou conteúdo que represente valor estratégico, operacional, jurídico ou pessoal para a Onfly, seus clientes, fornecedores ou demais partes interessadas.
- **Dado Pessoal:** Informação relacionada a pessoa natural identificada ou identificável, conforme definido na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018).
- **Parte Interessada:** Toda organização ou indivíduo externo à Onfly que, de forma direta ou indireta, interaja com seus dados, processos ou sistemas. Exemplos: fornecedores, parceiros, prestadores de serviço, clientes, órgãos reguladores.
- **Controle de Acesso:** Conjunto de mecanismos técnicos, físicos e organizacionais que garantem que apenas pessoas autorizadas tenham acesso às informações ou recursos específicos, conforme necessidade e perfil de privilégio.
- **Ativo da Informação:** Qualquer recurso que suporte o processamento, armazenamento ou transmissão de informações, incluindo equipamentos, softwares, documentos, contratos, sistemas e dados.
- **Incidente de Segurança da Informação:** Evento confirmado ou sob suspeita que comprometa, ou possa comprometer, a segurança da informação, como perda de dados, acesso não autorizado, indisponibilidade, vazamento ou uso indevido.
- **Classificação da Informação:** Processo de rotulagem das informações com base em sua criticidade e sensibilidade, sendo os níveis utilizados pela Onfly: Pública, Interna, Confidencial e Restrita.

- **SGSI (Sistema de Gestão de Segurança da Informação):** Estrutura composta por políticas, processos, controles e responsabilidades que sustentam a governança de segurança da informação da Onfly, conforme diretrizes da norma ISO/IEC 27001:2022.
- **Responsável pelo Risco:** Pessoa ou área designada formalmente para acompanhar, mitigar e responder a riscos que possam impactar a segurança da informação.
- **Fornecedor Crítico:** Terceiro cujo serviço tem impacto direto na continuidade, segurança ou conformidade das operações da Onfly. Está sujeito a controles e requisitos adicionais.

3. Relacionamento com partes interessadas

Os requisitos relacionados à segurança da informação, quando envolvem terceiros, devem ser documentados formalmente por meio de acordos específicos, como os Termos de Responsabilidade e Confidencialidade firmados entre a Onfly e as partes interessadas. Esses documentos têm como objetivo principal reduzir os riscos associados ao acesso, armazenamento, processamento ou qualquer outra forma de uso das informações estratégicas ou sensíveis da Onfly por parceiros externos.

As disposições estabelecidas nesta política são complementadas pelo questionário interno de Avaliação de Fornecedores, o qual integra os processos de diligência prévia e validação técnica exigidos pela organização. O referido acordo deverá contemplar, de maneira inequívoca e expressa, os controles mínimos de segurança da informação exigidos pela Onfly, além das cláusulas específicas que delineiam o escopo dos serviços contratados e os deveres correlatos do contratado.

Nos casos em que haja subcontratação ou envolvimento de outras entidades na cadeia de fornecimento, especialmente em contratações que envolvam serviços de tecnologia da informação, o acordo deverá assegurar que os mesmos padrões de segurança sejam observados por todos os participantes da cadeia, mediante cláusulas de extensão de responsabilidade e aderência às normas internas da contratante.

A Onfly mantém estabelecido um processo formal de gestão de fornecedores, o qual compreende etapas de avaliação, classificação de risco e monitoramento contínuo das práticas relacionadas à segurança da informação.

Esta política deve ser objeto de ampla divulgação junto às partes interessadas, sendo obrigatória sua revisão sempre que houver alterações materiais em seu conteúdo. A comunicação formal será realizada por intermédio dos canais oficiais previamente acordados com cada parceiro.

4. Controle de Acesso

Colaboradores vinculados a fornecedores e/ou clientes, incluindo eventuais terceiros por eles contratados, que tenham acesso a dados sob responsabilidade da Onfly, devem estar formalmente submetidos a compromissos de confidencialidade, firmados previamente ao início de suas atividades.

O fornecedor e/ou cliente responsável deverá manter um registro continuamente atualizado de usuários e perfis autorizados a acessar os sistemas de informação, garantindo a rastreabilidade e a conformidade com os princípios de necessidade e mínima permissão.

Adicionalmente, quaisquer dados pessoais armazenados fora das dependências da Onfly ou sob responsabilidade de fornecedores devem estar protegidos por controles adequados, incluindo procedimentos formais de autorização de acesso e uso de mecanismos de segurança como criptografia. O acesso a essas informações deve ser restrito exclusivamente a pessoal autorizado, de acordo com os níveis de privilégio definidos.

5. Análise de Segurança da Informação

Todos os fornecedores contratados pela Onfly devem demonstrar que adotam práticas consistentes de Segurança da Informação, implementadas, mantidas e operadas conforme normas reconhecidas internacionalmente, atendendo, no mínimo, aos requisitos estabelecidos em contrato.

A Onfly reserva-se o direito de realizar auditorias nos fornecedores, sempre que considerar necessário, com o propósito de verificar a conformidade com os controles definidos, além de avaliar a efetividade das medidas de proteção utilizadas.

Quando não for possível realizar auditorias diretamente, devido a limitações contratuais, operacionais ou riscos adicionais, recomenda-se que o fornecedor apresente evidências independentes que comprovem a adoção de controles compatíveis com os padrões exigidos, tanto antes da contratação quanto durante a vigência do contrato.

Nesse cenário, documentos como relatórios de conformidade (ex.: ISO/IEC 27001, PCI-DSS) ou auditorias realizadas por instituições qualificadas e confiáveis serão aceitos como alternativa, desde que proporcionem transparência suficiente para análise criteriosa das práticas do fornecedor.

6. SGSI e Comitê de Segurança da Informação

A Onfly mantém um Sistema de Gestão de Segurança da Informação (SGSI) estruturado com fundamento nos princípios estabelecidos pela norma ABNT NBR ISO/IEC 27001:2022, assegurando a proteção contínua das informações sob sua responsabilidade, inclusive aquelas compartilhadas com fornecedores, clientes e demais parceiros institucionais.

O SGSI contempla um conjunto abrangente de políticas, processos, controles técnicos e administrativos voltados à preservação da confidencialidade, integridade, disponibilidade e rastreabilidade das informações. Esse sistema é submetido a revisões regulares com vistas à manutenção de sua eficácia e conformidade com os requisitos legais, contratuais e regulatórios aplicáveis, em especial com a Lei Geral de Proteção de Dados Pessoais (LGPD). A presente política é parte integrante do SGSI e direciona as ações necessárias para atingir os objetivos determinados previamente.

A governança do SGSI é conduzida pelo setor de Cyber Security que fica responsável pela análise de riscos, proposição de melhorias e deliberação sobre incidentes relevantes.

Já o Comitê de Segurança da Informação, realiza o monitoramento de desempenho de fornecedores considerados críticos, assegurando a adoção de medidas corretivas frente a eventuais desvios identificados, alinhamento das decisões estratégicas em matéria de segurança da informação aos objetivos organizacionais e às expectativas das partes interessadas. Quando necessário, delibera sobre recomendações de aprimoramento de cláusulas contratuais, procedimentos operacionais e práticas de segurança adotadas por terceiros.

Esse modelo de governança tem como propósito promover a transparência, estimular a responsabilidade compartilhada e fortalecer relações de confiança entre todos os agentes que integram o ecossistema corporativo da Onfly.

7. Políticas Internas

Este material tem como objetivo apresentar, de forma transparente e acessível, um resumo das principais políticas internas da Onfly relacionadas à Segurança da Informação. É direcionado a todas as partes interessadas externas que, direta ou indiretamente, mantêm relacionamento com a empresa, incluindo clientes, fornecedores, parceiros comerciais e institucionais, além de demais stakeholders.

As diretrizes resumidas neste documento refletem o compromisso da Onfly com a proteção de dados, a integridade dos processos e o alinhamento contínuo às boas práticas e normas internacionais. Ao compartilhar

essas informações, reforçamos nosso propósito de garantir um ambiente de confiança mútua, responsabilidade e conformidade.

Espera-se que todas as partes interessadas compreendam e respeitem os princípios aqui descritos, contribuindo para a construção de relações sólidas e sustentáveis, pautadas pela segurança e pela transparência.

7.1 Política de Fornecedores

Estabelece critérios de avaliação, seleção e monitoramento de fornecedores, com foco em segurança da informação e privacidade. Os fornecedores devem firmar compromissos contratuais de confidencialidade, proteção de dados e cumprimento da LGPD.

Serão avaliados quanto à capacidade técnica, reputação e conformidade. A política exige cláusulas específicas para tratamento de dados e ações corretivas em caso de não conformidade. Incidentes devem ser reportados à Onfly, que se reserva o direito de auditar ou encerrar parcerias em caso de falhas críticas.

7.2 Política de Gestão de Acessos Privilegiados

Define diretrizes para o controle rigoroso de acessos administrativos e privilegiados. Todo acesso deve ser justificado, aprovado formalmente e monitorado continuamente. É proibido o compartilhamento de credenciais. Registros de atividades são mantidos para auditoria. O uso indevido de acessos pode gerar sanções. Fornecedores com acesso privilegiado devem cumprir os mesmos requisitos.

7.3 Política de Mesa e Tela Limpa

Prevê boas práticas para manter o ambiente de trabalho seguro, evitando exposição de informações confidenciais. Documentos sensíveis devem ser guardados após o uso e telas devem ser bloqueadas quando o usuário se ausentar.

Aplica-se tanto a ambientes físicos quanto ao trabalho remoto. Impressoras e mesas não devem conter papéis com dados pessoais ou confidenciais sem necessidade.

7.4 Política de Recrutamento e Seleção

Estabelece princípios para tratamento seguro e ético dos dados de candidatos. Informa que dados pessoais só são acessados por profissionais autorizados e são descartados ou anonimizados ao fim do processo. Fornecedores terceirizados de RH devem adotar práticas compatíveis com a LGPD e assinar termos de confidencialidade.

7.5 Política de Transferência de Dados

Regula como dados devem ser transferidos, interna e externamente, com base em criptografia e canais autorizados (ex: VPN, SFTP).

Transferências internacionais seguem os critérios da LGPD (Art. 33), com necessidade de consentimento, garantias contratuais ou autorização legal. Fornecedores devem garantir meios seguros, justificar a finalidade da transferência e manter a rastreabilidade.

7.6 Política de Hardening

Define requisitos técnicos mínimos de segurança para servidores, dispositivos e redes. Inclui desativação de serviços desnecessários, aplicação de patches de segurança e configuração de firewalls. Todos os ativos devem ser protegidos contra ataques conhecidos. Fornecedores devem manter seus sistemas em conformidade com esses padrões.

7.7 Política de Cookies

Informa sobre o uso de cookies no site e app da Onfly. Os cookies são utilizados para melhorar a experiência do usuário e fins analíticos, com base no consentimento do visitante. O usuário pode configurar suas preferências e revogar consentimento a qualquer momento. A coleta respeita a LGPD e apresenta transparência sobre os dados tratados.

7.8 Política de Descarte de Dados

Estabelece normas para eliminação segura de informações sensíveis em meios físicos ou digitais. Discos, pendrives e documentos impressos devem ser descartados por métodos que garantam a irrecuperabilidade (ex: trituração, wiping seguro). O descarte deve ser autorizado, rastreado e registrado, conforme exigido pela LGPD.

7.9 Política de SI em Serviços de Nuvem

Regula o uso seguro de serviços em nuvem, exigindo que provedores adotem medidas compatíveis com ISO/IEC 27001 e LGPD. Reforça uso de autenticação multifator, separação de ambientes (produção *x* homologação) e criptografia de dados em trânsito e repouso. A Onfly exige cláusulas contratuais específicas e pode auditar a conformidade com frequência.

7.10 Política de SLA

Define os níveis de serviço mínimos esperados de fornecedores e parceiros. Inclui indicadores como tempo de resposta, resolução de incidentes e disponibilidade. O não cumprimento pode gerar penalidades ou revisão contratual. Os fornecedores devem manter registros de SLA e comunicar imediatamente falhas críticas.

7.11 Política de Trabalho Remoto

Regula o trabalho remoto para colaboradores e terceiros. O uso de dispositivos pessoais é restrito, devendo-se preferir equipamentos corporativos com criptografia e antivírus.

Todo acesso deve ocorrer por VPN ou autenticação multifator. Redes públicas são proibidas ou devem ser validadas previamente pelo time de Cyber.

Todos os incidentes de segurança devem ser comunicados à área de Cyber Security, para o acionamento do Plano de Resposta a Incidentes de forma mais rápida possível.

7.12 Política de Gestão de Vulnerabilidades

Determina a execução periódica de varreduras de segurança com ferramentas como Nessus. As vulnerabilidades devem ser priorizadas e corrigidas conforme criticidade.

Todos os fornecedores devem reportar falhas relevantes e apresentar plano de mitigação. A Onfly acompanha os prazos e eficácia das correções aplicadas. Já os clientes devem entrar em contato com a Onfly o quanto antes ao perceber qualquer tipo de falha, através dos meios de contato disponibilizados via contrato.

7.13 Política de Gestão de Mudanças

Regula a implementação de mudanças em sistemas e infraestrutura. Toda alteração deve seguir um fluxo formal (GMUD), com análise de risco, aprovação e registro.

Mudanças emergenciais possuem tratamento especial, mas também devem ser documentadas. Fornecedores que realizam alterações devem seguir o mesmo processo.

7.14 Política de Continuidade de Negócio

Estabelece planos para manter os serviços essenciais operacionais em caso de falha ou desastre. Inclui:

- análise de impacto
- definição de processos críticos
- testes periódicos

Fornecedores estratégicos devem possuir plano de continuidade compatível e apoiar os processos de retomada da Onfly.

7.15 Política de Resposta a Incidentes

Define as etapas que devem ser seguidas em caso de incidente de segurança:

- identificação
- contenção
- erradicação
- recuperação
- lições aprendidas

Todos os incidentes devem ser registrados e analisados. Caso envolvam dados pessoais, é obrigatório acionar o DPO e, se necessário, a ANPD. Fornecedores devem notificar imediatamente a Onfly e colaborar com investigações e correções.

7.16 Política de Classificação da Informação

As informações são rotuladas conforme seu grau de sensibilidade

- Pública
- Interna
- Confidencial
- Restrita

Cada classificação define o nível de proteção, controle de acesso e forma de tratamento. Informações confidenciais ou secretas devem ser protegidas com criptografia e acesso restrito. O fornecedor que trata dados da Onfly deve respeitar essa classificação em todos os níveis.

7.17 Política de Desenvolvimento Seguro

Estabelece práticas obrigatórias para garantir a segurança no ciclo de desenvolvimento de software. Envolve:

- Análise de requisitos de segurança
- Uso de bibliotecas seguras
- Revisão de código
- Testes de vulnerabilidades
- Conformidade com OWASP

Fornecedores que prestam serviços de desenvolvimento devem seguir os mesmos critérios.

7.18 Política de Gestão de Acessos

Todos os acessos a sistemas e dados devem seguir o princípio do menor privilégio. O processo de concessão exige solicitação formal, aprovação e registro. Contas inativas são bloqueadas após 30 dias. A autenticação multifator (MFA) é obrigatória. Fornecedores devem garantir que seus colaboradores sigam os mesmos controles quando acessarem recursos da Onfly.

7.19 Política de Gestão de Riscos

Define o processo de identificação, análise, avaliação e tratamento de riscos. Cada risco tem um responsável e deve ser documentado em matriz de probabilidade × impacto. Ativos da informação são mapeados com riscos associados.

Fornecedores devem comunicar riscos identificados e colaborar na mitigação de impactos que possam afetar a Onfly.

7.20 Política de Inventário e Uso de Ativos

Todos os ativos (físicos, lógicos, sistemas, informações) devem estar catalogados com responsável e classificação. O uso deve ser feito de forma adequada, com controles de acesso e proteção.

Fornecedores que manipulam ou têm posse de ativos da Onfly devem garantir rastreabilidade, segurança e devolução ao término do contrato.

8. Requisitos legais, Contratuais e Propriedade Intelectual

Os fornecedores contratados e/ou clientes devem permitir à Onfly o monitoramento contínuo do desempenho dos serviços prestados, assegurando a transparência, rastreabilidade e conformidade com os indicadores acordados.

É responsabilidade dos fornecedores, clientes, e colaboradores da Onfly garantir que suas atividades não violem direitos de terceiros, incluindo, mas não se limitando a, direitos autorais, marcas registradas, licenças de uso ou patentes, devendo atuar sempre em conformidade com a legislação vigente e as diretrizes contratuais estabelecidas.

9. Compromisso da Alta Direção

A alta direção da Onfly reafirma seu compromisso em proteger as informações sob sua responsabilidade e em prover os recursos, liderança e apoio necessários para implementar, manter e melhorar continuamente o Sistema de Gestão de Segurança da Informação (SGSI), em conformidade com a norma ABNT NBR ISO/IEC 27001:2022, com a LGPD (Lei 13.709/2018) e demais requisitos legais, regulatórios e contratuais aplicáveis.

Esta política se aplica integralmente a todas as partes interessadas internas e externas e é pilar fundamental para a preservação da confidencialidade, integridade, disponibilidade e rastreabilidade das informações.

10. Documentos de Referência

- NORMA ABNT NBR ISO 27001:2022
- Acordo de Confidencialidade
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)
- Contrato de prestação de serviços