

5. POLÍTICA DE GESTÃO DE PATCHES E ATUALIZAÇÕES

1. OBJETIVO

Esta política tem como finalidade garantir que todos os **dispositivos, sistemas operacionais, aplicativos e softwares utilizados pela empresa Simone Yagui** estejam devidamente atualizados, com **patches de segurança aplicados em tempo hábil**, reduzindo vulnerabilidades que possam comprometer a integridade, confidencialidade ou disponibilidade dos dados pessoais e sensíveis tratados, em conformidade com a LGPD.

2. ABRANGÊNCIA

Aplica-se a todos os dispositivos, programas e plataformas utilizados pela empresa, incluindo:

- Notebooks e celulares da titular e colaboradores;
 - Sistemas de gestão e loja virtual;
 - Aplicativos de comunicação (WhatsApp Business, e-mail, redes sociais);
 - Navegadores de internet e sistemas operacionais (Windows, Android, iOS).
-

3. PRINCÍPIOS NORTEADORES

- **Segurança preventiva:** prevenir falhas de segurança por meio da atualização contínua dos sistemas;
 - **Conformidade legal:** atender às obrigações da LGPD, que exige medidas técnicas para proteger os dados;
 - **Responsabilidade compartilhada:** todos os envolvidos na operação devem colaborar com a segurança digital da empresa.
-

4. RESPONSABILIDADES

4.1. Da Titular / Encarregada de Dados (Simone Yagui):

- Garantir a implementação desta política e supervisionar seu cumprimento;
- Verificar semanalmente a existência de atualizações nos dispositivos e softwares principais da empresa;
- Realizar ou orientar a aplicação de patches de segurança em sistemas de gestão, loja virtual, e-mails e nuvens;

- Registrar, em planilha interna, os ciclos de atualização e correções aplicadas;
- Manter cópias de segurança antes de atualizações críticas.

4.2. Dos Colaboradores:

- Manter seus dispositivos de trabalho (celulares, notebooks) **atualizados com as versões mais recentes dos sistemas operacionais**;
- Atualizar **manualmente** aplicativos utilizados nas funções da empresa, caso não haja atualização automática;
- Aplicar, assim que notificados, **patches de segurança** de softwares como antivírus, navegador, aplicativos de mensagens e redes sociais;
- **Comunicar imediatamente à titular** caso surjam falhas, travamentos, alertas de segurança ou erros após atualizações;
- Não utilizar softwares desatualizados, piratas, sem suporte ou de procedência duvidosa;
- Seguir todas as instruções fornecidas pela titular sobre atualizações obrigatórias e configurações de segurança.

5. DIRETRIZES DE ATUALIZAÇÃO

5.1. Atualizações automáticas

- Sempre que possível, devem ser ativadas nos dispositivos e aplicativos utilizados, especialmente:
 - Sistemas operacionais (Android, iOS, Windows);
 - WhatsApp Business, e-mail, antivírus, navegador e ferramentas de backup.

5.2. Verificações manuais

- A titular realizará **verificação semanal** de atualizações pendentes nos sistemas utilizados profissionalmente;
- Os colaboradores devem realizar verificação em seus dispositivos pessoais utilizados no trabalho, no mínimo **quinzenalmente**.

5.3. Aplicação de patches críticos

- Sempre que identificados patches de segurança classificados como **críticos**, a aplicação deve ser **imediate**;
- A titular poderá suspender temporariamente o uso de sistemas ou dispositivos que estejam vulneráveis, até a atualização ser concluída.

6. PROCEDIMENTOS DE RESTAURAÇÃO

- Antes de atualizações críticas, recomenda-se a realização de **backup local ou em nuvem** dos arquivos e dados relevantes;
- Em caso de falha após uma atualização, o dispositivo deverá ser restaurado para a versão anterior ou encaminhado à assistência confiável;
- A titular avaliará, caso necessário, a suspensão do uso de um sistema até que sua estabilidade e segurança estejam restabelecidas.

7. MONITORAMENTO E REGISTRO

- A empresa manterá um **registro mensal simples** contendo:
 - Nome do dispositivo;
 - Data da verificação de atualização;
 - Aplicações atualizadas;
 - Incidentes ou anomalias observadas;
- O registro poderá ser feito em planilha interna e revisado periodicamente.

8. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

- Esta política será revisada **anualmente** ou sempre que houver alteração significativa na infraestrutura tecnológica, sistemas utilizados ou nas exigências legais;
- A titular poderá emitir instruções complementares em casos específicos, como mudanças de plataforma, aquisição de novos dispositivos ou expansão de atividades.

9. DISPOSIÇÕES FINAIS

O cumprimento desta política é **obrigatório por todos os colaboradores** que tenham acesso a dados ou sistemas da empresa. O uso de softwares ou dispositivos desatualizados representa risco direto à segurança da informação e poderá acarretar responsabilização conforme os termos do Acordo de Confidencialidade, das políticas internas da empresa e da LGPD.

E, por estarem de pleno acordo, firmam o presente instrumento .

Campina Grande – PB, ____ de _____ de 2025.

Simone Yagui

Titular e Encarregada de Dados

[Nome do(a) Colaborador(a)]

CPF: [preencher]