1. POLÍTICA DE GESTÃO DE PATCHES E ATUALIZAÇÕES

1. Objetivo

Esta política tem como objetivo estabelecer diretrizes para a gestão regular de patches e atualizações de software nos sistemas de informação da empresa, visando proteger os dados pessoais conforme as exigências da Lei Geral de Proteção de Dados (LGPD).

2. Escopo

Aplica-se a todos os colaboradores, prestadores de serviços e parceiros que utilizam ou gerenciam os sistemas de informação da empresa, incluindo computadores, dispositivos móveis, servidores e redes.

3. Responsabilidades

- TI e Consultoria: Responsáveis pela implementação de patches e atualizações, monitoramento de sistemas, e condução de testes e auditorias de segurança, bem como assegurar que as práticas de gestão de patches estão em conformidade com a LGPD e outras regulamentações pertinentes.
- Gerência: Aprovar a política e assegurar recursos suficientes para sua implementação.
- Colaboradores: Cumprir com a política e participar dos treinamentos requeridos.

4. Diretrizes para Gestão de Patches

- Identificação e Avaliação: Regularmente, verificar atualizações disponíveis e avaliar a criticidade dos patches utilizando fontes confiáveis e comunicados dos fabricantes de software.
- Priorização de Patches: Patches críticos de segurança devem ser tratados como prioridade para mitigar riscos associados a vulnerabilidades que podem afetar a proteção de dados pessoais.
- Testes Antes da Implementação: Implementar patches em um ambiente de teste para verificar compatibilidade e funcionalidade antes do lançamento em ambiente de produção.
- Programação de Patches: Patches devem ser aplicados fora do horário de pico para minimizar o impacto nas operações da empresa, sempre que possível.

5. Diretrizes para Atualizações de Software

- Monitoramento Contínuo: Manter-se atualizado sobre as últimas versões de software e as recomendações dos fabricantes para atualizações.
- Validação e Licenciamento: Garantir que todas as atualizações de software estejam em conformidade com as licenças de uso e sejam obtidas de fontes oficiais e seguras.
- Documentação: Manter registros detalhados de todas as atualizações e patches aplicados, incluindo datas, detalhes técnicos e resultados dos testes.

6. Treinamento e Conscientização

- Treinamento Regular: Realizar treinamentos regulares para as equipes de TI e todos os usuários sobre a importância da atualização de software e as práticas seguras de gestão de patches.

- Comunicação de Políticas: Disseminar esta política em toda a organização e garantir que todos os colaboradores estejam cientes de suas responsabilidades.

7. Auditoria e Conformidade

- Auditorias Regulares: Realizar auditorias regulares para assegurar a conformidade com esta política e identificar oportunidades de melhoria.
- Relatórios de Conformidade: Preparar relatórios periódicos sobre o status das atualizações e patches para revisão da gerência e auditorias externas, conforme necessário.

8. Revisão e Atualização da Política

- Revisões Periódicas: Esta política deve ser revisada anualmente ou conforme necessário para refletir mudanças nas tecnologias, práticas de negócios e requisitos legais.

9. Aplicação da Política

O não cumprimento desta política pode resultar em ações disciplinares, incluindo advertência, suspensão ou rescisão do contrato de trabalho, bem como possíveis sanções legais devido à não conformidade com a LGPD.