Política de Segurança Digital

Ágila Tecnologia da Informação Ltda

Maio de 2024

Ágila
Soluções em Gestão

1 Introdução

A Ágila Tecnologia da Informação compromete-se com a proteção de informações sensíveis, confidenciais e pessoais, conforme os requisitos da Lei Geral de Proteção de Dados (LGPD). Esta política abrange a gestão de vulnerabilidades, gestão de incidentes, classificação de informação, descarte de informação e segurança da informação.

2 Objetivo

Estabelecer diretrizes para garantir a segurança e integridade das informações, protegendo-as contra acessos não autorizados, alterações, destruição ou divulgação indevida.

3 Âmbito

Esta política aplica-se a todos os colaboradores, prestadores de serviços, parceiros e quaisquer outras partes que tenham acesso às informações da Ágila Tecnologia da Informação.

4 Gestão de Vulnerabilidades

4.1 Identificação e Avaliação

- Realizar varreduras periódicas para identificar vulnerabilidades em sistemas e aplicativos.
- Avaliar a criticidade das vulnerabilidades identificadas com base no impacto potencial e probabilidade de exploração.

4.2 Tratamento

- Priorizar a correção das vulnerabilidades de acordo com sua criticidade.
- Aplicar patches e atualizações em tempo hábil para corrigir as vulnerabilidades.
- Documentar todas as ações de mitigação realizadas.

4.3 Monitoramento

- Monitorar continuamente os sistemas para novas vulnerabilidades e ameaças.
- Revisar regularmente a eficácia das medidas de mitigação implementadas.

5 Gestão de Incidentes

5.1 Identificação e Relato

Estabelecer canais claros para relato de incidentes de segurança da informação.

Treinar colaboradores para reconhecer e relatar incidentes de forma imediata.

5.2 Resposta

Designar uma equipe de resposta a incidentes com responsabilidades claras.

Implementar procedimentos de resposta rápida para conter e mitigar os impactos dos incidentes.

5.3 Investigação e Análise

- Conduzir investigações detalhadas para identificar a causa raiz dos incidentes.
- Documentar todos os achados e as ações tomadas durante a investigação.

5.4 Comunicação

- Notificar as partes interessadas relevantes, incluindo autoridades competentes, conforme exigido pela LGPD.
- Informar os titulares dos dados afetados sobre o incidente e as medidas tomadas para mitigar os impactos.

5.5 Melhoria Contínua

- Revisar os incidentes para identificar oportunidades de melhoria nos processos de segurança.
- Atualizar procedimentos e políticas conforme necessário para prevenir futuros incidentes.

6 Política de Classificação de Informação

6.1 Classificação

- Classificar informações com base na sensibilidade e no impacto potencial em caso de divulgação ou comprometimento:
    - **Pública:** Informações que podem ser divulgadas sem restrições.
    - **Interna:** Informações que devem ser protegidas, mas cujo impacto de divulgação é limitado.
    - **Confidencial:** Informações sensíveis que exigem proteção rigorosa.
    - **Secreta:** Informações extremamente sensíveis que, se divulgadas, podem causar danos severos à empresa ou aos indivíduos.

6.2 Proteção

- Aplicar controles de segurança adequados com base na classificação da informação.
- Garantir que o acesso às informações seja restrito conforme necessário.

7 Política de Descarte de Informação

7.1 Identificação

- Identificar regularmente informações que não são mais necessárias para operações ou requisitos legais.

7.2 Métodos de Descarte

- Utilizar métodos seguros para descarte de informações, como destruição física de documentos e apagamento seguro de dados eletrônicos.
- Assegurar que todos os descartes sejam irreversíveis e não permitam a recuperação de dados.

7.3 Conformidade

- Garantir que o descarte de informações esteja em conformidade com a LGPD e outras regulamentações aplicáveis.

8 Segurança da Informação

8.1 Acesso e Controle

- Implementar controles de acesso baseados em função (RBAC) para garantir que apenas pessoas autorizadas possam acessar informações sensíveis.
- Utilizar autenticação multifator (MFA) para acesso a sistemas críticos.

8.2 Treinamento e Conscientização

- Realizar programas de treinamento regulares para todos os colaboradores sobre práticas de segurança da informação e conformidade com a LGPD.
- Promover uma cultura de segurança da informação dentro da organização.

8.3 Auditoria e Conformidade

- Conduzir auditorias internas regulares para garantir conformidade com esta política e com a LGPD.
- Manter registros detalhados de todas as atividades de segurança e conformidade.

8.4 Proteção de Dados Pessoais

- Garantir que o processamento de dados pessoais esteja em conformidade com os princípios da LGPD, incluindo transparência, finalidade, necessidade e segurança.
- Implementar medidas técnicas e administrativas para proteger dados pessoais contra acesso não autorizado, perda, alteração ou destruição.

9 Revisão da Política

- Esta política será revisada anualmente ou sempre que houver mudanças significativas na legislação ou nos processos da empresa.
- Todas as revisões devem ser aprovadas pela alta administração da Ágila Tecnologia da Informação.

10 Consequências do Não Cumprimento

- O não cumprimento desta política pode resultar em ações disciplinares, incluindo demissão, além de possíveis ações legais conforme permitido pela legislação aplicável.

11 Aprovação

- Esta política foi aprovada pela diretoria da Ágila Tecnologia da Informação em 24 de maio de 2024 e entra em vigor na data de sua publicação.