toga.digital

Checklist de segurança da informação

Biblioteca de materiais para advogados e escritórios de advocacia

Material original: Autoridade Nacional de Proteção de Dados (ANPD)

A publicação institucional a seguir é reproduzida sem alterações. O Toga Digital atua apenas como organizador desta cópia de consulta e não é autor nem possui endosso da instituição responsável.

Verifique a vigência das orientações antes de aplicá-las. A disponibilização pública desta versão deve observar as permissões de reprodução da fonte.

ANPD
Autoridade Nacional de Proteção de Dados

CHECKLIST DE MEDIDAS DE SEGURANÇA PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



- [ ] Estabelecer uma política de segurança da informação simplificada, que estabeleça controles relacionados ao tratamento de dados pessoais, como cópias de segurança, uso de senhas, acesso à informação, compartilhamento de dados, atualização de softwares, uso de correio eletrônico e uso de antivírus.

- [ ] Realizar revisões periódicas da política de segurança da informação.

- [ ] Gerenciar contratos e aquisições com observância ao tratamento adequado dos dados pessoais.

CONSCIENTIZAÇÃO E TREINAMENTO



- [ ] Realizar a conscientização dos funcionários, via treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD e normas da ANPD.

- [ ] Informar e sensibilizar todos os funcionários da organização, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD.

CONSCIENTIZAÇÃO E TREINAMENTO



Informar os funcionários sobre:

- como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário; ☐
- como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail; ☐
- manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas; ☐
- não compartilhar logins e senhas de acesso das estações de trabalho; ☐
- bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros; ☐
- seguir as orientações da política de segurança da informação. ☐

Criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas. ☐

GERENCIAMENTO DE CONTRATOS



Estabelecer contratos com cláusulas de segurança da informação que assegurem a proteção de dados pessoais, tais como:

- regras para fornecedores e parceiros; ☐
- regras sobre compartilhamentos; ☐
- relações entre controlador-operador; ☐
- orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador. ☐

Assinar termos de confidencialidade (non-disclosure agreement - NDA) com os funcionários da empresa. ☐

CONTROLE DE ACESSO



- [ ] Implementar um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais.

- [ ] Configurar funcionalidades no sistema de controle de acesso que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade.

- [ ] Implementar um adequado gerenciamento de senhas, estabelecendo controles tais como:
    - [ ] evitar o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos;
    - [ ] utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos;
    - [ ] não reutilizar senhas.

- [ ] Proibir o compartilhamento de contas ou de senhas entre funcionários.

- [ ] Aplicar o princípio do menor privilégio (need to know).

- [ ] Utilizar a autenticação multi-fator para acessar sistemas ou base de dados que contenham dados pessoais.

- [ ] Implementar um sistema de controle de acesso aplicável a todos os usuários que acessam o sistema de TI (caso o agente de tratamento possua rede interna de computadores).

SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

- [ ] Coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados.
- [ ] Implementar soluções de pseudonimização, como a criptografia, para cifrar dados pessoais.
- [ ] Orientar os funcionários para não desativar ou ignorar as configurações de segurança de estações de trabalho.
- [ ] Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos.
- [ ] Inventariar e cifrar dados de dispositivos externos e armazena-los em locais seguros.
- [ ] Realizar backups offline, periódicos e armazená-los de forma segura.
- [ ] Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las, ou, quando não for possível a sobrescrita, destruir as mídias físicas.
- [ ] Estabelecer no contrato de serviço o registro da destruição/descarte (caso o agente de tratamento utilize serviços de terceiros para o descarte).

SEGURANÇA DAS COMUNICAÇÕES



- [ ] Utilizar conexões cifradas *(TLS/HTTPS)* ou aplicativos com criptografia fim- a-fim para serviços de comunicação.
- [ ] Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall *(WAF – Filtro de Aplicação)*.
- [ ] Proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e, integrar o antivírus ao sistema de e-mail.
- [ ] Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.

GERENCIAMENTO DE VULNERABILIDADES



- [ ] Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores).
- [ ] Adotar e atualizar periodicamente softwares antivírus e antimalwares.
- [ ] Realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.

DISPOSITIVOS MÓVEIS



- [ ] Utilizar técnicas de autenticação multi-fator para controle de acesso de dispositivos móveis – como smartphones e laptops.
- [ ] Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível.
- [ ] Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

SERVIÇOS EM NUVEM



- [ ] Realizar um contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados.
- [ ] Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende os demais requisitos de segurança da informação estabelecidos.
- [ ] Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado.
- [ ] Utilizar técnicas de autenticação multi-fator para acesso aos serviços em nuvem relacionados a dados pessoais.