Orientação Técnica:

MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

MEDIDAS ADMINISTRATIVAS

1 - Política de segurança da informação

Contempla simples 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; uso de antivírus, entre outros.

2 - Conscientização e Treinamento

Essa conscientização implica informar e sensibilizar todos os servidores, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD. Algumas informações úteis que podem ser passadas aos funcionários são:

• 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;

• bloquear os computadores quando se afastar do local de trabalho para evitar o acesso indevido de terceiros;

• seguir as orientações da política de segurança da informação.

3 - Gerenciamento de contratos

a) É recomendável que termos de confidencialidade sejam assinados com as empresas prestadoras de serviço, para que estes se comprometam a não divulgar informações confidenciais que envolvam dados pessoais;

b) É indicado que seja realizado o gerenciamento de contratos e aquisições, para atenção à distribuição de funções e responsabilidades entre as partes, com observância à LGPD e ao tratamento adequado dos dados pessoais;

c) No caso de agentes de tratamento terceirizados de serviços de TI, recomenda-se que estabeleçam com os fornecedores contratos que incluam, dentre outras, cláusulas de segurança da informação que assegurem a adequada proteção de dados pessoais.

d) Tais instrumentos poderão conter, por exemplo, cláusulas que tratam de:

• 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.

MEDIDAS TÉCNICAS

1 - Controle de acesso

a) O controle de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele consiste em processos:

• autenticação: identifica quem acessa o sistema ou os dados;

• autorização: determina o que o usuário identificado pode fazer;

• auditoria: registra o que foi feito pelo usuário.

Obs.: Sobre esse aspecto sugerimos que, caso possua rede interna de computadores, seja implementado um sistema de controle de acesso aplicável a todos os usuários, com vários níveis de permissão, necessidade de trabalhar com o sistema e de acessar dados pessoais.

b) Sugerimos que o sistema de controle de acesso seja configurado com funcionalidades que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade. Isso significa que é importante que o sistema possa estabelecer o número de caracteres para se criar uma senha e definir se é necessário o uso de um caractere especial.

c) É importante, ainda, na implementação de sistemas de segurança, utilizar um adequado gerenciamento de senhas, evitando o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos, tendo em vista que geralmente os atacantes utilizam estas senhas padronizadas para tentativas de conexão e realizar os seus ataques. As senhas precisam ser alteradas por outras com requisitos mais seguros.

d) Outra medida sugerida é que os agentes de tratamento não permitam o compartilhamento de contas ou de senhas entre servidores, visto que isso é um vetor crítico de vulnerabilidade de segurança da informação.

e) Os usuários de um sistema terão somente o nível de acesso necessário para a realização de suas atividades. Funções de alta complexidade, tais como as de administrador de sistema, devem ser restringidas apenas àqueles funcionários que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade.

Obs.: importante mencionar que a melhora de processos de identificação e autenticação em serviços e sistemas, incluindo a não reutilização de senhas, estão entre as três medidas de maior impacto na segurança da informação.

f) Por fim, sugere-se que os agentes considerem utilizar a autenticação multi-fatores para acessar sistemas ou base de dados que contenham dados pessoais. Essa autenticação consiste em estabelecer uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de

autenticação. Exemplo: podemos citar o envio de códigos de segurança por SMS ou por e-mail e o uso de aplicativos autenticadores ou tokens de segurança.

SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

a) Inicialmente, cabe salientar que, muitas vezes, os agentes de tratamento coletam mais dados do que o necessário para a realização de suas atividades ou para uma finalidade específica.

Para se evitar riscos de incidentes de segurança e outros comprometimentos, e em atenção ao princípio da necessidade previsto no art. 6º, III, da LGPD, os agentes de tratamento devem coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida.

No contexto atual da LGPD, tratar (coletar e guardar, por exemplo) dados pessoais sem uma utilidade imediata e concreta, apenas porque um dia poderão ser úteis (sem se saber exatamente para quê), não é uma prática adequada, considerando os princípios da finalidade e da necessidade previstos na referida Lei.

b) Além disso, tendo em vista que os dados pessoais sensíveis gozam de uma proteção especial pela LGPD, sugere-se que os agentes de tratamento que armazenam dados dessa natureza implementem soluções que dificultem a identificação do titular, como as técnicas de pseudonimização. Ex. Brasileiro, masculino, meia idade.

c) Em relação a locais de trabalho, sugere-se que seja orientado aos servidores a importância das configurações de segurança, a fim de que eles não as desativem ou ignorem, inclusive quanto a restrições de acesso de determinados tipos de sites.

d) Evitar a transferência de dados pessoais de locais de trabalho para dispositivos de armazenamento externo, como pendrives ou discos rígidos externos, tendo em vista o risco de se perder a guarda dos dados pessoais transferidos. Caso essa operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como cifrar os dados com senha.

e) Em relação às cópias de segurança (backups) é importante que elas sejam realizadas regularmente de forma completa e armazenadas em locais seguros e distintos (nuvem) dos dispositivos de armazenamento principais. Também é importante que essas cópias não sejam sincronizadas online (em tempo real), para evitar a perda de dados em casos de infecções por códigos maliciosos que sequestram os dados (ransomware).

f) Por fim, sobre a eliminação de dados pessoais, sugere-se que em todas as mídias que contenham dados pessoais seja executado o método de formatar antes de descartá-las. Quando isso não for possível, como em CDs e DVDs, sugere-se que seja realizada a destruição física da mídia – o que também se aplica para destruição de papel e de mídia portátil para armazenar dados pessoais.

Além disso, para os agentes que fazem uso de serviço de terceiros para o descarte, seja de mídia ou registro de papel, sugere-se que seja estabelecido um contrato de serviço com cláusulas de registro da destruição que for realizada.

SEGURANÇA DAS COMUNICAÇÕES

As comunicações são um importante ponto relacionado à segurança de dados pessoais, tendo em vista a possibilidade da existência de vulnerabilidades no processo de transmissão de dados ou informações.

Por exemplo, aplicativos de mensagens podem comprometer a segurança de qualquer negócio se houver troca de links maliciosos ou se o usuário receber algum arquivo infectado.

a) Destaca-se a relevância de se utilizar conexões cifradas (senha) ou aplicativos com criptografia fim a fim. Isso se aplica também ao uso de e-mails, por exemplo, para envio de informações de servidores, como salários, ou de prontuários. Nesses casos, sugere-se que os e-mails sejam cifrados ou, opcionalmente, que os arquivos sejam cifrados para envio.

b) Além disso, sugere-se que o tráfego de rede seja gerenciado. Algumas formas de fazer isso, são:

• instalar e manter um sistema de firewall, que monitore, detecte e bloqueie ameaças, impedindo conexões a redes não confiáveis. Caso serviços web sejam utilizados, sugere-se o uso de firewalls de aplicação web.

• Proteger serviços de e-mail, utilizando antivírus integrados, ferramentas anti-spam e filtros de e-mail;

c) Outro cuidado importante é remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas, por exemplo, o site do município.

MANUTENÇÃO DE PROGRAMA DE GERENCIAMENTO DE VULNERABILIDADES

a) Em relação a uso de um programa de gerenciamento de vulnerabilidades, muito importante o monitoramento da existência de novas versões e correções disponíveis em todos os sistemas e aplicativos. Nesse sentido, é também relevante manter todos os sistemas e aplicativos em suas últimas versões, bem como instalar todas as correções de segurança disponíveis lançadas pelo desenvolvedor do sistema operacional e aplicativos.

b) A adoção e atualização de softwares antivírus ou antimalwares, que detectam, impedem e atuam na remoção de programas maliciosos, como vírus. Diante disso, sugere-se que os agentes de tratamento implementem antivírus em seus sistemas, em especial em computadores e laptops.

Obs.: é importante que esses mecanismos sejam mantidos funcionando ativamente e atualizados e que realizem varreduras periódicas nos dispositivos, bem como que não possam ser desativados ou alterados pelos usuários.

GRUPO PÚBLICA

MEDIDAS RELACIONADAS AO USO DE DISPOSITIVOS MÓVEIS

a) Em relação aos dispositivos móveis, como smartphones e laptops, caso seu uso seja necessário para fins institucionais, sugere-se que estejam sujeitos aos mesmos procedimentos de controle de acesso que os outros equipamentos de TI, além de serem guardados em locais seguros quando não estiverem em uso.

b) Quando possível separem os dispositivos móveis de uso privado daqueles de uso institucional. Dispositivos móveis de uso privado estão sujeitos a mais vulnerabilidades, pelo uso de aplicativos potencialmente inseguros para fins pessoais. Já em dispositivos para uso exclusivamente institucional, pode-se ter mais gerenciamento no acesso e nos aplicativos utilizados.

Obs.: Caso não seja possível implementar medidas de segurança equivalentes às do Município, recomenda-se que dispositivos móveis pessoais não sejam utilizados para fins institucionais.

c) Tendo em vista que dispositivos móveis podem ser comprometidos mais facilmente em eventual perda ou roubo, e que isso pode colocar em risco a guarda dos dados pessoais, sugere-se também que os agentes avaliem e implementem funcionalidades que permitam apagar remotamente os dados pessoais relacionados à sua atividade de processamento. Isso poderá diminuir a chance de eventual incidente de segurança com dados pessoais. As medidas sugeridas valem tanto para dispositivos móveis de propriedade institucional quanto os pessoais.

MEDIDAS RELACIONADAS AO SERVIÇO EM NUVEM

Serviço em nuvem é o fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, pela Internet (nuvem).

a) E esperado que essas empresas fornecedoras observem e implementem as recomendações internacionais e as boas práticas de segurança da informação.

b) Com relação à prestação de serviços de computação em nuvem, sugere-se que o agente de tratamento realize um contrato de acordo de nível de serviço, contemplando a segurança dos dados armazenados.

c) A partir dos requisitos de segurança da informação definidos pelo agente de tratamento, sugere-se que seja avaliado se o serviço oferecido pelo provedor do serviço em nuvem atende os requisitos estabelecidos.

d) Por fim, sugere-se que sejam especificados os requisitos para o acesso do usuário a cada serviço em nuvem utilizado, bem como que sejam usadas técnicas de autenticação multi fator, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

GRUPO PÚBLICA

DICAS PARA INICIAR UMA ESTRUTURA DE SEGURANÇA DA INFORMAÇÃO:

1 - Controle de acesso (login e senha). Acessos disponíveis apenas para os funcionários que realmente precisam acessá-los.

2 - Política de senhas fortes, criá-las e alterá-las sempre que necessário.

3 - Políticas de uso da internet/Intranet/extranet. Deixar claro o que é e não é permitido acessar e quais arquivos podem ser baixados nos computadores. Essas diretrizes devem ser divulgadas para toda a equipe e reforçadas periodicamente.

4 - Cuidados mínimos devem ser tomados no momento de navegar pela internet e principalmente na hora de abrir arquivos duvidosos via e-mail, sites ou redes sociais. Neste momento é que a maioria dos vírus maliciosos são aceitos.

5 - Desativação reprodução automática de dispositivos.

6 - Contratação de Firewall e manter sempre atualizados.

7 - Antivírus em todas as máquinas para realizar análises de vulnerabilidade periódicas e identificar arquivos suspeitos.

8 - Atualizações de versão dos sistemas operacionais. Sistemas desatualizados estão mais propensos aos ataques cibernéticos e facilitam a entrada de vírus e hackers.

9 - Avaliação de riscos, a fim de examinar quais ferramentas e departamentos estão mais suscetíveis a ameaças e danos.

10 - Identificar as principais vulnerabilidades presentes em seus sistemas internos, traçando estratégias para reduzir os potenciais riscos e fortalecer a segurança de dados. Ex: Uso de Scan de vulnerabilidades

11 - SEGURANÇA DE PROCESSOS:

- 11.1 - Implantar assinatura digital;
- 11.2 - Estratégia de criptografia;
- 11.3 - Estratégia de backup, Migração de servidores para a nuvem.