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 servidores e usuários são:

a) como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;

b) 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;

c) manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;

d) não compartilhar logins e senhas;

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

f) seguir as orientações da política de segurança da informação.

3) Gerenciamento de contratos

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;

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;

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.

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

a) Regras para fornecedores e parceiros;

b) regras sobre compartilhamentos;

c) relações entre controlador-operador;

d) orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador.

MEDIDAS TÉCNICAS

1) Controle de acesso

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

a) autenticação: identifica quem acessa o sistema ou os dados;

b) autorização: determina o que o usuário identificado pode fazer;

c) auditoria: registra o que foi feito pelo usuário.

RECOMENDAÇÕES TÉCNICAS PARA CONTROLE DE ACESSO E AUTENTICAÇÃO

Para assegurar a confidencialidade, integridade e disponibilidade dos ativos de informação e dos dados pessoais tratados, em conformidade com as melhores práticas de segurança e os requisitos da Lei Geral de Proteção de Dados (LGPD), recomenda-se a implementação das seguintes medidas técnicas e organizacionais:

1. Política de Controle de Acesso Lógico

Sugere-se a implementação de um sistema de Controle de Acesso Baseado em Função (RBAC - *Role-Based Access Control*) para a rede corporativa e todos os sistemas de informação. Este controle deve garantir que:

- **Princípio do Menor Privilégio (*Least Privilege*):** Cada usuário terá acesso apenas aos dados e funcionalidades estritamente necessários para o desempenho de suas atribuições. As permissões devem ser concedidas com base na necessidade de conhecimento (*need-to-know*).
- **Segregação de Funções:** Perfis de acesso com privilégios elevados, como os de administrador de sistema, devem ser severamente restringidos, monitorados e atribuídos somente a colaboradores cuja função exija tal nível de acesso e que possuam a capacitação técnica necessária.

2. Gestão de Credenciais e Política de Senhas

Uma gestão de credenciais robusta é um dos pilares da segurança da informação. Recomenda-se:

- **Implementação de Política de Senhas Fortes:** O sistema deve forçar a criação de senhas que atendam a critérios mínimos de complexidade, como comprimento, e a obrigatoriedade do uso de diferentes conjuntos de caracteres (letras maiúsculas, minúsculas, números e símbolos especiais).
- **Eliminação de Credenciais Padrão:** É mandatório estabelecer um procedimento para a alteração imediata de todas as senhas padrão de fábrica de qualquer software ou hardware adquirido. A utilização dessas credenciais representa um vetor de ataque crítico e de alto risco.
- **Vedação ao Compartilhamento de Contas:** Deve ser expressamente proibido o compartilhamento de contas de usuário ou senhas. Cada agente de tratamento deve possuir uma credencial de acesso única, pessoal e intransferível, a fim de garantir a rastreabilidade e a responsabilização individual pelas ações realizadas no sistema.

3. Autenticação Multifator (MFA)

Recomenda-se enfaticamente a adoção da Autenticação Multifator como camada adicional de segurança para o processo de login, especialmente para o acesso a sistemas, bases de dados ou serviços remotos que contenham dados pessoais. A MFA exige que o

usuário forneça ao menos duas formas distintas de comprovação de identidade (fatores de autenticação), como:

- Algo que o usuário sabe (a senha).
- Algo que o usuário possui (um código gerado por aplicativo autenticador, token físico ou recebido por SMS).

A implementação de processos robustos de identificação e autenticação, incluindo a não reutilização de senhas e a adoção de MFA, figura entre as medidas de maior impacto para a mitigação de riscos e o fortalecimento da segurança da informação da organização.

DIRETRIZES DE SEGURANÇA PARA O ARMAZENAMENTO E TRATAMENTO DE DADOS PESSOAIS

1. Minimização de Dados e Aderência ao Princípio da Necessidade

É fundamental ressaltar que a coleta e o armazenamento de dados pessoais devem ser estritamente limitados ao que é essencial para o cumprimento de finalidades específicas, legítimas e informadas ao titular. Em atenção ao **princípio da necessidade**, previsto no Art. 6º, III, da LGPD, os agentes de tratamento devem abster-se de coletar volumes de dados superiores ao necessário para os objetivos pretendidos.

A prática de coletar e reter dados pessoais sem uma utilidade imediata e concreta, sob a justificativa de uma possível utilização futura e indeterminada, é incompatível com os princípios da finalidade e da necessidade. Tal conduta amplia desnecessariamente a superfície de risco e a responsabilidade do controlador em caso de incidentes de segurança.

2. Proteção de Dados Pessoais Sensíveis

Os dados pessoais sensíveis, por sua natureza, recebem proteção especial da LGPD e exigem a implementação de medidas de segurança reforçadas. Recomenda-se fortemente que, sempre que possível, os agentes de tratamento apliquem técnicas que dificultem a associação direta dos dados ao titular, como a **pseudonimização**.

A pseudonimização é um tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente seguro e controlado. Essa técnica é uma medida de segurança eficaz para mitigar os riscos associados ao tratamento de dados sensíveis.

3. Medidas de Segurança no Ambiente de Trabalho

A segurança da informação é uma responsabilidade compartilhada, e a conscientização dos colaboradores é um componente crítico para a proteção dos dados.

- **Segurança da Estação de Trabalho:** Os servidores e colaboradores devem ser orientados a manter ativas todas as configurações de segurança de suas estações de trabalho, incluindo firewalls, antivírus e restrições de acesso a sítios eletrônicos não autorizados. A desativação ou a não observância dessas configurações representa uma vulnerabilidade significativa.
- **Controle de Dispositivos de Armazenamento Removível:** A transferência de dados pessoais para dispositivos de armazenamento externo (ex: *pen drives*, HDs externos) deve ser evitada como regra, pois aumenta exponencialmente o risco de perda, furto e acesso não autorizado. Caso a transferência seja imprescindível para a atividade, a operação deve ser formalmente autorizada e condicionada à implementação de controles adicionais, como a **criptografia integral dos dados** contidos no dispositivo.

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).

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.

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.

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

a) 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.
b) 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

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.

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.

MEDIDAS RELACIONADAS AO USO DE DISPOSITIVOS MÓVEIS

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.

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.

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).

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

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.

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.

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.

DICAS PARA INICIAR UMA ESTRUTURA DE SEGURANÇA DA INFORMAÇÃO:

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

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

- 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.

- 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.

- Desativação reprodução automática de dispositivos.

- Contratação de Firewall e manter sempre atualizados.

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

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

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

- 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.

SEGURANÇA DE PROCESSOS

- Implantar assinatura digital;

- Estratégia de criptografia;

- Estratégia de backup, Migração de servidores para a nuvem.