N&A INFORMÁTICA
SOLUÇÕES EM GESTÃO PÚBLICA

MANUAL DE ORIENTAÇÃO

SEGURANÇA DA INFORMAÇÃO - LGPD

SUMÁRIO

APRESENTAÇÃO

A N&A Informática é uma empresa 100% sul-mato-grossense, nascida do sonho de um casal de empreendedores, que desde a década de 1990 apresenta soluções tecnológicas para a gestão pública, contribuindo para que as cidades do estado de Mato Grosso do Sul tornem-se melhores e mais organizadas, com maior controle sobre todos os recursos financeiros, organizacionais e administrativos, com foco nos princípios da eficiência, eficácia e efetividade.

Nosso sistema organiza e define processos, armazena dados, gera informação e auxilia usuários e gestores na gestão, com apoio de profissionais e serviços capacitados para treinar pessoas para a utilização das informações disponibilizadas, de forma a prestar o melhor atendimento ao cidadão.

A Tecnologia da Informação (TI) possui um papel cada vez mais relevante para o as instituições da Administração Pública. Assim, tem crescido também a importância da proteção de dados e informações geradas e armazenadas.

Em razão de diversos ciberataques ocorridos em todo o mundo, a segurança da informação tornou-se um ponto crucial à manutenção e ao avanço das instituições.

Considerando a relevância desse tema, e ainda importância de sua conscientização, elaboramos este manual com intuito de despertar a atenção para os aspectos da segurança da informação nas instituições governamentais.

Nossa expectativa é que o presente trabalho auxilie os nossos clientes e seus usuários internos a aprimorar a segurança da informação das instituições públicas, criando um ambiente cada vez melhor e mais seguro para o atendimento às demandas da sociedade sulmatogrossense.

LGPD – LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em agosto de 2020 - **Lei nº13.709/2018**

A nova Lei faz menção à Lei de Acesso à Informação, que determina que os dados pessoais só devem ser utilizados pelas entidades e órgãos públicos para o atendimento de interesses públicos, vetando qualquer tipo de divulgação das informações dos cidadãos

O Poder Público poderá coletar dados pessoais, desde que os mesmos sejam utilizados para atender a finalidades específicas e claras de políticas públicas (exemplo: Vacinação, Segurança, Investigações etc.).

Em caso de infração a esta Lei por órgãos públicos, poderão ser enviados informes com medidas cabíveis como advertência, bloqueio ou eliminação dos dados.

A autoridade nacional pode solicitar aos agentes do Poder Público relatórios de proteção de dados e a adoção de padrões de boas práticas.

Por fim, a lei ainda obriga que em caso de ataque cibernético a empresa, ou órgão público, deverá comunicar a ANPD para que seja investigada a possibilidade de vazamento das informações. Essa obrigação fará com que as organizações invistam mais em segurança interna e externa dos dados, fazendo com que os usuários se sintam mais seguros ao acessar conteúdo online.

ASSESSMENT LGPD – AÇÕES

Um dos primeiros passos a serem dados é a revisão de todos os processos que envolvam dadospessoais e sensíveis, aplicando uma política de governança para tratamento dessas informações em conformidade com a legislação.

OS 10 REQUISITOS PARA TRATAMENTOS DE DADOS PESSOAIS

I. **Finalidade** - Finalidade específica para tratamento dos dados pessoais - coletar os dados parafins indefinidos.
II. **Adequação** - Coletar apenas os dados compatíveis com a finalidade informada.
III. **Necessidade** - Utilizar o mínimo necessário de dados pessoais para realização de suasfinalidades.
IV. **Livre acesso** - Acesso livre e gratuito ao tratamento e à integralidade dos dados do titular.
V. **Qualidade dos dados** - O titular pode conferir se seus dados são exatos, claros, relevantes eatualizados.
VI. **Transparência** - Garantir, ao titular, informações claras e precisas aos titulares.
VII. **Segurança** - Apresentar medidas técnicas e administrativas adequadas.
VIII. **Prevenção** - Apresentar medidas para prevenir danos aos titulares.
IX. **Não Discriminação** - Não utilização para fins discriminatórios, ilícitos ou abusivos.
X. **Responsabilidade e Prestação de Contas** - Comprovar o cumprimento das normas de proteçãode dados pessoais.

- Incorporação de métodos para proteção de dados desde a concepção do sistema ou produto(Privacy by Design).
- Controle de acesso (perfis/senhas)
- Revisar acessos diretos a banco de dados
- Mapear acessos internos a diretórios de rede compartilhados
- Revisar acesso a sites que possuam dados pessoais e e-mail externo (gmail, hotmail, etc.)
- Mudanças de hábito:
    - Política de mesa limpa
    - Descarte consciente de informações confidenciais

CONCEITOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

Existem três conceitos básicos que englobam a segurança da informação. O primeiro é a **confidencialidade**, que significa que uma informação só pode ser aberta para pessoas autorizadas. O segundo é o conceito de **integridade**, que está ligado a ideia de manter todas as informações originais armazenadas em um local seguro. O terceiro conceito é o da **disponibilidade**, que significa que a informação deve estar sempre disponível para ser usada por quem precisa.

APLICAÇÃO DE ESTRATÉGIAS DE SEGURANÇA

CONTROLE DO ACESSO AO USUÁRIO

I. **Acesso à rede -** No campo de redes, a área de segurança de rede, consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados. Segurança de rede envolve a autorização de acesso aos dados de uma rede, os quais são controlados pelo administrador de rede. A segurança de rede cobre uma variedade de redes de computadores, tanto públicas como privadas. A maneira mais comum e simples de proteger um recurso de rede é atribuir um nome único e uma senha correspondente.

II. **Acesso ao Banco de Dados** - A porta de acesso de um banco de dados é o ponto mais vulnerável a invasões e comprometimento de informações vitais para a entidade, assim como o acesso aos sistemas.
A melhor forma de mitigar os riscos é **bloquear totalmente o acesso ao banco de dados**, criando credenciais com níveis de acesso para restringir e controlar quem pode acessar o banco de dados.

III. **Acesso aos sistemas da N&A Informática -** Outro item fundamental para confidencialidade da informaçãona entidade é a atenção e cuidado com os **USUÁRIOS** dos sistemas, que devem ser criados individualmente, **não podendo criar usuário Genérico**, pois, caso ocorra alguma ação indevida no sistema, não serápossível identificar quem realizou a ação para uma auditoria.
Os níveis e controles de acesso são fundamentais e devem estar atrelados às funções das pessoas na entidade, para definir o acesso a uma funcionalidade específica. Deve ser assegurado o acesso de usuário autorizado aos processos estritamente necessários ao desenvolvimento de suas tarefas.

Ressaltamos que todos os sistemas desenvolvidos pela N&A Informática possuem a opção de **permissão de acesso** para que a entidade configure os usuários X atividades.

Cuidados a serem tomados com a senha:

- Não divulgue e nem compartilhe – a senha é de uso pessoal e de mais ninguém.
- Não escreva sua senha em local público ou de fácil acesso.
- Não deixe sua senha visível ao digitá-la, muito menos na presença de desconhecidos.
- Nunca use palavras de dados pessoais como senha.
- Crie senhas com mais de oito caracteres e que misture letras maiúsculas, minúsculas números e caracteres especiais.
- Mude de senha regularmente, principalmente se compartilhar a utilização de máquinas com outras pessoas.
- Utilize criptografia para definir sua senha pessoal, tornando muito difícil alguém adivinhar a senha definida. Por exemplo: utilize a última letra do nome de seus irmãos e o ano de nascimento do seu primeiro filho. Utilizando sua criatividade e dificultando bastante o acesso indevido.

GARANTIA DA SEGURANÇA DO BACKUP

O backup ou cópia de segurança é um mecanismo fundamental para assegurar a disponibilidade da informação, caso as bases de dados em que a informação esteja armazenada sejam roubadas ou danificadas, **sendo de inteira responsabilidade do cliente da N&A Informática, conforme previsão contratual**.

Fazer backup dos seus dados, evita que os arquivos sejam permanentemente perdidos ou danificados em caso de algum incidente, seja ele físico, lógico, ambiental, ou, uma falha humana. Os arquivos de backup ajudam a evitar ou minimizar as perdas de trabalho executado caso algo indesejado aconteça, e por isso deve-se gerá-los regularmente.

Recomendações para evitar perda de dados:

I. **Automatize seu backup -** Com backups automáticos, não é preciso se lembrar de fazer backup dos arquivos, você pode configurar a frequência de acordo com a carga de trabalho esperada, escolhendo o melhor horário para que ele seja executado.

II. **Criar agendas de backup –** É extremamente importante que você defina a periodicidade do seu backup, o que vai variar da criticidade do seu negócio. Se questione o quanto vale a informação para a sua organização.

III. **Atenção à escolha da mídia utilizada para o backup -** Recomendamos que você **não faça o backup dos arquivos no mesmo disco rígido** em que o banco de dados se encontra instalado, dando preferência a mídias removíveis como discos rígidos externos, pastas compartilhadas e serviços de backup's especializados na nuvem.

IV. **Documentos dos sistemas da N&A Informática -** Além dos bancos de dados é extremamente importante fazer uma cópia semanal das pastas que possuem documentos da N&A Informática que ficam em pastas compartilhadas na rede ou em computador local.

V. **Testar o restore do backup do Banco de Dados –** Para garantir que o processo de cópia está íntegro e funcionando corretamente, após restaurar o Banco de Dados acessar o sistema no banco cópia, com um usuário real, com o objetivo de realizar os testes.

AMBIENTE SEGURO E ADEQUADO

O ambiente também é importante estar atualizado e preparado caso ocorra algum ataque cibernético ou problemas físicos, sendo assim, relacionamos algumas boas práticas para melhorar a segurança do ambiente:

I. Tenha antivírus e firewall no seu servidor e restrinja o acesso a ele. Prolongar a vida útil do seuservidor é fundamental.

II. Oriente sempre os usuários quanto às melhores práticas de segurança, como não clicar em popup's de e-mails, verificar o remetente, não enviar senhas por e-mail.

III. Tenha antivírus em todos os computadores, de preferência licenciados, pois eles abrangemuma área de segurança maior.

IV. Mantenha um firewall ativo e configurado corretamente para não prejudicar seus acessos emrede.

V. Tenha cuidado com os e-mails, com utilização da internet, com os dispositivos que sãoconectados aos computadores.

VI. Tenha equipamentos de qualidade e sistemas operacionais atualizados.

VII. Tenha bons nobreaks, especialmente para servidor(es).

DÚVIDAS?

Em caso de dúvidas, entre em contato com nosso setor de Atendimento ao Cliente, pelo e-mail atendimento@neainformatica.com.br ou pelo telefone (67) 3047-2500.