NORMAS DE SEGURANÇA PARA CONTROLE DE ACESSO REMOTO E USO DE CRIPTOGRAFIA

1. OBJETIVO

Esta norma de segurança tem por objetivo definir critérios de segurança e descrever as ações para efetuar o acesso remoto no âmbito da Prefeitura Municipal e visa controlar e proteger os recursos de hardware e software institucionais contra acessos não autorizados.

2. DEFINIÇÃO

Aplica-se a todos os colaboradores do Departamento de TI que possuam acesso aos sistemas de informação, redes, serviços ou recursos tecnológicos.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

Lei nº 13.708/18 - Lei Geral de Proteção de Dados Pessoais (LGPD);
Política de Segurança da Informação da Prefeitura;
ABNT NBR ISO/IEC 27001 - Estabelece os elementos de um Sistema de Gestão de Segurança da Informação e da Comunicação.

4. RESPONSABILIDADE

É responsabilidade do DTI garantir a aplicação desta norma.

5. DIRETRIZES:

5.1. Autorização:

A autorização do funcionário para acessar remotamente a rede de computadores da organização será determinada por seus respectivos superiores. O DTI deve aprovar o uso de acesso remoto de cada membro da equipe. Todos os funcionários devem enviar via memorando a solicitação para uso ao acesso remoto.

5.2. Quanto ao Acesso Remoto:

I - É imprescindível que os usuários dos serviços do DTI que utilizem o acesso remoto estejam conscientes dos riscos e responsabilidades envolvidos em decorrência de mau uso do serviço de suas credenciais.

II - O acesso remoto deve ser provido por meio de canal criptografado, preferencialmente utilizando as recomendações da ICP-Brasil;

III - O acesso remoto à rede terá privilégios diferenciados do acesso local, de acordo com o perfil de acesso, com serviços explicitamente controlados;

IV - O uso do acesso remoto se restringe a jornada de trabalho ou de colaboração, não sendo permitido que sejam utilizados além desse horário, salvo por extrema necessidade.

V - O DTI fornecerá ao usuário a documentação necessária e/ou suporte para colocar o software de acesso remoto em execução e em funcionamento;

VI - As permissões de acesso remoto serão revisadas periodicamente.

VII - O Departamento de Recursos Humanos deverá apoiar os administradores de sistemas do DTI com as informações pertinentes dos servidores públicos/usuários como admissão, demissão, afastamento temporário ou permanente, subsidiando as ações de revogação de acessos;

5.3. Credenciais:

Cada usuário deve utilizar credenciais individuais, que devem ser mantidas em sigilo e não podem ser compartilhadas. O acesso remoto deve ser exclusivamente para finalidades relacionadas às atividades do DTI, sendo vedada qualquer utilização que não esteja vinculada ao desempenho das funções do usuário.

5.4. Confidencialidade:

Os usuários são responsáveis por garantir a confidencialidade das informações acessadas remotamente, não permitindo que terceiros não autorizados tenham acesso ou visualizem tais informações, minimizando assim os riscos de roubo de credenciais e outras ameaças digitais.

5.5. Uso de Criptografia:

Todos os dados sensíveis, incluindo informações pessoais, financeiras, comerciais e confidenciais, devem ser criptografadas quando armazenadas (em repouso) e durante a transmissão (em trânsito) para proteger contra acessos não autorizados.

As chaves criptográficas utilizadas para criptografar e descriptografar dados são gerenciadas com o mais alto nível de segurança. O acesso às chaves é estritamente controlado e limitado a pessoal autorizado. Todos os backups de dados sensíveis devem ser criptografados, independentemente de serem armazenados localmente, em dispositivos externos ou em serviços de armazenamento na nuvem. Isso garante que os dados permanecem seguros, mesmo em caso de violação física ou digital dos backups.

O controle das chaves deve ser mantido pelo DTI bem como a liberação da sua existência catalogados em sistemas.

Todos os funcionários que lidam com dados sensíveis são treinados regularmente sobre a importância da criptografia e as práticas recomendadas para proteger os dados da organização. Isso inclui o uso adequado de ferramentas de criptografia e a responsabilidade de manter as chaves e senhas seguras.

Visando minimizar os riscos relacionados à segurança das informações, é recomendável o uso de software anti-malware e firewall nos dispositivos pessoais utilizados pelos usuários para acesso remoto;

Não é recomendado o acesso remoto utilizando redes Wi-Fi públicas, abertas (sem criptografia) ou compartilhadas por terceiros.

5.6. Proteção conta ameaças:

O DTI deve garantir que todos os dispositivos que se conectarão às redes ou recursos da empresa por meio de acesso remoto não tenham software ou aplicativos de terceiros que representem uma ameaça aos sistemas e redes da organização ou que possam introduzir incompatibilidades de aplicativos. Se possível, o monitoramento periódico desses dispositivos deve ser realizado para garantir que eles continuem a atender aos padrões de conformidade.

5.7. Monitoramento e Auditoria:

Todas as atividades realizadas por meio de acesso remoto poderão ser monitoradas e registradas para fins de auditoria e segurança. O DTI tem competência de revogar o acesso remoto de qualquer usuário que não cumpra esta norma, que represente risco à segurança ou que atue em interesse próprio.

5.8. Aquisição de hardware e software:

Toda aquisição de hardware e software necessária para o desempenho das atividades dos colaboradores deverá ser coordenada pela área do DTI, para garantir a aderência aos requisitos técnicos e funcionais de tecnologia e segurança da informação.

6. PROCEDIMENTOS:

I - O acesso remoto à rede da Prefeitura deve ser realizado exclusivamente relacionada à atividade profissional, sendo proibida a sua utilização para finalidades distintas do desempenho das atividades inerentes ao cargo / função do servidor;

II - O DTI deve utilizar software de acesso remoto padrão e manter um conjunto de instruções para ajudar os usuários a instalar e usar esses produtos. O software deve corresponder aos ambientes de sistema operacional em uso na organização.

III - Os usuários estão sujeitos às técnicas de autenticação que permitam validar a identidade do Usuário da Rede (biometria, tokens, smartcards, entre outros);

IV - Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à área de gestão de incidentes;

V - Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a área de gestão de incidentes deverá ser imediatamente acionada para tomar as providências necessárias a sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação Prefeitura.

VI - Qualquer mudança nesta política deve ser aprovada pelo DTI e/ou qualquer violação desta norma poderá resultar em ação disciplinar.