Política de acesso remoto

Norma #	Vigência	Versão
07	01/11/2021	1.0

Contato	E-mail	Telefone
Lemuel Victor Dias	victor.dias@medicamental.com.br	(16) 3505-4900

Índice:

1 Visão geral

O acesso remoto seguro aos sistemas e redes da empresa agora é um modelo de trabalho para a maioria das empresas. À medida que conglomerados corporativos, pequenos negócios e lojas físicas desaparecem em favor de uma força de trabalho externa distribuída, as empresas e os funcionários podem ganhar com a maior conveniência e eficiência proporcionada pelo acesso remoto.

Uma implementação de acesso remoto pode reduzir os custos de equipamentos, reduzir as despesas gerais da empresa e facilitar a produtividade dos funcionários.

No entanto, as vantagens do acesso remoto também incluem alguns desafios que são mais facilmente superados pela equipe no local: garantir que apenas o pessoal autorizado possa acessar os recursos da empresa, proteger dispositivos que não estão diretamente sob controle de TI (nem disponíveis para suporte prático) e lidar adequadamente com as demissões dos funcionários.

2 Objetivo

Esta política descreve as diretrizes e processos da empresa para solicitar, obter, usar e encerrar o acesso remoto às redes, sistemas e dados da organização.

Aplica-se a cenários em que os funcionários se conectam remotamente a datacenters internos e também a instalações externas, como provedores de serviços de computação em nuvem.

3 Aplicabilidade

Esta norma se aplica:

- À todas as unidades, áreas, setores e departamentos da empresa.

- A todos os analistas de segurança da informação e administradores de sistemas responsáveis pela manutenção de sistemas, softwares, aplicativos, programas, dispositivos e equipamentos de TI gerenciados pela empresa.

- A todos os dirigentes, funcionários em tempo integral, funcionários em meio período, funcionários em tempo parcial, trabalhadores contratados, consultores, estagiários, trabalhadores temporários, prestadores de serviços, agentes, parceiros, fornecedores e usuários autorizados que acessam remotamente sistemas da empresa.

4 Norma

4.1. Determinando usuários elegíveis

Somente usuários com necessidade comprovada de se conectar aos recursos da empresa devem ter recursos de acesso remoto. Isso obviamente se aplicará a trabalhadores externos por padrão, mas os trabalhadores locais devem ser selecionados de forma criteriosa. Usuários com acesso a dados de cartão de crédito, por exemplo, podem ser

inelegíveis para o recurso de acesso remoto se isso representar um risco financeiro ou de segurança. Os usuários cujas responsabilidades de trabalho envolvem interação prática ou face a face também podem ser impedidos de privilégios de acesso remoto.

A elegibilidade do funcionário para acessar remotamente a rede de computadores da organização será determinada por seus respectivos gerentes. O departamento de TI também deve aprovar o uso de acesso remoto de cada membro da equipe.

Todos os funcionários devem enviar uma solicitação de acesso remoto.

4.2. Determinando o software de acesso remoto apropriado

O departamento de TI deve utilizar software de acesso remoto padrão e manter um conjunto padrão 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 (ou em dispositivos de propriedade do funcionário, se aplicável); exemplos comuns são Windows, Linux e Apple OS. Também pode ser necessário utilizar software de acesso remoto nos sistemas operacionais Android e iOS usados por dispositivos móveis.

O software de acesso remoto deve proibir o split-tunneling (acessar duas redes ao mesmo tempo). Em vez disso, deve limitar a conexão de dispositivos para funcionar apenas nas redes da empresa.

4.3. Determinando o equipamento de acesso remoto elegível

O departamento de TI deve desenvolver e manter uma lista de equipamentos aprovados e com suporte a serem usados para acesso remoto aos sistemas, redes e dados da empresa. Este equipamento envolve dispositivos de hardware (incluindo tokens VPN físicos, RSA *SecurIDs, hotspots Wi-Fi*, roteadores, *smartphones, tablets, laptops* e *desktops*), que devem ser usados apenas para criar, pesquisar e processar responsabilidades relacionadas à empresa.

Todos os usuários e dispositivos de acesso remoto estão sujeitos às políticas e padrões de segurança existentes. Os exemplos podem incluir a política de segurança de informações da empresa, política de segurança de rede, política de uso de software e política de computação de dispositivo móvel.

4.4. Padrões aplicados ao acesso remoto

O uso de equipamentos e software fornecido pela organização para o acesso remoto a sistemas empresa, rede, e dados é limitado a pessoas

autorizadas e única para fins relacionados ao cumprimento dos negócios e operações da empresa.

As contas de usuário de acesso remoto devem ser configuradas com senhas complexas e definidas para serem bloqueadas após um determinado número de falhas de autenticação.

As senhas de proteção de tela também devem ser empregadas.

O departamento de TI 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.

4.5. Uso de computadores e equipamentos pessoais

Os funcionários terão permissão para usar computadores e equipamentos pessoais para acesso remoto, desde que atendam aos padrões estabelecidos pelo departamento de TI.

O suporte aos computadores e equipamentos pessoais deve ser fornecido a critério do departamento de TI e deve ser restrito a resolver problemas de acesso remoto. Durante o processo de suporte, o departamento de TI pode exigir que a os funcionários autorizados e os contratados reinstalem completamente os sistemas operacionais de computadores domésticos e pessoais e o software aplicativo.

Problemas gerais de sistema operacional / *software* / *hardware* devem ser resolvidos pelo fornecedor ou empresa terceirizada autorizada, quando aplicável. O funcionário também é responsável por garantir que o software anti-malware esteja presente e atualizado nos dispositivos que se conectam às redes e/ou recursos computacionais da empresa e que eles recebam atualizações regulares de aplicativos e sistemas operacionais.

A empresa não poderá ser responsabilizada se a instalação ou uso de qualquer acesso remoto necessário e/ou software de segurança causar travamentos do sistema, travamentos ou perda total ou parcial de dados armazenados nos equipamentos pessoais do funcionário. O funcionário ou contratado autorizado é o único responsável por fazer backup dos dados em sua máquina pessoal antes de iniciar qualquer trabalho organizacional e se conectar aos sistemas, redes ou recursos de informática da empresa.

A seu critério, a empresa não permitirá o acesso remoto para qualquer usuário que opere um computador pessoal doméstico ou dispositivo que se mostre incapaz, por qualquer motivo, de não funcionar corretamente com o software ou sistemas fornecidos pela empresa, ou que seja considerado um risco de segurança.

4.6. Autorização de acesso remoto e processo de implementação

Sempre que qualquer usuário da empresa – seja um funcionário em tempo integral, executivo, contratado, consultor ou voluntário – quiser usar um dispositivo pessoal ou de propriedade/fornecido pela empresa para se conectar às redes, sistemas e recursos da organização, as seguintes etapas devem ser completadas:

- Se o departamento de TI for fornecer ao usuário equipamentos de propriedade da empresa, eles devem ser adquiridos e fornecidos ao usuário.
- Se o funcionário fornecer seu próprio equipamento para o acesso remoto, o departamento de TI deve garantir que ele atenda aos requisitos da empresa conforme necessário para recursos de acesso remoto.

- O departamento de TI fornecerá ao usuário a documentação necessária e/ou suporte para colocar o software de acesso remoto em execução e em funcionamento.

4.7. Responsabilidade do usuário no acesso remoto

Apenas o pessoal autorizado da empresa deve usar o equipamento fornecido pela empresa ou acessar os sistemas e redes da empresa.

Se um usuário acredita que o equipamento usado para acessar remotamente os recursos, sistemas e redes da empresa pode estar infectado com um vírus, infecção por spyware ou outra ameaça de malware ou que pode estar de alguma forma comprometido, ele deve notificar imediatamente o departamento de TI sobre o potencial risco à segurança e disponibilizar o equipamento para análise e remediação.

Se um usuário perder o equipamento autorizado a se conectar remotamente aos recursos, sistemas e redes da empresa, ele deve notificar imediatamente o departamento de TI sobre o risco potencial à segurança. Será então responsabilidade do departamento de TI limpar remotamente o (s) dispositivo (s), alterar as senhas ou bloquear a conta do usuário conforme necessário.

Se os dispositivos envolvidos forem de propriedade do funcionário, será responsabilidade do funcionário buscar e financiar os itens de reposição.

4.8. Processo de suspensão do acesso remoto

Sempre que um usuário desativar um dispositivo ou equipamento ou de outra forma parar de usar hardware e/ou software autorizado para acesso remoto, ele deve notificar o departamento de TI de que o equipamento e qualquer software correspondente não serão mais usados para se conectar aos recursos, sistemas e redes e, em seguida, devolver qualquer equipamento de propriedade da empresa (quando aplicável) para o departamento de TI.

Os usuários não podem descartar equipamentos de acesso remoto previamente autorizados de propriedade da empresa, a menos que o departamento de TI autorize o descarte do equipamento.

O departamento de TI será responsável por apagar e reutilizar com segurança qualquer equipamento de propriedade da empresa para disponibilizá-lo para um futuro funcionário.

O departamento de TI será responsável por remover qualquer software de acesso remoto, criptografia, VPN e licenciamento anti-malware necessários do equipamento de propriedade do funcionário e garantir que

todos e quaisquer dados da empresa sejam removidos do (s) dispositivo (s). Caso o usuário não disponibilize o equipamento para a área de TI, ele deve ser apagado ou desabilitado remotamente, se possível.

5 Responsabilidade

É responsabilidade do departamento de TI e de cada gestor de departamento, área, setor ou unidade da empresa garantir a aplicação desta norma.

6 Verificação da Conformidade

A equipe de TI, o departamento de RH e os gestores de cada departamento, área, setor ou unidade da empresa verificará a conformidade com esta política por meio de vários métodos, incluindo, mas não se limitando a, walk-thrus periódicos, logs de auditoria de sistemas e banco de dados, auditorias de TI e feedbacks para o responsável pela política.

Qualquer mudança nesta política deve ser aprovada pelo departamento de TI.

7 Exceções

Não há exceções a esta política. Qualquer exceção à esta norma deverá ser previamente aprovada pela equipe de TI.

8 Violação

Qualquer violação desta norma pode resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho. A empresa reserva-se o direito de notificar as autoridades responsáveis pela aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade. A empresa não considera que a conduta que viole esta norma esteja dentro do curso e âmbito das atividades de um funcionário, parceiro ou prestador de serviço, ou como consequência direta da execução de suas funções. Consequentemente, na medida do permitido por lei, a empresa reserva-se o direito de não defender ou pagar quaisquer danos concedidos aos funcionários, parceiros ou prestadores de serviços que resultem da violação desta norma.

9 Aprovação

Responsável	Cargo/Função	Data
LEMUEL VICTOR DIAS	ADVOGADO	18/10/2021
Aprovado por	**Cargo/Função**	**Data**
EDGAR ROBERTO THEODORO	DIRETOR	19/10/2021

10 Histórico de versões

Versão	Descrição	Última Revisão	Próxima Revisão	Revisor/ Aprovador
1.0	Versão inicial	01/03/2021	01/03/2022	