

Política de acesso ao datacenter

Norma #
08

Vigência
01/11/2021

Versão
1.0

Contato
Lemuel Victor Dias

E-mail
victor.dias@medicamental.com.br

Telefone
(16) 3505-4900



Índice:

1	Visão Geral	1
2	Objetivo	1
3	Aplicabilidade	1
4	Norma	2
5	Responsabilidade	4
6	Verificação da conformidade	4
7	Exceções	4
8	Violação	4
9	Aprovação	5
10	Histórico de revisão	5

1 Visão geral

O datacenter de uma empresa serve como a verdadeira força vital da organização contendo dados, sistemas que executam serviços críticos, firewalls que permitem o acesso dentro e fora das redes da empresa, e outros elementos dos quais a empresa precisa para funcionar adequadamente.

Com isso em mente, é importante garantir que o datacenter seja totalmente protegido e acessado apenas por pessoal autorizado para a condução de esforços relacionados aos negócios, a fim de garantir o

máximo de tempo de atividade, reduzir desastres operacionais e evitar o roubo de equipamentos e dados da empresa.

2 Objetivo

O objetivo desta política é fornecer diretrizes para o acesso apropriado, presença e operações conduzidas no datacenter da empresa.

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

O datacenter deve ser fisicamente protegido contra acessos não autorizados.

A autenticação de dois fatores poderá ser usada para se obter acesso ao datacenter.

O crachá (ou sistema biométrico) e as câmeras de segurança devem ser utilizados para registrar o acesso de pessoas ao datacenter. Este acesso deve ser monitorado e evidenciado, com registros mantidos por pelo menos 30 dias.

Alertas devem ser configurados para notificar a equipe apropriada de acesso não autorizado ao datacenter.

Os registros de acesso ao datacenter não devem ser alterados, removidos ou desligados.

Apenas pessoal autorizado deve ter permissão para entrar no datacenter para fins de condução dos negócios da empresa. Qualquer outro uso do datacenter, como, por exemplo, o armazenamento de equipamentos diversos deve ser proibido.

Todo pessoal que não seja da empresa deverá ter acesso permitido ao datacenter apenas em uma base temporária, a fim de realizar operações relacionadas com as instalações, manutenção, reparo ou outras atividades necessárias para manter os equipamentos e instalações em funcionamento. Este acesso deve ser solicitado com pelo menos 24 horas de antecedência e deve receber aprovação do Departamento de TI.

Todo pessoal que não seja da empresa deve estar acompanhado durante a realização dos trabalhos no interior do datacenter da empresa.

Todo pessoal que não seja da empresa deve exibir um crachá de visitante enquanto trabalha no interior do datacenter para garantir que a autorização de seu acesso foi aprovada.

O datacenter deve registrar a entrada e saída para rastrear atividades de pessoal não pertencente à empresa. Estes logs devem ser guardados de forma segura e o acesso a esses logs deve ser limitado a pessoal autorizado.

Nenhum alimento ou bebida deve ser permitido no interior do datacenter.

Todos os indivíduos que trabalham no datacenter, sejam funcionários ou indivíduos externos, devem seguir todas as diretrizes de segurança

envolvendo procedimentos contra incêndio, controles ambientais e uso de equipamentos.

Nenhum trabalho pode ser executado em um sistema de produção crítico sem autorização prévia usando uma cadeia de aprovação, como uma solicitação de mudança ou ordem de trabalho de produção. Os detalhes do trabalho devem ser revisados e acordados antes de ser dada a aprovação para prosseguir.

Todo o trabalho realizado no datacenter deve ser registrado. Os detalhes devem incluir o (s) sistema (s) envolvido (s), o tipo de trabalho que está sendo executado, os indivíduos associados ao trabalho, a duração do tempo gasto e o resultado das operações.

As visitas ao datacenter poderão ser autorizadas com as devidas permissões, mas os visitantes poderão tocar nos equipamentos e devem estar acompanhados por um representante do departamento de TI em todos os momentos.

O acesso ao datacenter deve ser auditado pelo menos semestralmente para garantir a conformidade com essas diretrizes.

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. Conseqüentemente, 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
LEMEUL 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	