Política de eliminação segura de equipamentos, dispositivos, mídias e dados

Norma #	Vigência	Versão
11	01/03/2021	1.0

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

Índice:

1 Visão Geral 1

2 Objetivo 1

3 Aplicabilidade 2

4 Norma 2

5 Responsabilidade 7

6 Verificação da conformidade 8

7 Exceções 8

8 Violação 8

9 Aprovação 9

10 Histórico de revisão 9

1 Visão geral

Cada dispositivo de hardware usado por uma empresa tem uma vida útil finita ou período viável de uso, e a desativação ou eliminação de dispositivos antigos e a aquisição de novos faz parte da vida com a tecnologia.

Na verdade, setores e metodologias inteiros surgiram para ajudar a facilitar esse processo: produtos de backup e armazenamento baseados em nuvem, recursos de armazenamento externo, transferência de dados

automatizada e técnicas de gerenciamento de configuração para colocar sistemas substitutos em funcionamento rapidamente.

A desativação de hardwares pode ocorrer por uma série de razões, incluindo cortes nas despesas operacionais, atualizações para hardwares mais recentes, falha de equipamento e obsolescência. Independentemente do raciocínio por trás disso, a consistência no manuseio do processo é essencial.

Ao desativar o hardware, as práticas padrão e bem documentadas são essenciais. As práticas descritas nesta política guiarão a equipe adequada durante o processo de desativação.

Se esta política for seguida corretamente, os ativos não serão desnecessariamente desperdiçados ou colocados em mãos erradas, os dados armazenados serão preservados conforme necessário (ou eliminados com segurança) e todas as informações auxiliares relativas ao hardware (etiquetas de ativos, localização, status, etc.) serão atualizadas em conformidade.

2 Objetivo

Esta política fornece diretrizes para a remoção e descarte apropriados de todo hardware tecnológico usado pela empresa e dos dados nele contidos.

Abrange cenários em que o hardware é doado, vendido, desativado, reciclado ou destruído.

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 as dependências da empresa.

- A qualquer dispositivo usado na empresa seja de propriedade do funcionário, de propriedade da empresa ou alugado pela empresa, incluindo, mas não se limitando a roteadores, switches, hubs,

impressoras, scanners, copiadoras, servidores, desktops, laptops, dispositivos móveis, tablets e mídia de armazenamento.

4 Norma

4.1. Responsabilidade pela remoção ou descarte de hardwares

A remoção, descontinuidade, desativação, descarte ou destruição de hardwares (seja devido à obsolescência, falha ou outro motivo) será de responsabilidade exclusiva do departamento de TI, que trabalhará com quaisquer gestores e partes interessadas relacionadas.

4.2. Remoção ou descarte de hardwares

Às vezes, a decisão de remover ou descartar o hardware é fácil, mas em outros casos pode ser difícil encontrar a resposta certa. Em caso de dúvida, a decisão deve sempre estar baseada nas seguintes questões:

- O dispositivo não está funcionando?
- O dispositivo não é mais necessário?
- O dispositivo é de propriedade de um funcionário que não exige mais seu uso para as operações da empresa ou está saindo da empresa?

- O dispositivo está funcionando mal ou causando interrupções nas operações da empresa?
- O dispositivo pode ser reparado ou atualizado para ter um desempenho mais confiável?
- O dispositivo está desatualizado e não é mais a melhor escolha para uso?
- O dispositivo é redundante?
- Quais serviços serão afetados pela remoção deste dispositivo?
- Esses serviços podem ser substituídos ou realocados para outro lugar?

Ao responder estas perguntas, o departamento de TI poderá decidir se continua a utilizar o equipamento, se irá doá-lo, se irá remover do equipamento os dados da empresa nele contidos ou se irá reciclá-lo ou destruí-lo.

A escolha feita aqui dependerá do dispositivo, da equipe envolvida e das políticas e procedimentos de segurança. Portanto, isso irá variar de acordo com as circunstâncias.

4.3. Eliminação segura de dados dos hardwares

O apagamento seguro de dados de um hardware ou dispositivo móvel é necessário quando um dispositivo for doado, vendido ou quando for enviado para ser reciclado ou destruído, mas sua mídia de armazenamento ainda puder ser utilizada por outras pessoas sem relação com a empresa.

O departamento de TI deve ser consultado para garantir que as medidas apropriadas estão sendo adotadas durante o processo de remoção/destruição segura do equipamento para proteger a empresa e seus dados.

A mídia de armazenamento pode ser apagada apenas se puder ser gravada, o que significa que será necessário realizar alterações nas informações nela contidas. Os discos CD-R ou DVD-R, por exemplo, não podem ser apagados com segurança e, portanto, devem ser destruídos.

Discos rígidos, unidades USB e cartões de armazenamento, como micro-SD, devem ser apagados com segurança em um computador usando softwares apropriados. Tal processo substitui os dados com fluxos aleatórios de caracteres para garantir que as informações confidenciais não sejam recuperadas.

Softwares de apagamento seguro de mídia (também conhecido como ferramentas de limpeza) deverão ser utilizadas para limpar essas unidades com segurança.

Muitas ferramentas de apagamento seguro de mídia são independentes do sistema operacional, o que significa que podem ser executadas em qualquer disco rígido, independentemente de ter o sistema operacional Windows, Mac ou Linux instalado.

Se o dispositivo incluir ou utilizar fitas de backup que possam ser usadas em outro lugar, as fitas devem ser totalmente reutilizadas e substituídas (com dados irrelevantes, por exemplo) para garantir que quaisquer dados confidenciais sejam tornados inacessíveis.

4.4. Eliminação segura de dados de dispositivos móveis

Todos os dispositivos móveis (exceto aqueles pertencentes a funcionários que não os usam nas operações da empresa) devem ter os seus dados apagados. Softwares de apagamento seguro de dados deverão ser utilizadas para limpar esses dispositivos com segurança. O processo deverá retorná-los aos padrões originais de fábrica. As instruções variam de acordo com o dispositivo, e por isso devem ser pesquisadas e documentadas com antecedência.

Cartões de armazenamento externos também devem ter os dados apagados utilizando-se softwares de apagamento seguro de dados

Para cenários BYOD (Bring your own device), a equipe de TI deve trabalhar com os funcionários para garantir que apenas os dados da empresa sejam

apagados e não todo o sistema operacional ou dados particulares do funcionário.

4.5. Destruição segura de mídias de armazenamento

Nesta situação, o dispositivo em questão está sendo retirado de uso, seja por obsolescência, falha do equipamento ou algum outro motivo, e a mídia de armazenamento que ele contém não poder ser reutilizada em outro lugar.

Se o dispositivo incluir ou utilizar fitas de backup que não podem ser usadas em outro lugar, as fitas devem permanecer sob o controle do departamento de TI até que sejam destruídas.

Ao doar ou vender um dispositivo, a mídia de armazenamento associada deve ser deixada intacta assim que for confirmado que todos os dados foram removidos com segurança. Nos casos em que o dispositivo não for ser reaproveitado, a mídia de armazenamento deve ser destruída.

Fitas magnéticas devem ser desenroladas e cortadas. Os discos rígidos devem ser desmagnetizados e / ou abertos até expor os seus componentes internos. As unidades USB devem ser quebradas em duas partes e os discos de CD ou DVD devem ser quebrados ao meio. O objetivo é garantir que nenhum dado possa ser recuperado.

Isso deve ser feito na frente de uma testemunha para confirmar o processo e, no caso de servidores que contenham dados altamente confidenciais, deve-se registrar os detalhes incluindo a data e o pessoal envolvido no processo.

Os restos da mídia devem ser descartados de forma segura, como por meio de uma lixeira específica para este tipo de descarte.

4.6. Remoção de servidores

Todos os certificados SSL relacionados ao equipamento deverão ser revogados.

O equipamento deverá ser retirado de qualquer monitoramento existente ou sistemas de gerenciamento de configuração, backups, ambientes de patching, firewalls, forward/reverse DNS, Active Directory, IP spreadsheets, licenças, scripts e qualquer outro elemento no ambiente que se comunica com ou refere-se ao dispositivo.

Quaisquer contas usadas exclusivamente pelo sistema do Active Directory ou qualquer outro sistema / mecanismo de autenticação deverão ser revogadas. Se aplicável, o equipamento deverá ser removido de seu local de instalação.

Durante o processo de doação, reciclagem ou descarte/destruição o dispositivo deverá ser entregue somente a pessoal autorizado.

A sala do servidor, a rede de computadores e qualquer documentação relacionada com o equipamento deverão ser atualizados para refletirem as mudanças realizadas.

4.7. Notificação de pessoal relacionado

Os departamentos de compra e financeiro deverão ser informados sobre a doação, venda, desativação, remoção ou descarte do equipamento para garantir que licenças, contratos de suporte, acordos de manutenção ou outras despesas contínuas relacionadas ao hardware sejam encerrados.

Todas as informações de registro do equipamento deverão ser atualizadas para refletirem a suspensão do uso do hardware.

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	