Empresa : eBrejas

Comercio e distribuidora de bebidas

A empresa irá atuar na área de compra, vendas e distribuição de bebidas.

Funcionarios

* Guilherme
* Gustavo
* Rafael
* Aline
* Joice
* Rubens
* Joao
* Mateus
* Judas
* Augusto

Recursos necessários:

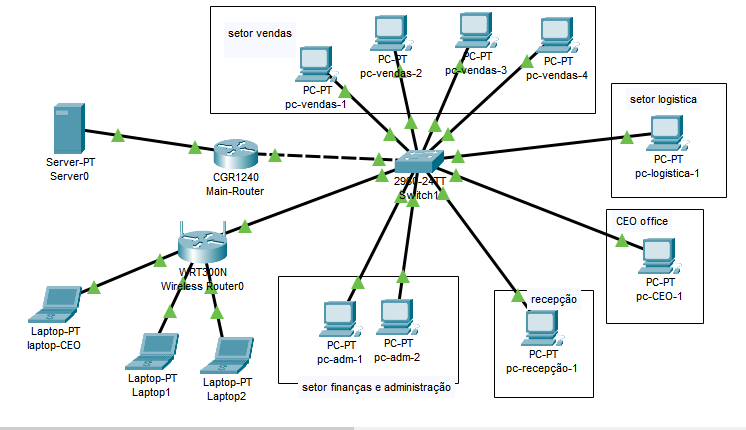
* Servidor
* Roteadores
* Roteadores Wi-Fi
* switch ou Hub
* cabos

Topologia da rede Estrela:

* Foi escolhido essa rede , pois é uma topologia de fácil gerenciamento para pequenas empresas.
* Tem menos problemas em relação a rede falhar, caso algum computador falhe ainda é possível utilizar a rede sem problemas.
* Fácil gerenciamento e identificação dos erros.
* Fácil de adicionar novos dispositivos .

Objetivos da documentação:

* Esta documentação inicial tem o objetivo de facilitar o gerenciamento da rede, facilitar a identificação e solução dos problemas encontrados e serve de guia para futuros gerenciadores.
* Caso ocorra problemas como congestionamento de rede ou problemas em dispositivos possa ser solucionada da maneira mais rápida.



Especificações

* **Nome do dispositivo**: pc-vendas-1;
* **Endereço IP : 192.168.1.5**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** escritório de vendas
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-vendas-2;
* **Endereço IP : 192.168.1.6**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** escritório de vendas
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-vendas-3;
* **Endereço IP : 192.168.1.7**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** escritório de vendas
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-vendas-4;
* **Endereço IP : 192.168.1.8**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** escritório de vendas
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-adm-1;
* **Endereço IP : 192.168.1.9**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** escritório de administração
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-adm-2;
* **Endereço IP : 192.168.1.10**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** escritório de administração
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-recepcao-1;
* **Endereço IP : 192.168.1.11**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** recepção
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-CEO-1;
* **Endereço IP : 192.168.1.12**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** escritório de Diretor
* **Modelo**: Dell Aurora r15 13º i9
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: pc-logistica-1;
* **Endereço IP : 192.168.1.13**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** almoxarifado
* **Modelo**: Dell Vostro small desktop 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: main-router;
* **Endereço IP : 192.168.1.2**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** Server and data Store
* **Modelo**: Tp-Link Archer AX72
* **Firmware:** Archer AX72(US)\_V1\_1.2.2 Build 20230927
* **Nome do dispositivo**: wireless-router;
* **Endereço IP : 192.168.1.3**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** recepção
* **Modelo**: Tp-Link Archer AX72
* **Firmware:** Archer AX72(US)\_V1\_1.2.2 Build 20230927
* **Nome do dispositivo**: server0;
* **Endereço IP : 192.168.1.4**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** Server and data Store
* **Modelo**: dell servidor torre poweredge t150
* **Sistema Operacional** : Linux CentOS Stream 9
* **Nome do dispositivo**: switch-1;
* **Endereço IP :**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Localização física :** Server and data Store
* **Modelo**: switch cisco bussines 220
* **Firmware:** 2.0.2.12
* **Nome do dispositivo**: laptop-CEO-1;
* **Endereço IP : DHCP**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Modelo**: Dell inspiron 15 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: laptop1;
* **Endereço IP : DHCP**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Modelo**: Dell inspiron 15 12º i5
* **Sistema Operacional** : Windows 11
* **Nome do dispositivo**: laptop2;
* **Endereço IP : DHCP**
* **Endereço MAC**: MAC: 00:1B:44:11:3A:B7
* **Modelo**: Dell inspiron 15 12º i5
* **Sistema Operacional** : Windows 11

**Configurações do Software.**

Introdução

Este documento descreve as regras de firewall implementadas para controlar o tráfego de entrada e saída em nosso sistema de rede. O objetivo principal é garantir a segurança e a integridade dos dados, permitindo apenas o tráfego necessário e autorizado.

**Regras do Firewall**

Trafego de Entrada:

HTTP (Porta 80): O tráfego HTTP é permitido para possibilitar o acesso aos sites da web.

HTTPS (Porta 443): O tráfego HTTPS é permitido para garantir comunicações seguras com sites que utilizam SSL/TLS.

SSH (Porta 22): O acesso SSH é permitido apenas para endereços IP autorizados, para administração remota segura.

SMTP (Porta 25): O tráfego SMTP é permitido apenas para servidores de correio eletrônico autorizados.

DNS (Porta 53): O tráfego DNS é permitido para resolução de nomes de domínio.

ICMP (Protocolo): O tráfego ICMP é permitido para permitir a comunicação de diagnóstico e controle de rede.

Outros Protocolos: Outros protocolos específicos podem ser permitidos conforme necessário, desde que aprovados pelo administrador de rede.

Trafego de Saída:

HTTP (Porta 80) e HTTPS (Porta 443): Permitido para permitir que os usuários acessem a internet e naveguem na web.

SMTP (Porta 25): Permitido para permitir o envio de e-mails pelos clientes de correio eletrônico autorizados.

DNS (Porta 53): Permitido para permitir a resolução de nomes de domínio pelos clientes.

FTP (Porta 21): Permitido para permitir transferências de arquivos FTP autorizadas.

Outros Protocolos: Outros protocolos específicos podem ser permitidos conforme necessário, desde que aprovados pelo administrador de rede.

Essas portas são padrões estabelecidos para facilitar a comunicação entre diferentes dispositivos em uma rede. Ao controlar o tráfego com base nessas portas, podemos garantir que apenas o tráfego autorizado seja permitido e que nossa rede permaneça segura e eficiente.

**Níveis de Segurança**

Este conteúdo descreve o nível de segurança implementados em nosso sistema de rede. Os níveis de segurança definem o grau de restrição e controle aplicado ao tráfego de rede, garantindo a proteção dos recursos e dados da empresa.

Nível de Segurança Médio

Descrição: Este nível impõe algumas restrições ao tráfego de rede para melhorar a segurança.

Características:

* Algumas portas de entrada podem ser bloqueadas, exceto as essenciais para operações básicas.
* O tráfego de saída para portas não essenciais pode ser bloqueado.
* Endereços IP específicos podem ser bloqueados para mitigar ameaças conhecidas.
* Recomendado para ambientes de produção que requerem um equilíbrio entre segurança e funcionalidade.

**Documentação de Redes - Logging**

Introdução

Este conteúdo descreve a prática de logging implementada em nosso sistema de rede. Logging refere-se ao processo de registrar eventos, ações ou dados relevantes que ocorrem em um sistema de computador ou rede. O registro desses eventos é essencial para monitorar e auditar a segurança e o desempenho da rede.

**Logging na Rede**

Finalidade

**Monitoramento de Segurança**: O logging é usado para identificar e acompanhar atividades suspeitas ou maliciosas na rede, como tentativas de acesso não autorizadas ou tráfego bloqueado pelo firewall.

**Diagnóstico de Problemas**: Os registros de eventos ajudam a identificar e solucionar problemas de rede, como falhas de conexão, erros de configuração ou congestionamento de tráfego.

**Auditoria e Conformidade**: O logging é essencial para atender a requisitos regulatórios e de conformidade, fornecendo uma trilha de auditoria de todas as atividades relevantes na rede.

Tipos de Logs

**Firewall**: Os firewalls podem ser configurados para registrar eventos de rede, como tentativas de acesso não autorizadas, tráfego bloqueado ou permitido, e alterações nas regras de firewall.

**Servidores**: Os logs de servidores podem incluir informações sobre tentativas de login, acessos a arquivos ou diretórios, atividades de serviços e erros de sistema.

**Dispositivos de Rede**: Roteadores, switches e outros dispositivos de rede podem registrar eventos relacionados ao tráfego de rede, status da interface, atualizações de firmware e alterações de configuração.

Formato de Logs

**Registros Estruturados**: O sistemas de registro produzem registros estruturados em formatos como JSON, XML ou CSV, o que facilita a análise automatizada e a integração com sistemas de gerenciamento de logs.

Retenção de Logs

**Política de Retenção**: Uma política de retenção de logs deve ser definida para determinar por quanto tempo os registros serão mantidos. Isso pode ser influenciado por requisitos regulatórios, práticas recomendadas da indústria e necessidades específicas da organização.

**Armazenamento Seguro**: Os registros devem ser armazenados de forma segura para protegê-los contra acesso não autorizado, adulteração ou exclusão acidental. Isso pode incluir o uso de sistemas de gerenciamento de logs dedicados e medidas de segurança de dados.

**Antivírus Integrado ao Firewall**

Introdução

Este conteúdo descreve os recursos de antivírus integrados ao nosso firewall. A integração de funcionalidades de antivírus ao firewall ajuda a fortalecer a segurança da rede, proporcionando uma camada adicional de proteção contra ameaças cibernéticas, como malware, vírus e cavalos de Troia.

Finalidade

**Detecção e Prevenção de Ameaças**: O antivírus integrado ao firewall é projetado para detectar e bloquear ameaças cibernéticas em tempo real, antes que elas possam comprometer os sistemas da rede.

**Proteção Multicamadas**: Combinado com as funcionalidades de firewall, o antivírus oferece uma abordagem multicamadas para proteger a rede contra uma variedade de ameaças, incluindo vírus, worms, spyware e ransomware.

**Redução de Complexidade**: A integração do antivírus ao firewall simplifica a gestão de segurança, reduzindo a necessidade de implantar e gerenciar soluções de segurança separadas.

Configuração e Gerenciamento

**Interface Unificada**: O antivírus é configurado e gerenciado por meio da mesma interface de gerenciamento utilizada para o firewall, proporcionando uma experiência de usuário integrada.

**Relatórios e Logs**: O antivírus integrado registra atividades de detecção e ações tomadas, permitindo que os administradores monitorem e analisem a eficácia da proteção.

**Política de Segurança de Rede**

Introdução

Esta política de segurança de rede define as regras e procedimentos que devem ser seguidos por todos os funcionários, contratados e terceiros que acessam a rede da empresa. O objetivo é proteger os recursos de tecnologia da informação (TI) e os dados confidenciais contra ameaças cibernéticas e garantir a integridade, confidencialidade e disponibilidade das informações.

Regras e Procedimentos

**1. Contas de Usuário**

Todos os usuários devem ter contas de usuário individuais.

As senhas devem ser complexas, exclusivas e alteradas regularmente.

O compartilhamento de contas e senhas é estritamente proibido.

**2. Acesso à Rede**

O acesso à rede é concedido com base na necessidade de trabalho.

O acesso remoto à rede requer autenticação multifatorial.

Dispositivos não autorizados não podem ser conectados à rede corporativa sem aprovação prévia.

**3. Política de Firewall**

O firewall deve ser configurado para controlar o tráfego de entrada e saída.

As regras do firewall devem ser revisadas regularmente e atualizadas conforme necessário.

Somente tráfego essencial para operações de negócios deve ser permitido.

**4. Atualizações de Software**

Todos os sistemas e dispositivos devem ter as atualizações de segurança aplicadas regularmente.

As atualizações automáticas devem ser habilitadas sempre que possível.

A instalação de software não autorizado é estritamente proibida.

**5. Backup de Dados**

Os dados críticos devem ser regularmente salvos e armazenados em locais seguros.

Os backups devem ser testados periodicamente para garantir a sua integridade e recuperação eficaz.

Um plano de contingência de dados deve estar em vigor para lidar com incidentes de perda de dados.

**Política de Proteção de Dados**

Introdução

Esta política de proteção de dados estabelece os princípios e procedimentos que devem ser seguidos para garantir a confidencialidade, integridade e disponibilidade dos dados da rede da empresa. O objetivo é proteger as informações confidenciais e garantir que elas sejam acessadas e utilizadas de maneira segura e responsável.

Princípios de Proteção de Dados

1. Confidencialidade

* Os dados confidenciais só podem ser acessados por pessoal autorizado e para fins legítimos de trabalho.
* A criptografia deve ser usada para proteger dados sensíveis durante a transmissão e armazenamento.
* Informações confidenciais devem ser adequadamente marcadas e classificadas de acordo com sua sensibilidade.

2. Integridade

* Os dados devem ser precisos, completos e atualizados conforme necessário.
* Mecanismos de controle de acesso e prevenção de alterações não autorizadas devem ser implementados.
* Deve-se ter um controle rigoroso sobre as alterações nos dados, garantindo que apenas pessoal autorizado possa modificá-los.

3. Disponibilidade

* Os dados devem estar disponíveis quando necessários para operações comerciais legítimas.
* Devem ser implementadas medidas de segurança para proteger os dados contra interrupções, falhas de sistema e ataques cibernéticos.
* Deve haver um plano de contingência para restaurar rapidamente a disponibilidade dos dados em caso de incidentes.

Procedimentos de Proteção de Dados

1. Controle de Acesso

* O acesso aos dados deve ser baseado no princípio do mínimo privilégio, concedendo apenas as permissões necessárias para realizar as funções do trabalho.
* Senhas fortes e autenticação multifatorial devem ser usadas para proteger o acesso aos sistemas e dados.

2. Criptografia

* Dados confidenciais devem ser criptografados durante a transmissão pela rede e armazenamento em dispositivos.
* Devem ser utilizados algoritmos de criptografia robustos e atualizados para garantir a segurança dos dados.

3. Backup e Recuperação

* Deve ser realizado backup regular de todos os dados críticos e sensíveis.
* Os backups devem ser armazenados em locais seguros e testados periodicamente para garantir sua integridade e recuperação eficaz.

4. Monitoramento e Auditoria

* As atividades de acesso aos dados devem ser registradas e monitoradas para identificar comportamentos suspeitos ou atividades não autorizadas.
* Devem ser realizadas auditorias periódicas para garantir o cumprimento das políticas de proteção de dados e identificar possíveis vulnerabilidades.

**Política de Atualizações de Segurança**

Introdução

Esta política estabelece os procedimentos e as responsabilidades relacionadas à implementação de atualizações de segurança em todos os sistemas e dispositivos da rede da empresa. O objetivo é garantir que todas as correções de segurança mais recentes sejam aplicadas de forma oportuna para proteger os sistemas contra vulnerabilidades conhecidas.

Procedimentos de Atualizações de Segurança

1. Identificação de Atualizações

* A equipe de TI é responsável por monitorar regularmente as fontes de informações sobre atualizações de segurança, incluindo boletins de segurança, alertas de fornecedores e comunidades de segurança.
* Todas as atualizações de segurança relevantes devem ser identificadas e avaliadas quanto à sua importância e impacto potencial nos sistemas e na rede.

2. Priorização e Programação

* As atualizações de segurança devem ser priorizadas com base em seu impacto potencial na segurança dos sistemas e na criticidade dos ativos de TI afetados.
* As atualizações críticas e de alto risco devem ser aplicadas imediatamente, enquanto as atualizações de menor impacto podem ser agendadas conforme a disponibilidade de recursos e o impacto nos sistemas em produção.

3. Teste de Atualizações

* Antes de serem implementadas em ambientes de produção, todas as atualizações de segurança devem ser testadas em ambientes de desenvolvimento ou teste para garantir que não causem problemas de compatibilidade ou falhas nos sistemas.
* Os testes devem abranger cenários de uso típicos e simular possíveis impactos nas funcionalidades dos sistemas e na integridade dos dados.

4. Implementação

* As atualizações de segurança devem ser implementadas por técnicos devidamente treinados e qualificados, seguindo os procedimentos recomendados pelo fornecedor e as melhores práticas da indústria.
* Deve ser mantido um registro detalhado de todas as atualizações aplicadas, incluindo data, hora, sistemas afetados e resultados dos testes.

5. Monitoramento e Verificação

* Após a implementação das atualizações de segurança, os sistemas devem ser monitorados de perto para identificar possíveis problemas ou anomalias relacionadas à atualização.
* Verificações periódicas devem ser realizadas para garantir que todas as atualizações tenham sido aplicadas com sucesso e que os sistemas estejam funcionando conforme o esperado.

**Política de Nomes e Senhas de Login**

Introdução

Esta política estabelece os procedimentos de segurança e as políticas de senha para os nomes de usuário e senhas de login na rede da empresa. O objetivo é garantir que as contas de usuário sejam protegidas adequadamente contra acessos não autorizados e que as credenciais sejam gerenciadas de forma segura e responsável.

Procedimentos e Políticas de Senhas

1. Requisitos de Comprimento de Senha

* As senhas devem ter no mínimo oito caracteres de comprimento.
* Senhas de maior comprimento são encorajadas para aumentar a segurança.
* Os funcionários devem ser incentivados a criar senhas longas e complexas que sejam difíceis de adivinhar.

2. Exigência de Caracteres Especiais

* As senhas devem conter uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
* Caracteres especiais, como !, @, #, $, %, são altamente recomendados para aumentar a complexidade das senhas.

3. Política de Expiração de Senha

* As senhas devem expirar regularmente de acordo com uma política de expiração definida.
* Recomenda-se uma política de expiração de senha de 90 dias, mas isso pode variar dependendo das necessidades específicas da organização.

4. Proibição de Senhas Anteriores

* Os usuários não podem reutilizar senhas anteriores.
* O sistema deve impedir o uso de senhas recentes para garantir a segurança das contas de usuário.

5. Autenticação Multifatorial (MFA)

* A autenticação multifatorial deve ser habilitada sempre que possível para aumentar a segurança das contas de usuário.
* Além da senha, os usuários devem fornecer um segundo fator de autenticação, como um código enviado por SMS ou gerado por um aplicativo de autenticação.

6. Armazenamento Seguro de Senhas

* As senhas devem ser armazenadas de forma segura usando técnicas de hash e salting para proteger contra ataques de força bruta e vazamentos de dados.
* O acesso às senhas armazenadas deve ser restrito apenas aos administradores de sistema autorizados.

7. Educação e Conscientização do Usuário

* Os funcionários devem receber treinamento regular sobre a importância da segurança de senha e as melhores práticas para criar e gerenciar senhas seguras.
* Os usuários devem ser incentivados a relatar imediatamente qualquer suspeita de comprometimento da senha ou atividade não autorizada.

**Procedimentos de Backup e Recuperação**

Formas de Realização dos Procedimentos

1. Backup Regular

Definição de Agenda: Os backups devem ser realizados regularmente de acordo com uma agenda definida, levando em consideração a criticidade dos dados e a frequência de alterações.

Seleção de Dados: Todos os dados importantes, incluindo documentos, bancos de dados, e-mails e configurações do sistema, devem ser incluídos nos backups.

Técnicas de Backup: Podem ser utilizadas técnicas de backup como backup completo, incremental ou diferencial, dependendo das necessidades de proteção e dos recursos disponíveis.

2. Armazenamento Seguro

Local de Armazenamento: Os backups devem ser armazenados em locais seguros, protegidos contra acesso não autorizado, danos físicos e desastres naturais.

Redundância: É recomendável manter cópias de backup em locais geograficamente diferentes para aumentar a resiliência e a disponibilidade dos dados.

Criptografia: Os backups devem ser criptografados durante o armazenamento para proteger os dados contra acesso não autorizado.

3. Testes de Recuperação

Procedimentos de Teste: Devem ser realizados testes regulares de recuperação para garantir a eficácia dos procedimentos de backup e a integridade dos dados.

Simulações de Incidentes: Simulações de incidentes podem ser realizadas para avaliar a capacidade de resposta da equipe de TI e identificar possíveis melhorias nos procedimentos de recuperação.

4. Documentação e Monitoramento

Documentação Detalhada: Todos os procedimentos de backup e recuperação devem ser documentados de forma clara e detalhada para facilitar a implementação e a manutenção.

Monitoramento Contínuo: Deve ser implementado um sistema de monitoramento contínuo para garantir que os backups sejam executados conforme agendado e que os dados sejam protegidos adequadamente.

**Registro de Manutenção da Rede**

Introdução

* Este documento descreve como serão registradas as manutenções realizadas na rede da empresa, incluindo atualizações de software, substituição de hardware e resolução de problemas. O objetivo é manter um histórico detalhado das atividades de manutenção para garantir a integridade, disponibilidade e eficiência da infraestrutura de rede.

Itens a serem Registrados

Os seguintes itens devem constar no registro de manutenção da rede:

1. Identificação do Equipamento

* Nome ou identificação do equipamento ou sistema de rede afetado pela manutenção.

2. Data da Manutenção

* Data e horário em que a manutenção foi realizada.

3. Tipo de Manutenção

* Indicação do tipo de manutenção realizada, como atualização de software, substituição de hardware, resolução de problemas, etc.

4. Descrição do Problema

* Descrição detalhada do problema ou da necessidade que motivou a realização da manutenção.

5. Solução

* Descrição detalhada da solução adotada para resolver o problema ou atender à necessidade identificada.

6. Tempo de Inatividade

* Tempo total de inatividade do equipamento ou sistema durante a execução da manutenção.

7. Custos

* Custos associados à manutenção, incluindo custos de peças de reposição, horas de trabalho da equipe técnica, despesas adicionais, etc.

8. Responsável pela Manutenção

* Nome ou identificação da pessoa responsável pela execução da manutenção.

**Procedimento de Registro**

O registro de manutenção será feito por meio de um sistema de gerenciamento de tickets ou um registro em formato eletrônico ou físico, conforme preferência da equipe de TI.

Cada manutenção será documentada em um registro individual, que será atualizado com as informações relevantes conforme a manutenção é realizada.

Os registros de manutenção serão arquivados e mantidos por um período adequado, conforme requisitos regulatórios e melhores práticas da indústria.