PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

RELATÓRIO TÉCNICO

SEGURANÇA E POLÍTICA:
REDES DE COMPUTADORES

GRUPO

Augusto Henrique Lage

Camila Ferreira Borges

Kener de Almeida Silva

Pedro Henrique Rodrigues da Silva

Sergio de Oliveira Bernardes Nunes

Raynan Rainer Ferreira de Almeida

2023

SUMÁRIO

1 Introdução

A segurança da rede de computadores seja ela em uma empresa de pequeno, médio ou grande porte é um aspecto crítico que deve ter a devida atenção para proteger as informações e recursos tecnológicos contra ameaças cibernéticas.

Segundo o relatório da Kaspersky, empresa internacional de cibersegurança e privacidade digital, os ataques hackers em pequenas e médias empresas Brasileiras cresceram 41% de janeiro a abril de 2022, em comparação ao mesmo período do ano passado. Esse crescimento é alarmante, pois em uma pesquisa da National Cyber Security Alliance em 2017, foi identificado que 60% das empresas médias e pequenas que sofrem um ciberataque fecham as portas 6 meses depois do ocorrido.

As redes de computadores são cada vez mais complexas e interconectadas, tornando-se cada vez mais um alvo atraente para os cibercriminosos. Estes ataques podem causar uma variedade de danos, incluindo roubo de dados, interrupção de serviços, ataques físicos e até mesmo a falência de uma empresa. Abordaremos do decorrer deste documento algumas formas de tentar reduzir estes ataques.

A informação pode existir em diversos formatos tais como: impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio eletrônico e/ou por outros meios eletrônicos, mostrada em filmes ou falada em conversas. Independentemente de sua natureza ou de sua origem, e da forma apresentada, compartilhada e/ou armazenada, ela deve estar protegida de acordo com sua relevância em relação ao negócio das empresas

2 Objetivos

Garantir a confidencialidade, integridade, disponibilidade e legalidade da informação necessária para o negócio.

A implementação dessa política é importante para sustentar e demonstrar a capacidade e integridade em lidar com todas as partes interessadas. Portanto, essa política assegura que:

- As informações estão protegidas contra acesso não autorizado;
- A confidencialidade da informação é mantida;

- As informações não são divulgadas às entidades não autorizadas por meio de ações deliberadas ou descuidadas;
- A integridade das informações é mantida para impedir modificações não autorizadas;
- As informações estão disponíveis para usuários autorizados, quando necessário;
- Requisitos contratuais, de regulamentação e legais são cumpridos;
- Sempre que ocorrer alterações legais, regulamentares ou normativas que impactem o negócio, uma análise crítica é realizada a fim de que as adequações, se necessário, sejam realizadas;
- Os planos de continuidade da atividade são produzidos, mantidos e testados de acordo com as expectativas da gestão;
- Treinamento de segurança da informação e privacidade são dados a todos os colaboradores e, quando aplicável, a provedores externos;
- Potenciais violações de segurança da informação e suspeitas de vulnerabilidades sejam relatadas, investigadas e mitigadas;
- Cada indivíduo tenha conhecimento adequado dos controles de gestão, dos controles operacionais e técnicos que ajudam a proteger os recursos e bens tecnológicos de informação;
- As metas e objetivos são divulgados para as partes interessadas envolvidas, para que cada indivíduo tenha uma compreensão adequada de seu papel e responsabilidade em relação à segurança da informação e à missão da organização;
- As políticas, procedimentos e práticas são comunicados às partes;

3 Dever de todos

I. Zelar pela Segurança da Informação na Empresa/Instituição;
II. Seguir as diretrizes contidas nesta política e demais políticas e procedimentos de segurança da informação;
III. Manter a segurança física de equipamentos e informações;
IV. Participar dos programas de conscientização providos;
V. Informar fragilidades, vulnerabilidades e riscos pertinentes a Segurança da Informação que venham a ter conhecimento;

VI. Acompanhar incidentes e propor melhorias, evitando reincidências de problemas;
VII. Utilizar com responsabilidade e para fins de trabalho e de forma profissional, ética e legal os ativos de tecnologia da informação;
VIII. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
IX. Garantir que os sistemas e informações sob sua responsabilidade estejam protegidos;
X. Comunicar qualquer descumprimento da Política de Segurança da Informação.

4 Requisitos de Segurança

Existe uma série de diretrizes que podem ser seguidas para proteger as redes de computadores contra-ataques. Essas diretrizes incluem:

- Políticas e procedimentos de segurança;
- Implementar tecnologias de segurança;
- Capacitar os usuários;
- Monitorar o ambiente;
- Usar política de se senhas fortes;
- Autenticação de dois fatores (2FA);
- Sistemas atualizados;
- Uso de VPN para conexões remotas;
- Restrições de acesso;
- Backup;
- Antivírus;

4.1 Aspectos importantes

4.1.1 Confidencialidade

Segundo o Princípio da Confidencialidade, a informação pode ser acessada apenas por pessoas autorizadas – isso significa o sigilo da informação. Portanto, a confidencialidade garante o sigilo da informação e impede que pessoas não autorizadas tenham acesso ao conteúdo.

Exemplo de ferramenta: A Criptografia.

É uma técnica que embaralha a informação por meio de algoritmos, e faz com que a informação se transforme em algo ininteligível.

4.1.2 Integridade

De acordo com o Princípio da Integridade, **a informação só pode ser alterada por pessoas autorizadas**, ou seja, a Integridade garante o controle das alterações, impedindo que pessoas não autorizadas façam alterações indevidas na informação. O princípio da integridade também garante a completude da informação, para que não haja perda de partes da informação.

Exemplo de ferramenta: Assinatura Digital e Backup.

Assinatura Digital: Quando o usuário assina digitalmente um documento, qualquer alteração que for feita no documento violará essa assinatura. Portanto, se houver alteração em um documento assinado digitalmente ou eletronicamente, ele precisará ser assinado novamente, pois a assinatura anterior foi violada. A assinatura garante o controle das alterações.

Backup: A completude faz parte do backup. Quando parte da informação se corrompe e o usuário restaura o backup, a totalidade da informação é recuperada, tornando-se íntegra novamente.

4.1.3 Disponibilidade

De acordo com o Princípio da Disponibilidade, a informação estará disponível sempre que for preciso. Esse aspecto é de suma importância, principalmente para sistemas que não podem ficar indisponíveis, pois essas falhas comprometem o serviço.

As ferramentas que garantem o princípio da Disponibilidade são o Nobreak, o Firewall e o Backup.

Nobreak: Dispositivo alimentado por baterias, capaz de fornecer energia elétrica a um sistema durante um determinado período, em situações de emergência, no caso de

interrupção do fornecimento de energia da rede pública. Ou seja, o Nobreak impede que o sistema desligue e é uma ferramenta de Disponibilidade.

Firewall: O Firewall é uma barreira de proteção e um dispositivo indispensável dentro de uma organização. Ele impede que ataques de intrusão e de negação de serviço sejam efetuados no ambiente.

Backup: Quando uma informação é corrompida, ela se torna indisponível. O backup recupera essa informação, tornando-a disponível novamente.

4.1.4 Autenticidade

O Princípio da Autenticidade garante a veracidade da autoria da informação, porém, não garante a veracidade do conteúdo da informação. A autenticidade garante a veracidade do autor, de quem de fato produziu aquela informação, não importando se o conteúdo é verdadeiro ou falso.

Não Repúdio: A Autenticidade garante também um subproduto, que é o Não Repúdio. ***O Não Repúdio está contido na autenticidade e significa que o autor da informação não tem como negar que ele é o verdadeiro autor.***

Ferramentas que garantem o Princípio da Autenticidade

Biometria: A Biometria é uma ferramenta que verifica algumas características físicas da pessoa para certificar que aquela característica identifica a pessoa unicamente. A Biometria é muito utilizada nos bancos.

Assinatura Digital: A assinatura digital identifica unicamente o autor da informação, garantindo a autenticidade.

Certificados Digitais: Os certificados Digitais garantem a autenticidade da autoria dos sites. Ex.: Quando um usuário acessa um site de comércio eletrônico, geralmente há um cadeado no canto da tela, que mostra o certificado digital do site, afirmando que aquele site de fato pertence àquela empresa.

5. Política de Segurança

Estabelecer diretrizes para garantir a segurança das informações corporativas, buscando o equilíbrio entre performance e confiabilidade, objetivando a perenidade dos negócios da empresa/instituição, fundamentadas nos seguintes itens:

5.1 Gerenciamento de Acesso

A equipe de TI é responsável por atribuir, modificar e revogar direitos de acesso de acordo com a aprovação e a política da empresa.

Revisões regulares das permissões de acesso serão realizadas para garantir que os usuários ainda tenham apenas o acesso necessário para realizar suas funções.

5.2 Responsabilidades do Usuário

Os usuários são responsáveis por manter suas credenciais de acesso seguras e não devem compartilhá-las com outros indivíduos.

Os usuários devem seguir as práticas de segurança definidas pela empresa, incluindo a utilização de senhas fortes e a adoção de medidas de proteção contra malware.

5.3 Monitoramento e Auditoria

A atividade de acesso à rede pode ser monitorada para fins de auditoria e detecção de atividades suspeitas, é nesse ponto que a contratação de um bom serviço de proteção de end-point se torna o principal aliado, trazendo logs e relatórios sobre a atividade do usuário.

A violação desta política ou tentativas de acesso não autorizado podem resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho.

5.4 Métodos de Autenticação

Definir os métodos de autenticação a serem utilizados para proteger o acesso aos sistemas e recursos de tecnologia da informação.

a) **Senha:** Todos os usuários devem ter uma senha única e forte para acessar os sistemas. Senhas devem seguir as seguintes diretrizes:

- ✓ Ter no mínimo 8 caracteres.
- ✓ Incluir pelo menos uma letra maiúscula e uma letra minúscula.
- ✓ Incluir pelo menos um número.
- ✓ Incluir pelo menos um caractere especial (ex: !, @, #, $, etc.).
- ✓ Senhas devem ser alteradas a cada 90 dias.
- ✓ Senhas antigas não podem ser reutilizadas.

As senhas devem ser mantidas confidenciais e não compartilhadas com outros usuários.

b) **Autenticação Multifator (MFA):** Para acesso a sistemas e recursos críticos, a autenticação multifator é obrigatória. Isso inclui, pelo menos, dois dos seguintes fatores:

- ✓ Algo que você sabe: Senha ou PIN.
- ✓ Algo que você possui: Token de autenticação, aplicativo de autenticação móvel, cartão inteligente.
- ✓ Algo que você é: Biometria (impressão digital, reconhecimento facial etc.).

c) **Certificados Digitais:** Para acessar recursos especialmente sensíveis, o uso de certificados digitais pode ser requerido. Esses certificados devem ser emitidos e gerenciados pela equipe de TI da [Nome da Empresa].

d) **Autenticação por Token**: Alguns usuários poderão usar dispositivos de token físico ou aplicativos de autenticação móvel para autenticar o acesso. Esses tokens geram códigos únicos que são inseridos junto com a senha.

5.5 Treinamento e Conscientização

a) **Conscientização:** Os usuários serão capacitados sobre a importância de senhas fortes e práticas de segurança de senhas por meio de treinamentos regulares de segurança da Informação além da divulgação dos comunicados encaminhados via e-mail.

b) **Melhores Práticas:** Os usuários receberão orientações sobre como criar senhas seguras e como protegê-las para que possam pôr em prática.

c) **Testes de Capacitação:** Podem ser feitos na admissão do funcionário para atestar a capacidade de adaptação aos sistemas e ferramentas internas reduzindo assim a chance de algum erro operacional. Os treinamentos também podem ser realizados sempre que a empresa perceber que é necessário reforçar a

conscientização dos funcionários ou quando houver alteração de funções e remanejamento de funcionários.

d) **Trabalho em conjunto:** É de suma importância a parceria com outros setores como Marketing, RH e Jurídico para o desenvolvimento de ações de divulgação, conscientização e confecção de regras e penalidades por violações de segurança, por exemplo, trabalhar junto ao Marketing para desenvolver comunicados de alterações ou atualizações nas regras de segurança via cartazes/banners, hotspot ou newsletters. O Jurídico pode ajudar no desenvolvimento de termos de responsabilidade/confidencialidade e na aplicação de sanções legais quanto a violação de leis e de protocolos internos e o RH na conscientização dos colaboradores já no primeiro contato com a empresa.

Todos os usuários serão treinados na correta utilização dos métodos de autenticação, incluindo a importância de manter suas senhas confidenciais e adotar práticas de segurança adequadas.

5.6 Monitoramento e Melhoria Contínua

Esta política será revisada anualmente para garantir a sua relevância e eficácia. Alterações na política serão comunicadas a todos os usuários e aprovadas pela alta direção.

Esta política de acesso à rede é um exemplo genérico e deve ser adaptada às necessidades, regulamentos e características específicas da organização em questão. Ela serve como um guia para estabelecer diretrizes claras para o acesso à rede, a fim de garantir a segurança e o uso apropriado dos recursos de TI.

A eficácia dos métodos de autenticação será periodicamente avaliada pela equipe de TI.

Serão realizados testes de penetração para avaliar a resistência dos métodos de autenticação a ataques.

Novos ataques surgem constantemente e é importante repassar essas informações aos colaboradores, principalmente da equipe de TI. Por isso a atualização constante é uma parte fundamental, afinal há sempre novas estratégias sendo criadas por cibercriminosos. Deve ser compartilhado com os colaboradores dicas periodicamente, a parceria com empresas especializadas para a realização de treinamentos e certificação também é um dos meios de preparação da equipe diante da apresentação de novos modelos de ameaças

como, por exemplo, spear phishing e maneiras de como identificar links e-mails mal-intencionados.

5.7 Conformidade com Regulamentos

Garantir que a política de métodos de autenticação esteja em conformidade com regulamentos de segurança de dados e outras leis aplicáveis.

Esta política de métodos de autenticação é um exemplo que pode ser adaptado para atender às necessidades e regulamentos específicos da organização. A segurança da autenticação é crucial para proteger os sistemas e recursos da empresa contra ameaças internas e externas.

REFERÊNCIAS

- PSI-002 – Política de Segurança da Informação Pública
- NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos.
- NBR ISO/IEC 27002:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação.
- NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes.
- Lei nº 13.709/2018 – LGPD (Lei Geral de Proteção de Dados Pessoais).
- ISO 27000, Lei Nº 9.609