Política de Segurança da Informação

Versão	Data da versão	Mudanças executadas
2.0	09/07/2021	Colocado o conteudo para o item de comprometimento dos gestores, conforme as melhores práticas e necessidades verificadas para que os gestores possam conhecer e responder pelas políticas.

Empresa: NAI Informática e Consultoria Sociedade Limitada

Política de Segurança da Informação - Geral

1 - Introdução

A Tecnologia da Informação, TI, está cada dia mais presente nas empresas, mudando radicalmente os hábitos e a maneira de comunicação, sendo de vital importância a definição de normas de segurança que visem disciplinar o uso da tecnologia. **NBR ISO/IEC 27.001 principal objetivo documentar e proteger as informações** FJ REDEmpresa **Elaboração de Política de Segurança da Informação** estrutura de rede
Garante a proteção das informações entre clientes e empresa nos aspectos de confidencialidade, integridade e disponibilidade.

Confidencialidade Integridade Disponibilidade FJ REDEmpresa
Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais, (Lei nº 9610).

FJ REDEmpresa

2 - Comprometimento dos usuários

Em todos os pontos de conexão entre a rede interna e uma rede externa insegura (como a Internet), medidas eficazes, como um firewall, devem ser implementadas para garantir que apenas o tráfego de rede autorizado seja permitido.

Sempre que possível, várias camadas de proteção serão usadas para garantir que a falha de um único dispositivo não exponha a rede a ataques. Por exemplo, firewalls de rede (por exemplo, em um roteador) serão complementados por firewalls de software baseados em host em servidores e computadores clientes, a fim de fornecer vários níveis de proteção de firewall.

Os servidores que devem ser acessados da Internet (como servidores da Web) devem ser conectados a uma área separada do firewall (conhecida como Zona Desmilitarizada ou DMZ) para fornecer proteção adicional para a rede interna.

Quando as informações devem ser transferidas por uma rede pública como a Internet, técnicas de criptografia fortes devem ser usadas para garantir a segurança dos dados transmitidos.

O acesso a redes sem fio deve ser protegido por uma senha forte. Uma rede sem fio para convidados pode ser fornecida para os visitantes. Isso deve ser fisicamente separado de todas as redes internas (incluindo redes sem fio internas) e protegido por um firewall.

A capacidade de conectar dispositivos a uma rede sem fio usando o botão WPS (WiFi Protected Setup) no ponto de acesso ou roteador em si deve ser desabilitada.

As senhas de logon do administrador do ponto de acesso sem fio devem sempre ser alteradas do padrão para uma senha forte.

Os equipamentos de rede em escritórios remotos serão alojados em gabinetes seguros, que devem estar sempre

trancados.

Os pontos de acesso sem fio localizados em áreas públicas devem ser ocultados da vista sempre que possível e devem ser colocados em posições onde o acesso do público seja difícil, por exemplo, dentro ou perto do teto. Um invólucro de proteção com chave deve ser instalado onde um ponto de acesso está localizado em uma área pública desprotegida, por exemplo, um parque de estacionamento.

Onde houver necessidade de acesso remoto pela Internet à rede interna, será usada uma Rede Privada Virtual (VPN). A autenticação de dois fatores (por exemplo, usando um aplicativo de telefone ou uma mensagem de texto) deve ser usada para que o conhecimento de uma senha por si só não seja suficiente para obter acesso. O acesso remoto deve ser concedido “conforme necessário”, e não para todos os usuários por padrão.

As senhas de administrador para dispositivos de rede devem ser alteradas na instalação do dispositivo para uma senha forte de pelo menos oito caracteres. O acesso às configurações do roteador e do firewall na Internet deve ser restrito a endereços IP definidos ou usando autenticação de dois fatores ou, quando disponível, ambos. Esse acesso deve ser apoiado por um caso de negócios documentado que seja aprovado pela administração.

Sempre que possível, uma única política de fornecedor será usada para hardware de rede. Uma exceção será feita quando o uso de hardware de vários fornecedores pode aumentar o nível de segurança fornecido, por exemplo, usando dois firewalls diferentes.

O roteamento de rede será baseado em roteadores [insira o fabricante, por exemplo, Cisco]. [Insira o fabricante, por exemplo, Cisco] Switches Gigabit serão usados como padrão para conectar dispositivos à rede. As portas do switch serão configuradas para serem desabilitadas até que sejam necessárias. Dispositivos de rede mais básicos, como hubs, não serão usados devido às suas fragilidades de segurança inerentes.

O protocolo de rede IPv4 (Internet Protocol Version 4) será usado nas redes internas.

As métricas aqui elencadas inclui todos os dispositivos de comunicação sem fio capazes de transmitir dados de pacotes (por exemplo, computadores pessoais, telefones sem fio, telefones inteligentes, etc.) conectados a qualquer uma das redes internas da NAI-IT. Dispositivos sem fio e/ou redes sem qualquer conectividade com as redes da NAI-IT não se enquadram na alçada desta política.

Todos os dispositivos sem fio ponto a ponto (building-to-building) devem usar produtos de fornecedores aprovados pela NAI-IT e configurações de segurança. Um método de criptografia de dados, que atenda ou exceda o padrão de Tecnologia da Informação, é necessário.

Todos os pontos de acesso sem fio e estações base devem ser registrados e aprovados pela Tecnologia da Informação. Todo o acesso lan sem fio deve usar produtos de fornecedores aprovados pela cidade e configurações de segurança. Um método de criptografia de dados, que atenda ou exceda o padrão de Tecnologia da Informação, é necessário. A autenticação do cliente deve ser realizada usando um método de autenticação de dois fatores.

Todas as placas de interface de rede sem fio (NIC) (ou seja, cartões PC) usadas em laptops da cidade ou computadores desktop devem ser registradas e aprovadas pela Information Technology. Se um dispositivo móvel contiver um NIC LAN e nic sem fio, o NIC sem fio deve ser desativado enquanto o dispositivo estiver conectado à rede interna através da LAN NIC.

3 - Comprometimento dos gestores

Confidencialidade

A informação só pode ser acessada e atualizada por pessoas autorizadas e devidamente credenciadas. Dados e informações importantes de alguns setores ou clientes jamais podem ser acessados por terceiros estranhos à corporação.

Devem haver mecanismos de segurança de tecnologia da informação (TI) capazes de impedir que pessoas não autorizadas acessem informações confidenciais, seja por engano ou por má-fé.

Confiabilidade

Política de Segurança da Informação

É o caráter de fidedignidade da informação. Deve ser assegurada ao usuário a boa qualidade da informação com a qual ele estará trabalhando.

Integridade

É a garantia de que a informação estará completa, exata e preservada contra alterações indevidas, fraudes ou até mesmo contra a sua destruição.

Assim, são evitadas violações da informação, sejam elas de forma acidental ou mesmo proposital.

Disponibilidade

É a certeza de que a informação estará acessível e disponível em escala contínua para as pessoas autorizadas.

Hoje em dia, os mecanismos de acesso remoto tornam possível a disponibilidade da informação de qualquer lugar em que o usuário esteja no planeta e a qualquer hora do dia ou da noite.

Autenticidade

É saber, por meio de registro apropriado, quem realizou acessos, atualizações e exclusões de informações, de modo que haja confirmação da sua autoria e originalidade.

Como vimos, todos os aspectos da segurança da informação precisam estar em vista e serem tratados com o máximo de critério e cuidado para que os gestores e colaboradores da empresa sejam beneficiados, assim como os públicos externos — parceiros e clientes — que interagem com ela.

---

4 - Histórico de versões

Versão	Descrição	Data da revisão	Próxima revisão	Revisor / Aprovador
1.0	Versão inicial da política de segurança	10/06/2021	30/06/2021	Norberto Tordin

Aprovado por	Análise do aprovador	Data da análise
Norberto Tordin 2	ok. De acordo.....	
Norberto Tordin		
Norberto Tordin 1	ok.....	

Versão	Descrição	Data da revisão	Próxima revisão	Revisor / Aprovador
2.0	Revisão para conter novos tópicos definidos	09/07/2021	09/07/2022	Norberto Tordin 1

Aprovado por	Análise do aprovador	Data da análise
Andre Neves Lima		