



Elaboração de Políticas de Segurança Eficazes para Pequenas Empresas



Introdução

Políticas de Segurança são fundamentais para proteger os ativos de uma pequena empresa. Neste slide, discutiremos a importância de elaborar estratégias eficazes que garantem a **integridade**, a **confidencialidade** e a **disponibilidade** das informações. O objetivo é proporcionar um ambiente seguro para operações e dados sensíveis.



Identificação de Riscos

O primeiro passo na **elaboração de políticas de segurança** é a **identificação de riscos**. É essencial analisar as ameaças potenciais que podem afetar a empresa, como **ciberataques**, **fraudes** e **erros humanos**. Uma análise detalhada ajuda a priorizar as áreas que precisam de atenção imediata.



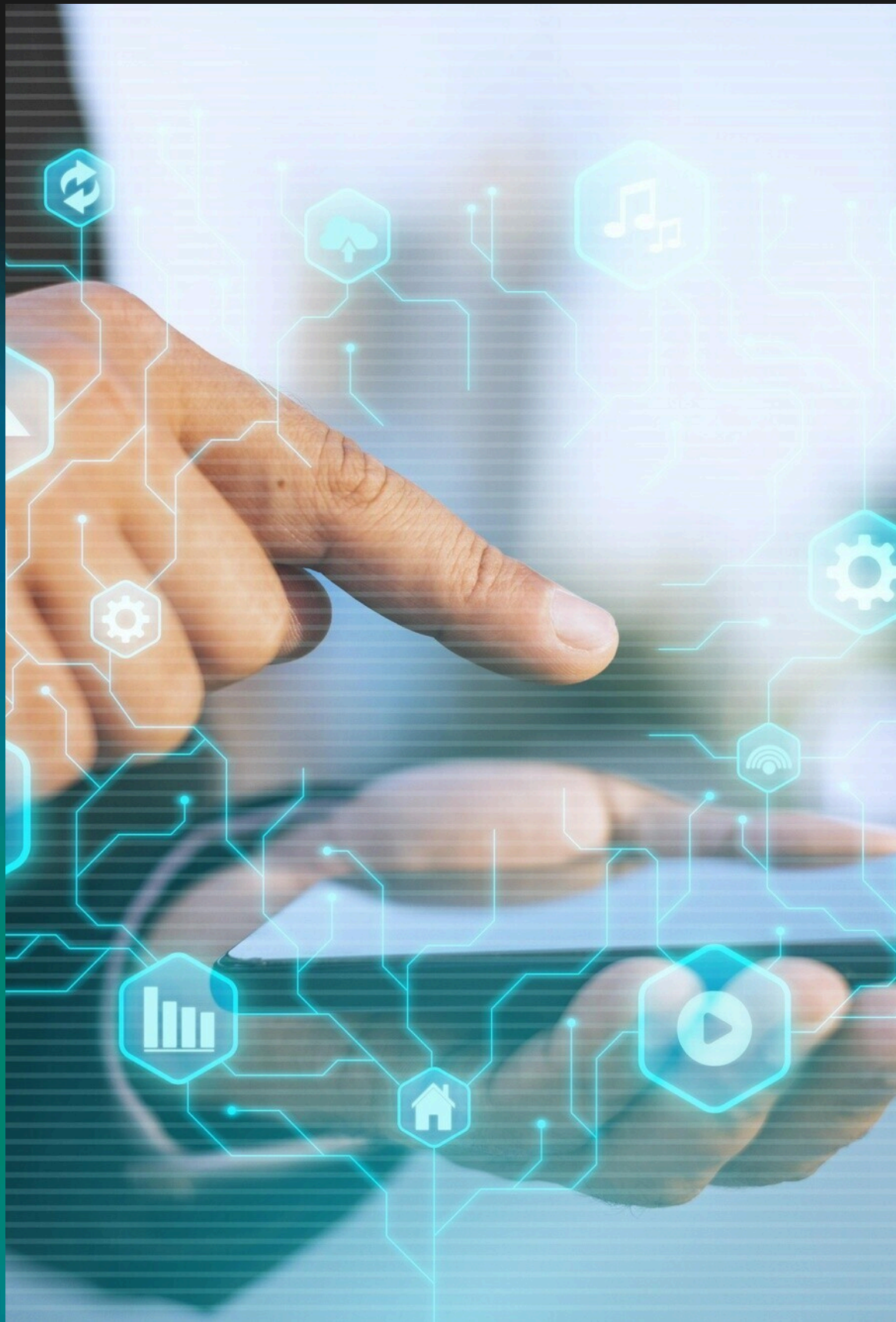


Acesso e controle de usuários.

Para melhorar o controle de acesso de usuários, as seguintes medidas podem ser implementadas:

1. **Classificação de Acesso:** Definir níveis de acesso com base nas funções dos colaboradores.
2. **Autenticação Forte:** Implementar autenticação de dois fatores (2FA) para usuários com acesso a informações sensíveis.
3. **Gestão de Identidade:** Utilizar um sistema que facilite a criação e revogação de acessos.
4. **Treinamento Contínuo:** Oferecer treinamento regular em segurança da informação.





Acesso e controle de usuários.

- 5. **Monitoramento e Registro:** Implementar soluções que registrem acessos e atividades, permitindo auditorias.
- 6. **Revisões Periódicas:** Realizar revisões das permissões de acesso para garantir que estejam atualizadas.
- 7. **Segurança Física:** Controlar o acesso físico a áreas sensíveis.
- 8. **Políticas de Senhas:** Estabelecer políticas para senhas fortes e troca regular.



Para melhorar a política de uso de dispositivos móveis e rede, utilizaremos as seguintes medidas:



Diretrizes para Dispositivos Móveis.

- Autenticação: Dispositivos devem ter senhas fortes e autenticação multifator (MFA).
- Criptografia: Dados sensíveis devem ser criptografados nos dispositivos.
- Atualizações: Manter sistemas e apps sempre atualizados.
- Aplicativos: Somente apps aprovados pela TI podem ser instalados.
- Perda/Roubo: Comunicar imediatamente qualquer perda ou roubo de dispositivos à TI para bloqueio remoto.



Para melhorar a política de uso de dispositivos móveis e rede, utilizaremos as seguintes medidas:



Diretrizes para Redes.

- Redes Wi-Fi: É proibido usar redes públicas para acessar os sistemas da empresa. Usar VPNs seguras.
- Segmentação de Redes: Redes internas devem ser separadas para minimizar riscos.
- Monitoramento: Tráfego de rede deve ser monitorado e logs analisados pela TI.
- Acesso Remoto: Acesso remoto só com ferramentas autorizadas e MFA.
- Treinamento e Consequências:
Conscientização: Treinamento regular sobre segurança para todos os funcionários.
Consequências: Não seguir a política pode resultar em sanções, incluindo demissão.



Políticas de backup



Objetivo: Garantir a segurança e integridade dos dados da clínica, em conformidade com a LGPD.

Dados Protegidos: Todos os dados da clínica, incluindo informações de pacientes, profissionais e financeiras.

Frequência:

- Diária: Backups diferenciais.
- Semanal: Backups completos.
- Mensal: Cópia em armazenamento externo.



Políticas de backup



Armazenamento: Disco rígido externo criptografado e nuvem segura.

Testes: Restauração mensal de arquivos aleatórios e teste anual completo.

Recuperação: Plano detalhado com responsabilidades definidas.

Retenção: Conforme LGPD e necessidades da clínica.

Segurança: Criptografia, controle de acesso e mecanismos de autenticação.

LGPD: Consentimento, transparência, segurança e direitos dos titulares.



Políticas de backup



Considerações Adicionais:

- Inativação de dados de pacientes inativos.
- Documentação atualizada.
- Consultoria especializada e software de backup.
- Testes de intrusão.

Em resumo: A política visa proteger os dados da clínica, garantindo a sua disponibilidade e integridade, em conformidade com a legislação vigente.

Pontos-chave:

- Frequência: Backups diários, semanais e mensais.
- Armazenamento: Local e nuvem.
- Segurança: Criptografia e controle de acesso.
- LGPD: Cumprimento integral.
- Testes: Verificação regular da integridade dos backups



Recuperação de Desastres



Procedimentos:

- **Notificação:** Informar o responsável pela TI e gestores em caso de incidente.
- **Avaliação:** Analisar a extensão do dano.
- **Ativação do plano:** Seguir o plano de recuperação detalhado.
- **Restauração:** Utilizar os backups mais recentes.
- **Verificação:** Confirmar a integridade dos dados restaurados.
- **Documentação:** Registrar todo o processo.

Plano de Recuperação:

- **Responsabilidades:** Definir quem faz o quê.
- **Procedimentos detalhados:** Passo a passo para cada fase.
- **Contatos de emergência:** Lista atualizada.
- **Testes:** Simulações regulares.



Recuperação de Desastres



Testes:

- Frequência: Anualmente, pelo menos.
- Escopo: Restauração de sistemas críticos e grandes volumes de dados.

Documentação:

- Manter: Documentos relacionados à recuperação por um período definido.

Treinamento:

- Capacitação: Treinar colaboradores.
- Simulações: Simular incidentes.



Recuperação de Desastres



Revisão:

- Periodicidade: Anual ou quando houver mudanças.

Considerações:

- LGPD: Conformidade com a lei.
- Segurança: Proteção dos dados durante a recuperação.
- Comunicação: Transparência com todos os envolvidos.

Recomendações:

- Software de backup: Automatizar o processo.
- Armazenamento offsite: Cópias em local remoto.
- Plano de continuidade de negócios: Integração com outros planos.



Recuperação de Desastres



Em resumo: A política garante a recuperação dos dados da clínica em caso de incidentes, com procedimentos claros e testes regulares.

Para uma política mais personalizada, forneça informações sobre:

- Sistemas mais críticos.
- Tempo máximo de inatividade tolerável.
- Ameaças à segurança.
- Orçamento

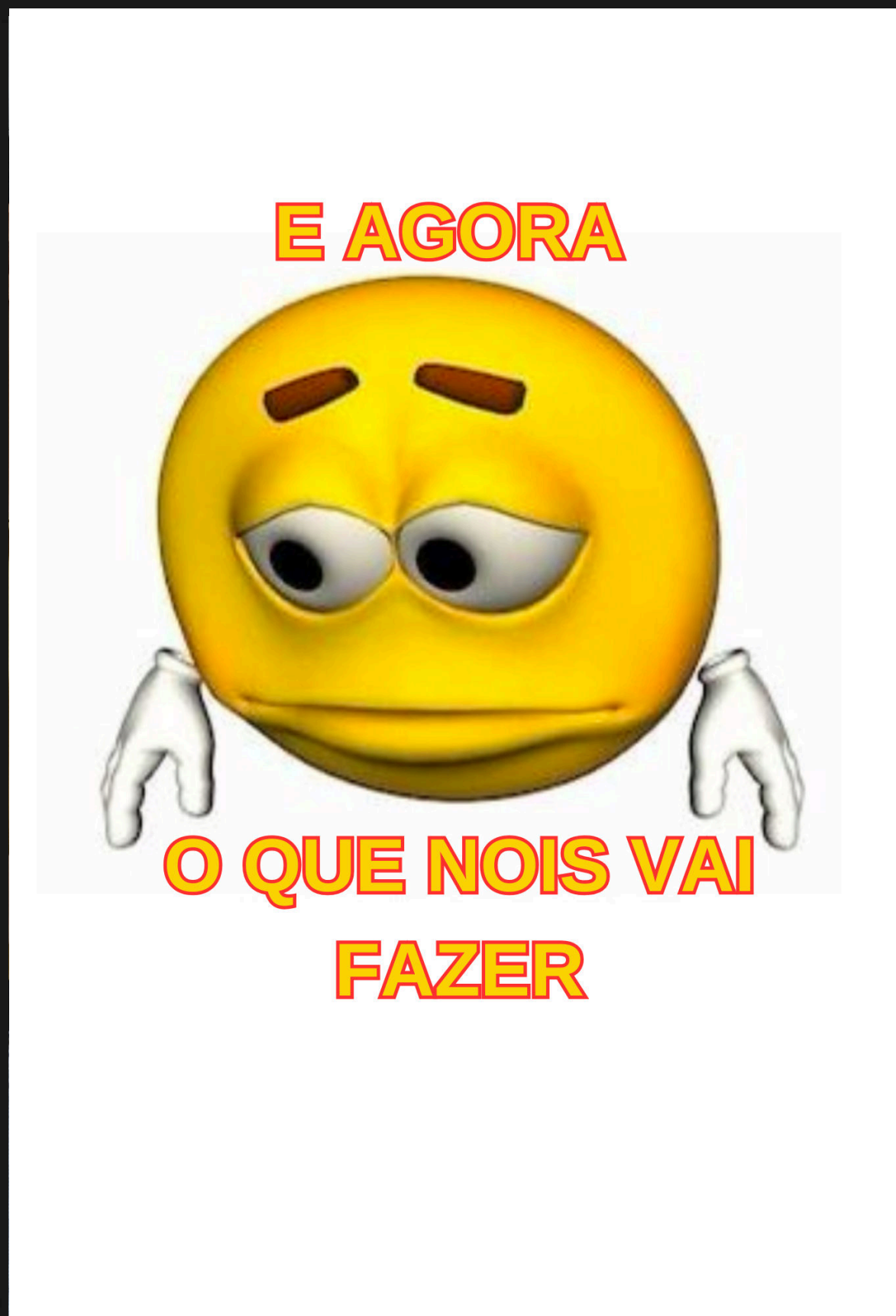


Diretrizes para resposta a incidentes de segurança



Definição: Estabelecer o que constituiu o incidente, e de que forma (um acesso não autorizado)

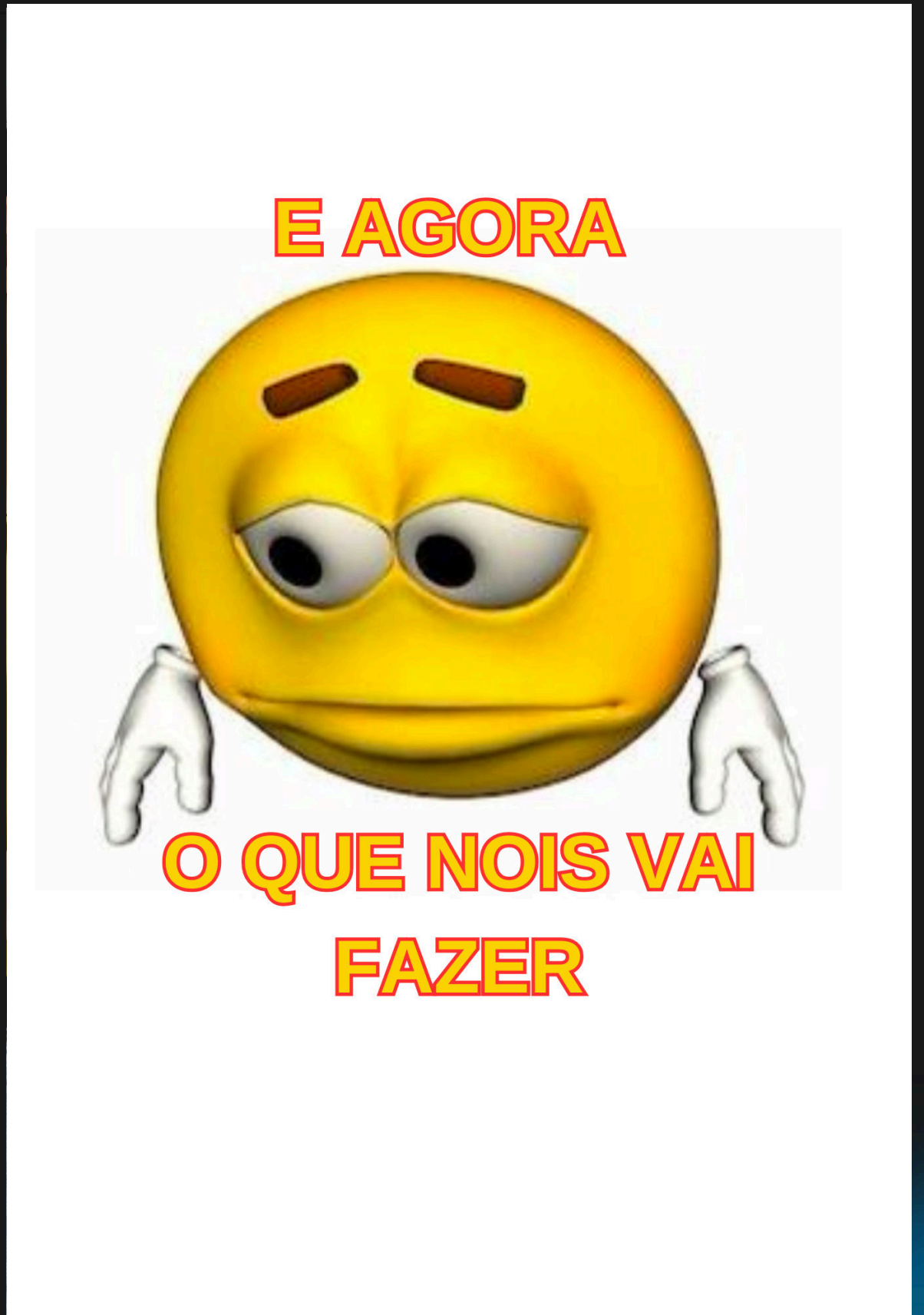
- **Monitoramento:** Implementar ferramentas para detectar atividades suspeitas, como acessos naturais aos sistemas.
- **Nível de Severidade:** Avaliar o impacto e a urgência do incidente.
- **Tipo de dados:** identificar se dados sensíveis, como informações de pacientes foram afetados.
- **Interna:** Informar imediatamente a equipe responsável pela segurança da informação.
- **Externa:** Se necessário, notifique os clientes afetados e as autoridades competentes em conformidade com as leis de proteção de dados LGPD
- **Isolamento:** Contenham o incidente para evitar mais danos, como desconectar sistemas comprometidos



Diretrizes para resposta a incidentes de segurança



- **Prevenção:** Tomar medidas para evitar que o incidente se repita, assim o eliminando pela raiz
- **Investigação:** Coletar informações sobre como o incidente ocorreu e quais dados foram comprometidos.
- **Documentação:** Registrar todos os passos tomados durante a resposta ao incidente.
- **Restaurar Sistemas:** Reverter para backups seguros ou reparar sistemas afetados.
- **Acompanhamento:** Monitorar os sistemas após o incidente para garantir que a situação foi completamente resolvida.
- **Análise Pós Incidente:** Reunir uma equipe para discutir o que aconteceu e como a resposta pode ser melhorada.
- **Atualização de Protocolos:** Revise e atualize políticas e procedimentos de segurança com base nas lições aprendidas.



Diretrizes


As políticas de segurança não são estáticas; elas precisam de **monitoramento e revisão** contínuos. É fundamental avaliar regularmente a eficácia das políticas implementadas e ajustar conforme necessário. Isso garante que a empresa permaneça protegida contra novas ameaças e vulnerabilidades.





Conclusão

Em resumo, a **elaboração de políticas de segurança eficazes** é vital para a proteção das pequenas empresas. Ao identificar riscos, desenvolver políticas claras, treinar funcionários e monitorar continuamente, as empresas podem criar um ambiente seguro e resiliente contra ameaças. A segurança é uma responsabilidade compartilhada.



Obrigado por sua atenção!

Samuel Costa - 824147380
João Pedro - 82427029
Guilherme Teixeira - 824212194

