POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

TechSolutions Contabilidade Ltda

SUMÁRIO

---

1. INTRODUÇÃO

1.1 Por que este documento é importante?

Este documento foi criado para ajudar a TechSolutions Contabilidade a proteger as informações dos seus clientes e evitar problemas de segurança. Escritórios de contabilidade lidam com dados muito sensíveis como declarações de imposto, informações bancárias e documentos pessoais dos clientes, por isso a segurança precisa ser levada a sério.

1.2 Para quem são essas regras?

Estas políticas valem para todos que trabalham na empresa: - Contadores e auxiliares - Estagiários - Secretárias - Prestadores de serviço - Qualquer pessoa que tenha acesso aos computadores e sistemas da empresa

1.3 Objetivo?

- **Confidencialidade**: Só pessoas autorizadas vejam informações sensíveis
- **Integridade**: Os dados não sejam alterados indevidamente
- **Disponibilidade**: Os sistemas funcionem quando precisarmos deles
- **Conformidade Legal**: Seguir a LGPD e outras leis

---

2. POLÍTICA DE ACESSO E CONTROLE DE USUÁRIOS

2.1 O que é isso?

São as regras sobre quem pode acessar o quê dentro da empresa. É importante controlar isso para evitar que informações caiam nas mãos erradas.

2.2 Objetivo:

Garantir que apenas pessoas autorizadas tenham acesso às informações e sistemas da empresa, prevenindo acessos indevidos e vazamentos de dados confidenciais.

2.3 Políticas:

1. Cada funcionário terá um login único e senha pessoal, não devendo compartilhar credenciais com terceiros.
2. Senhas devem ter no No mínimo 12 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais, e devem ser alteradas a cada 90 dias.
3. O acesso aos sistemas será concedido conforme a função do usuário (princípio do menor privilégio). Por exemplo, funcionários da contabilidade não terão acesso às informações de RH.
4. Para sistemas importantes, usar autenticação em duas etapas (recebe código no celular)
5. Todos os acessos aos sistemas críticos serão auditados e monitorados para identificar atividades suspeitas.

2.4 Exemplo de Privilégios

Contador Responsável: - Acessa todos os clientes - Assina documentos digitalmente - Usa certificados digitais

Assistente Contábil: - Acessa só os clientes que está cuidando - Não tem acesso a certificados digitais - Pode consultar mas não alterar certas coisas

Auxiliar Administrativo: - Acesso limitado a tarefas específicas (ex: só folha de pagamento) - Não vê informações financeiras estratégicas

Estagiário: - Acesso supervisionado - Só pode ver, não pode alterar - Acesso bloqueado a informações mais sensíveis

2.5 Justificativas:

- Se todo mundo usa a mesma conta, fica impossível saber quem fez o quê. Com contas individuais, dá pra rastrear ações e ter responsabilidade.

- Senhas fracas são fáceis de descobrir. Hackers usam programas que tentam milhões de combinações por segundo. Uma senha forte dificulta muito esse tipo de ataque. A autenticação em duas etapas adiciona uma camada extra de proteção - mesmo que alguém descubra sua senha, ainda vai precisar do código do seu celular.
- É o princípio do "menor privilégio" - dar só o acesso necessário. Se alguém tem acesso a tudo e essa conta é invadida, o estrago é muito maior. Limitando acessos, limitamos os danos potenciais
- Utilização de autenticação de 2 fatores é uma camada a mais de proteção contra invasores.

2.6 Boas Práticas do Dia a Dia

Regras simples mas importantes: - Nunca anotar senha em papel ou deixar grudado no monitor - Bloquear o computador quando se levantar (Windows + L) - Não deixar documentos sensíveis na mesa ao final do dia - Não compartilhar sua senha com ninguém, nem com o chefe - Não usar a mesma senha em vários lugares - Desconfiar de e-mails pedindo senha ou dados pessoais

---

3. POLÍTICA DE USO DE DISPOSITIVOS MÓVEIS E REDES

3.1 O que é isso?

São as regras sobre como usar celulares, tablets, notebooks e a internet da empresa de forma segura.

3.2 Objetivo:

Garantir que dispositivos móveis e conexões de rede sejam usados de forma segura, protegendo dados corporativos e de clientes.

3.3 Políticas:

1. Dispositivos móveis corporativos (celulares, laptops) devem ter senha de acesso, criptografia de dados e antivírus atualizado. Não Instalar produtos piratas.
2. Não Instalar produtos piratas, conectar pendrives ou hds desconhecidos e avisar imediatamente sobre perda ou roubo do aparelho.
3. Redes Wi-Fi externas (cafés, aeroportos) só podem ser usadas com VPN corporativa ativa.
4. O acesso à rede interna da empresa é permitido apenas para dispositivos autorizados e com políticas de segurança aplicadas.

5. Usar só o e-mail corporativo para assuntos de trabalho. Não mandar informações de clientes para seu e-mail pessoal .Cuidado com anexos de e-mails desconhecidos .Se receber e-mail suspeito pedindo senha, avisar a TI

6. 3 redes diferentes:

   Rede dos Funcionários:

   - Senha forte que muda a cada 3 meses
   - Acessa impressoras, servidores e sistemas internos
   - Só funcionários ativos conhecem a senha

   Rede de Visitantes/Clientes:

   - Senha simples que muda toda semana
   - Só acessa internet, nada interno
   - Separada da rede principal

   Rede dos Equipamentos (Câmeras, Impressoras):

   - Isolada das outras
   - Evita que impressora hackeada vire porta de entrada

3.4 Justificativas:

- Se alguém roubar um notebook sem proteção, pode acessar todos os documentos dos clientes. Com criptografia, mesmo roubando o aparelho, os dados ficam inacessíveis. Antivírus protege contra vírus que podem roubar informações.
- Uso de produtos piratas podem conter vírus ou trazer problemas judiciais de direito autorais para empresa
- Wi-Fi de aeroporto, café ou hotel é super inseguro. Qualquer hacker amador consegue interceptar dados. Com VPN, mesmo que alguém esteja espionando a rede, só vai ver dados criptografados inúteis.
- Usar conta pessoal do Google Drive para guardar arquivos de clientes, quando sair da empresa não dá pra apagar. Além disso, nuvens pessoais não têm os mesmos controles e backups das corporativas.
- Se um cliente na recepção conectar na mesma rede que os funcionários, ele pode tentar acessar nossos arquivos. Separando as redes, cada um fica na sua área sem risco de cruzar.

---

4. DIRETRIZES PARA RESPOSTA A INCIDENTES DE SEGURANÇA

4.1 O que é um incidente de segurança?

É qualquer coisa que ameace a segurança das informações da empresa ou dos clientes. Exemplos: - Vírus no computador - Conta invadida - Perda de notebook com dados de clientes - E-mail suspeito que alguém clicou - Arquivo apagado acidentalmente - Sistema parou de funcionar - Vazamento de informação de cliente

4.2 Objetivo:

Estabelecer um procedimento claro para identificar, comunicar e mitigar incidentes de segurança de forma rápida e eficiente.

4.3 Níveis de Gravidade

CRÍTICO - Resposta imediata (urgentíssimo!): - Ransomware (vírus que sequestra arquivos) - Vazamento de dados de vários clientes - Sistema parado em época de entrega de declaração - Certificado digital sendo usado por outra pessoa

ALTO - Responder em 4 horas: - Notebook roubado com dados de clientes - Vírus detectado mas controlado - Vazamento de dados de um cliente - Invasão de conta detectada

MÉDIO - Responder em 1 dia: - Tentativa de invasão que foi bloqueada - Funcionário acessou dados que não devia - Problema em sistema secundário

BAIXO - Responder em 3 dias: - Alerta de segurança sem impacto real - Senha fraca detectada - Atualização de segurança necessária

4.3 O que fazer quando acontece um problema?

PASSO 1: Detectar e Avisar (imediato!)

SITUAÇÕES:

- Computador travado com mensagem pedindo resgate
- E-mail estranho que você clicou sem querer
- Arquivo importante sumiu
- Sistema não está funcionando

O QUE FAZER: 1. Não entrar em pânico! 2. Avisar imediatamente o responsável de TI 3. Se possível, tirar foto da tela 4. Não tentar resolver sozinho coisas complexas

PASSO 2: Isolar o Problema (primeira hora)

O objetivo é impedir que o problema se espalhe.

O QUE FAZER: - Desconectar computador infectado da rede (tirar o cabo ou desligar Wi-Fi) - Importante: NÃO desligar o computador (pode perder evidências) - Bloquear conta de usuário se foi invadida - Trocar senhas que podem ter sido comprometidas - Se for ransomware, desligar a internet de todo escritório temporariamente para proteger outros computadores - Avisar todo mundo para não abrir e-mails suspeitos

Por que isolar rápido: Vírus modernos se espalham em minutos. Se um computador foi infectado e está conectado na rede, pode contaminar todos os outros. Desconectar rapidamente pode salvar o resto do escritório.

PASSO 3: Investigar e Limpar (primeiras 24 horas)

O QUE FAZER: - Investigar como o ataque aconteceu - Ver quais dados foram afetados - Verificar se mais computadores foram atingidos - Rodar antivírus em toda a rede - Remover vírus e programas maliciosos - Fechar a brecha que permitiu o ataque

PASSO 4: Recuperar e Voltar ao Normal (até 3 dias)

O QUE FAZER: - Restaurar arquivos do backup - Reconstruir computadores que foram muito afetados (formatar e reinstalar) - Reconectar sistemas à rede gradualmente - Monitorar de perto por alguns dias para ver se o problema volta - Testar se sistemas estão funcionando direitinho

PASSO 5: Aprender com o Erro (1 semana depois)

AÇÕES PÓS-INCIDENTE: - Atualizar este documento de políticas se necessário - Treinar equipe sobre o que aprendemos - Implementar melhorias de segurança identificadas - Atualizar procedimentos de backup se for o caso

---

5. POLÍTICA DE BACKUP E RECUPERAÇÃO DE DESASTRES

5.1 O que é Backup?

Backup é fazer cópia dos arquivos importantes em outro lugar. Se algo der errado (vírus, HD queimado, arquivo apagado por acidente), a gente tem como recuperar.

5.2 Objetivo:

Garantir a continuidade das operações e a proteção dos dados críticos da empresa, mesmo em casos de falhas ou desastres.

Situações que backup resolve: - Ransomware criptografou todos os arquivos - HD do servidor queimou - Arquivo importante foi apagado sem querer - Incêndio ou enchente no escritório - Sistema corrompeu dados

5.3 O que fazer Backup?

Dados Críticos (backup todo dia): - Banco de dados com informações de clientes - Declarações e documentos fiscais - Contratos e documentos legais - E-mails corporativos

Dados Importantes (backup semanal): - Documentos de trabalho - Planilhas e relatórios - Materiais de treinamento

Por que essa diferença: Dados que mudam todo dia precisam de backup diário para não perder muito trabalho. Documentos que raramente mudam podem ter backup menos frequente sem problema.

5.4 Onde Fazer Backup?

3 cópias dos dados: - 1 original (no servidor principal) - 2 backups (cópias de segurança)

2 tipos diferentes de mídia: - HD externo - Nuvem

1 cópia em lugar diferente: - Uma cópia fora do escritório - Protege contra incêndio, enchente, roubo

Exemplo prático: - Original: Servidor do escritório - Backup 1: HD externo que será armazenado em um lugar diferente do escritório - Backup 2: Nuvem (AWS, Azure, etc.)

Por que isso funciona: Se o servidor quebrar, tem o HD externo. Se o escritório pegar fogo, tem a nuvem. Se o HD externo falhar, tem a nuvem. Se houver problema na nuvem, tem o HD externo.

5.5 Quando Fazer Backup?

Cronograma:

Backup Completo (todo domingo de madrugada): - Copia tudo - Demora mais tempo

Backup Incremental (todo dia à noite): - Copia só o que mudou desde ontem - Mais rápido

Backup em Tempo Real (de hora em hora durante o dia): - Só de arquivos super importantes - Se alguém apagar algo importante, dá pra recuperar de poucas horas atrás

Por que de madrugada: Backup usa bastante recurso do servidor. Fazendo de madrugada não atrapalha o trabalho do dia.

5.6 Por Quanto Tempo Guardar os Backups?

Backup diário: 7 dias
Backup semanal: 4 semanas

Backup mensal: 12 meses
Backup anual: 7 anos

Por que 7 anos no backup anual: Legislação brasileira exige guardar documentos contábeis e fiscais por no mínimo 5 anos. Guardamos 7 para ter margem de segurança.

5.7 Testar dos backups:

Testes obrigatórios:

Todo mês: Restaurar um arquivo aleatório
A cada 3 meses: Restaurar um sistema completo
A cada 6 meses: Simular um desastre total (servidor "queimou")

Por que testar: É possível que um backup der problema e acabe não sendo possível fazer a restauração completa. É melhor descobrir isso durante os teste do que durante uma necessidade real

5.9 Segurança dos Backups

Objetivo: Impedir que atacantes possam ter acesso aos backups e criptografar eles ou remover os backups.

Proteções: - Backups são criptografados - Senha de descriptografia guardada em lugar diferente - Backup em nuvem usa autenticação forte - HD de backup desconectado da rede quando não está copiando - Só administradores acessam backups - Log de quem acessou backups e quando

---