# **Política Básica de Segurança Políticas de acesso e controle de usuários**

### **Criação e gerenciamento de contas**

Cada funcionário terá uma conta única para acessar os sistemas da empresa. Não permitindo contas que permitam vários acessos (ex: "financeiro", "vendas").

Permite rastrear ações individuais (Modo Audit), facilita a aplicação de permissões específicas e evita o compartilhamento indevido de credenciais, reduzindo o risco de acessos não autorizados.

### **Política de Senhas**

As senhas devem ter no mínimo 10 caracteres, combinando letras maiusculas, minúsculas, números e símbolos. As senhas devem ser alteradas a cada 90 dias. Senhas padrão devem ser alteradas imediatamente no primeiro uso. É proibido reutilizar senhas antigas ou usar a mesma senha em múltiplos serviços.

Senhas fortes e trocadas regularmente dificultam ataques de força bruta e adivinhação, sendo uma barreira essencial para proteger contas e dados contra acesso não autorizado.

### **Princípio do Menor Privilégio**

Os usuários terão acesso apenas aos dados e sistemas estritamente necessários para desempenhar suas funções. Privilégios administrativos (permissão para instalar softwares, alterar configurações) serão restritos a pessoal autorizado designado pela gerência.

Limita o dano potencial caso uma conta seja comprometida ou um usuário cometa um erro. Se um usuário só acessar o que precisa, um invasor que use sua conta também terá acesso limitado.

### **Processo de Desligamento**

As contas de acesso (e-mail, sistemas, VPN, etc.) de funcionários desligados devem ser desativadas imediatamente no último dia de trabalho. O acesso a e-mails e arquivos importantes deve ser transferido para um gerente ou substituto, conforme definido pela gerência.

Impede o acesso não autorizado a informações confidenciais ou sistemas da empresa por ex-funcionários, protegendo contra vazamento de dados, sabotagem ou uso indevido de recursos.

## **Política de Uso de Dispositivos Móveis e Redes**

### **Uso de Dispositivos Móveis**

Funcionários que acessam dados corporativos (e-mail, arquivos, sistemas) em dispositivos móveis devem:

* Configurar e manter ativo o bloqueio de tela (PIN forte, senha, biometria).
* Manter o sistema operacional e aplicativos sempre atualizados.
* Informar imediatamente a gerência em caso de perda ou roubo do dispositivo.
* Evitar instalar aplicativos de fontes não confiáveis ou desconhecidas.
* Não realizar "jailbreak" ou "root" nos dispositivos que acessam dados da empresa.
* A instalação de aplicativos é restrita aos aprovados pela gerência. A empresa reserva-se o direito de aplicar configurações de segurança e realizar limpeza remota dos dados corporativos.

Dispositivos móveis são alvos fáceis para perda, roubo e malware. Estas medidas protegem os dados armazenados ou acessados por eles, prevenindo acessos não autorizados e vazamentos.

### **Segurança da Rede Wi-Fi**

A rede Wi-Fi principal deve ser protegida com segurança WPA2 ou WPA3 e uma senha forte, que não deve ser compartilhada com não-funcionários. Se houver necessidade de acesso para visitantes, uma rede Wi-Fi separada ("Convidado" ou "Visitante") deve ser utilizada, isolada da rede principal.

Uma rede Wi-Fi insegura permite que qualquer pessoa próxima acesse a rede interna, potencialmente interceptando dados, introduzindo malware ou atacando outros dispositivos. A separação da rede de visitantes protege os ativos internos da empresa.

### **Uso de Redes Públicas**

Não é aconselhado acessar informações sensíveis da empresa (dados financeiros, dados de clientes, login em sistemas críticos) ao utilizar redes Wi-Fi públicas (aeroportos, cafés, hoteis). Se o acesso for estritamente necessário, o uso da VPN da empresa é obrigatório.

Redes públicas são inseguras e podem ser monitoradas por atacantes ("Man-in-the-Middle") para capturar senhas, dados de navegação e outras informações confidenciais. A VPN mitiga esse risco.

## 

## **Diretrizes para Resposta a Incidentes de Segurança**

### **Notificação Imediata**

Qualquer suspeita de incidente de segurança deve ser reportada imediatamente. Não tente apagar, consertar ou esconder o problema. Forneça o máximo de detalhes possível sobre o que aconteceu.

A notificação rápida é crucial para permitir uma resposta ágil, conter o dano e iniciar a recuperação. Tentar resolver sozinho pode piorar a situação ou destruir evidências importantes.

### **Contenção Inicial**

Se suspeitar que um dispositivo está infectado por malware (ex: aviso de ransomware), desconecte-o imediatamente da rede (remova o cabo de rede ou desligue o Wi-Fi). Se possível, não desligue o computador, apenas isole-o da rede e aguarde instruções.

Isolar um dispositivo comprometido impede que a ameaça (ex: malware) se espalhe para outros computadores na rede, limitando o alcance do incidente.

### **Preservação de Evidências**

Não delete e-mails suspeitos (mesmo que de phishing), arquivos de log, ou qualquer outro artefato digital que possa estar relacionado ao incidente. Anote detalhes importantes: hora do ocorrido, mensagens de erro, comportamento observado, sistemas/dados afetados.

As evidências digitais são vitais para investigar a causa do incidente, entender o impacto, identificar o invasor (se aplicável) e tomar medidas para prevenir recorrências. A exclusão de dados pode atrapalhar severamente a investigação.

### **Pós-Incidente**

Após a resolução de um incidente significativo, será feita uma breve análise para documentar o que aconteceu, como foi resolvido, qual foi o impacto e quais lições foram aprendidas. As descobertas podem levar a atualizações nas políticas, treinamentos e ferramentas de segurança.

Aprender com os incidentes é fundamental para melhorar continuamente a postura de segurança e reduzir a probabilidade ou o impacto de eventos futuros.

## 

## 

## **Política de Backup e Recuperação de Desastres**

### **Frequência e Método de Backup**

Os dados críticos identificados devem ser copiados automaticamente e diariamente, geralmente ao final do expediente ou durante a noite, para capturar o trabalho do dia. O método de backup deve incluir uma combinação de backup automatizado em nuvem e backup local automatizado, assim garantindo redundância e segurança.

Backups diários e automáticos são a rede de segurança contra perda de dados devido a falhas de hardware, erros humanos, desastres ou ataques cibernéticos como ransomware. A escolha de métodos que incluam armazenamento externo nuvem ou mídia física levada para fora é vital para a recuperação do negócio mesmo em cenários de perda total do local físico.

### **Armazenamento Seguro dos Backups (Regra 3-2-1)**

Deve-se seguir a regra 3-2-1: Manter pelo menos três cópias dos dados críticos, em dois tipos de mídia diferentes, com pelo menos uma cópia armazenada fora do local físico principal da empresa (off-site).

* Se usar backup em nuvem, garanta que a conta esteja protegida com senha forte e autenticação de dois fatores (MFA/2FA).
* Se usar mídia física (HD externo, NAS), uma cópia deve ser levada regularmente para um local seguro fora do escritório. O dispositivo de backup deve ser desconectado após a conclusão do backup para protegê-lo contra ransomware.

Ter múltiplas cópias em locais e mídias diferentes protege os dados contra uma variedade maior de falhas e desastres como incêndio que destroi o escritório e o backup local, ransomware que criptografa arquivos locais e backups conectados.

**Testes de Restauração**

Os procedimentos de restauração de backup devem ser testados periodicamente, no mínimo mensalmente, para verificar se os dados podem ser recuperados de forma eficaz e dentro de um tempo aceitável. O teste deve envolver a restauração de uma amostra de arquivos ou um sistema de teste.

Um backup que não pode ser restaurado é inútil. Testes regulares validam a integridade dos backups e garantem que a equipe saiba como realizar a restauração quando necessário, reduzindo o tempo de inatividade em um cenário real de recuperação.