Atividade 1

Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

As **políticas de acesso e controle de usuários** são diretrizes e regras estabelecidas para regular como indivíduos ou sistemas acessam e utilizam recursos em uma rede ou sistema. Elas são cruciais para proteger dados, sistemas e assegurar que o uso de informações sensíveis seja controlado e monitorado adequadamente. Vou detalhar alguns dos principais elementos dessas políticas:

1. Controle de Acesso Baseado em Função (RBAC - Role-Based Access Control)

- Usuários recebem permissões com base em suas funções dentro da organização.
- Restringe o acesso aos recursos necessários para o desempenho de suas atividades, minimizando o risco de acessos não autorizados.

2. Autenticação e Autorização

- **Autenticação**: processo de verificação da identidade de um usuário (ex.: login com senha, autenticação multifator, biometria).
- **Autorização**: após a autenticação, o sistema define quais recursos ou informações o usuário pode acessar com base em suas permissões.

3. Privilégios Mínimos

- Atribuição de permissões mínimas necessárias para que os usuários realizem suas tarefas. O princípio é limitar o acesso desnecessário para reduzir o risco de comprometimento de segurança.

4. Política de Senhas

- Definir requisitos para criação de senhas fortes (ex.: comprimento mínimo, complexidade, validade).
- Exigir troca periódica de senhas para aumentar a segurança.

5. Controle de Acesso Baseado em Contexto (ABAC - Attribute-Based Access Control)

- Acessos são concedidos com base em atributos do usuário (como horário de trabalho, localização, etc.), em vez de apenas suas funções.

6. Segregação de Funções (SoD - Segregation of Duties)

- Divide responsabilidades para que nenhum indivíduo tenha controle absoluto sobre um processo ou sistema. Exemplo: uma pessoa que aprova pagamentos não deve ser a mesma que processa os pagamentos.

7. Monitoramento e Auditoria

- Registrar e monitorar atividades de usuários em sistemas e redes, garantindo que ações suspeitas possam ser detectadas e analisadas.
- Logs e trilhas de auditoria ajudam a revisar acessos não autorizados ou violação de políticas.

8. Revogação e Modificação de Acesso

- Garantir que quando um funcionário muda de função ou deixa a organização, seus acessos sejam modificados ou revogados imediatamente para prevenir acessos indevidos.

9. Autenticação Multifator (MFA)

- Usar mais de um método de verificação (senha + código enviado ao celular, por exemplo) para aumentar a segurança no acesso.

10. Controle de Acesso Físico

- Além do controle de acesso digital, é importante que áreas com servidores, roteadores e outros equipamentos sensíveis tenham controle de acesso físico, como crachás ou biometria.

11. Políticas de Acesso Remoto

- Definir regras para quem pode acessar remotamente e com que medidas de segurança (ex.: VPN, autenticação multifator, criptografia).

Política de uso de dispositivos móveis e redes

A **política de uso de dispositivos móveis e redes** tem o objetivo de garantir a segurança de dados e a integridade dos sistemas organizacionais quando os funcionários usam dispositivos móveis (smartphones, tablets, laptops) e acessam redes (Wi-Fi, VPN, dados móveis). Essa política é crucial em um cenário em que o trabalho remoto e a mobilidade se tornaram mais comuns.

1. Dispositivos Móveis

- **Uso de Dispositivos Pessoais (BYOD - Bring Your Own Device)**:
  - O uso de dispositivos pessoais para acessar sistemas corporativos deve ser previamente autorizado.
  - Dispositivos pessoais devem ser equipados com software de segurança, como antivírus e criptografia.
  - A empresa pode exigir a instalação de um software de gestão de dispositivos móveis (MDM) para controlar o acesso e proteger dados corporativos.
- **Criptografia e Armazenamento Seguro**:
  - Todos os dados corporativos armazenados em dispositivos móveis devem ser criptografados.
  - Os usuários não devem armazenar informações sensíveis localmente em dispositivos móveis, sempre que possível, preferindo o uso de serviços em nuvem controlados pela organização.
- **Senhas e Bloqueio de Tela**:
  - Dispositivos móveis devem ter senha ou PIN de bloqueio, e, preferencialmente, autenticação biométrica (digital ou facial).
  - Configurar um bloqueio automático de tela após um período curto de inatividade (por exemplo, 5 minutos).
- **Aplicações Autorizadas**:
  - Apenas aplicativos aprovados pela organização devem ser utilizados para acessar dados e sistemas corporativos.
  - O uso de aplicativos de terceiros que possam representar riscos à segurança (ex.: apps de compartilhamento de arquivos inseguros) deve ser proibido.
- **Atualizações de Software**:

- Dispositivos móveis usados para trabalho devem estar sempre atualizados com as últimas versões do sistema operacional e aplicativos para corrigir vulnerabilidades de segurança.

2. Redes

- **Uso de Redes Wi-Fi Públicas**:
  - O acesso a redes corporativas a partir de redes Wi-Fi públicas deve ser feito apenas com o uso de uma **VPN** (Rede Privada Virtual).
  - Redes públicas devem ser evitadas sempre que possível, especialmente sem medidas adicionais de proteção.
- **Rede Virtual Privada (VPN)**:
  - É obrigatório o uso de VPN para acessar sistemas e dados corporativos remotamente, garantindo a criptografia da comunicação.
  - As credenciais de acesso à VPN devem ser fortes e, preferencialmente, utilizar autenticação multifator.
- **Compartilhamento de Redes**:
  - É proibido o compartilhamento de conexões de internet por meio de dispositivos móveis, como o uso de "tethering" ou "hotspots", sem autorização específica.
  - Apenas redes seguras e aprovadas pela organização devem ser usadas para conexões relacionadas ao trabalho.
- **Monitoramento de Rede**:
  - Todas as conexões à rede corporativa serão monitoradas para detectar e mitigar possíveis riscos de segurança.
  - O uso de redes corporativas é restrito a atividades relacionadas ao trabalho, sendo o uso pessoal limitado.

3. Segurança de Dados

- **Backups Automáticos**:
  - Dispositivos móveis devem ser configurados para realizar backups automáticos dos dados corporativos em serviços de nuvem ou servidores seguros, evitando a perda de informações.
- **Perda ou Roubo de Dispositivo**:
  - Em caso de perda ou roubo de um dispositivo usado para acessar informações corporativas, o incidente deve ser imediatamente reportado ao departamento de TI.
  - Os dispositivos devem ter um recurso de apagamento remoto para garantir que informações confidenciais sejam eliminadas se o dispositivo for perdido ou comprometido.
- **Uso de Dados Móveis**:
  - O uso de dados móveis para acessar sistemas corporativos deve seguir as mesmas diretrizes de segurança, como o uso de VPN e autenticação multifator.

Diretrizes para resposta a incidentes de segurança

As **diretrizes para resposta a incidentes de segurança** são essenciais para garantir uma ação rápida e eficaz quando ocorrerem violações ou ameaças à integridade de dados e sistemas. A resposta eficaz a incidentes minimiza os danos e permite a restauração rápida das operações. As etapas a seguir compõem um plano abrangente de resposta a incidentes de segurança.

1. Preparação

- **Treinamento e conscientização**: Garantir que todos os funcionários saibam identificar e reportar incidentes de segurança. Realizar treinamentos regulares para as equipes, especialmente as de TI e de segurança.
- **Equipe de resposta a incidentes**: Definir uma equipe responsável pela resposta a incidentes, composta por profissionais de TI, segurança da informação e, quando necessário, representantes legais e de comunicação.
- **Ferramentas e tecnologia**: Implementar e manter ferramentas de monitoramento de rede, detecção de intrusões e resposta a incidentes (IDS/IPS), além de soluções de backup e criptografia de dados.
- **Políticas e procedimentos claros**: Desenvolver políticas claras sobre o que constitui um incidente de segurança e como proceder em cada caso, desde pequenas ameaças até grandes violações de dados.

2. Identificação

- **Monitoramento de eventos**: Acompanhar logs e sistemas de monitoramento para identificar anomalias, acessos não autorizados ou atividades suspeitas.
- **Classificação do incidente**: Determinar a natureza e a gravidade do incidente, como tentativas de phishing, malware, ataque DDoS, roubo de dados ou falha de segurança física.
- **Notificação de incidentes**: Desenvolver um sistema para que os funcionários possam reportar incidentes imediatamente, incluindo canais de comunicação claros para emergências de segurança.

3. Conter o Incidente

- **Conter a ameaça imediatamente**: Dependendo do tipo de incidente, o objetivo inicial é impedir que o ataque ou violação se espalhe. Pode-se optar por uma contenção rápida ou uma contenção mais cuidadosa, que permite analisar o ataque antes de erradicá-lo.
    - **Curto prazo**: Isolar os sistemas afetados da rede para impedir o acesso a mais recursos ou dados.
    - **Longo prazo**: Aplicar patches, mudanças em firewall ou regras de acesso para garantir que o incidente esteja completamente contido.
- **Preservação de evidências**: Garantir que todos os dados e registros do incidente sejam preservados para análise e futuras investigações.

4. Erradicação

- **Remoção da ameaça**: Após a contenção, o próximo passo é remover o malware, corrigir vulnerabilidades de software ou hardware, e fechar acessos não autorizados.
- **Verificação de vulnerabilidades adicionais**: Analisar se outras partes do sistema foram comprometidas e verificar a integridade dos dados.
- **Aplicação de patches e correções**: Instalar correções de segurança, remover programas maliciosos ou vulnerabilidades que permitiram o incidente.

5. Recuperação

- **Restauração dos sistemas**: Reestabelecer o funcionamento normal dos sistemas e serviços após a remoção da ameaça. Isso

pode envolver o uso de backups ou a reinstalação de sistemas afetados.

- **Testes pós-incidente**: Garantir que todos os sistemas tenham sido devidamente restaurados e estejam funcionando normalmente, sem riscos adicionais de segurança.
- **Monitoramento adicional**: Monitorar os sistemas de forma mais intensiva após a recuperação para garantir que a ameaça não retorne ou não existam novas falhas.

Política de backup e recuperação de desastres

A **política de backup e recuperação de desastres** é fundamental para garantir a continuidade dos negócios e a proteção dos dados críticos em situações de falhas técnicas, desastres naturais, ataques cibernéticos ou erros humanos. Essa política estabelece processos e práticas para o backup regular de informações e sistemas, além de diretrizes para a restauração e recuperação em caso de perda de dados ou interrupção de serviços.

1. Objetivos da Política

- **Garantir a integridade e disponibilidade dos dados**: Proteger os dados críticos e garantir que possam ser restaurados em caso de falha.
- **Minimizar o tempo de inatividade**: Assegurar que as operações da organização possam ser retomadas rapidamente após um desastre.
- **Reduzir o impacto financeiro**: Limitar as perdas financeiras e os prejuízos causados pela perda de dados ou interrupção dos sistemas.

2. Definição de Dados e Sistemas Críticos

- **Identificação dos dados críticos**: Classificar os dados que são vitais para o funcionamento da organização, como informações financeiras, dados de clientes, registros de saúde (no caso de serviços de saúde) e sistemas de TI.
- **Priorização de sistemas**: Determinar quais sistemas e serviços precisam ser recuperados primeiro com base no impacto nos negócios e nas operações.

3. Frequência de Backup

- **Backups diários**: Realizar backups diários de todos os dados críticos para garantir que a perda de dados seja minimizada.
- **Backups incrementais**: Fazer backups incrementais (diários ou mais frequentes) para salvar apenas as alterações feitas desde o último backup completo, economizando tempo e espaço de armazenamento.
- **Backups completos periódicos**: Realizar backups completos em intervalos regulares (semanal ou mensalmente) para garantir a cópia de todos os dados.
- **Backups em tempo real**: Para sistemas críticos, considerar o uso de tecnologias de backup em tempo real para proteger dados à medida que são criados ou modificados.

4. Armazenamento de Backups

- **Localização de armazenamento**:
    - **On-site (local)**: Manter backups no local para recuperação rápida em caso de falhas menores, como perda de arquivos.

    - **Off-site (fora do local)**: Armazenar cópias de backups em locais remotos ou na nuvem para garantir a recuperação em caso de desastres no local principal, como incêndios ou inundações.
- **Redundância de locais**: Usar múltiplas localizações para armazenamento off-site, garantindo que um único evento catastrófico não comprometa todas as cópias de segurança.
- **Criptografia**: Os dados armazenados em backups, especialmente em localizações externas ou na nuvem, devem ser criptografados para garantir a confidencialidade e proteção contra acesso não autorizado.

5. Procedimentos de Recuperação de Desastres

- **Plano de recuperação**:
    - Definir claramente o processo a ser seguido em caso de desastre, com uma lista de prioridades de recuperação (dados e sistemas mais críticos).
    - Criar um plano de comunicação para notificar rapidamente as partes interessadas (funcionários, clientes, parceiros) sobre a interrupção e as etapas de recuperação.
- **Recuperação dos dados**: Detalhar os procedimentos para restaurar os dados a partir dos backups, incluindo a localização das cópias e o método de recuperação.
- **Recuperação de sistemas**: Descrever como restaurar os sistemas operacionais e aplicativos a partir de backups de sistema ou imagens de disco.
- **Teste de recuperação**: Realizar testes regulares de recuperação para garantir que o processo funcione conforme planejado e que os dados e sistemas possam ser restaurados rapidamente.

6. Pontos de Recuperação e Tempo de Recuperação

- **Objetivo de Ponto de Recuperação (RPO - Recovery Point Objective)**:
  - Define quanto tempo de dados a organização pode se dar ao luxo de perder em caso de falha (ex.: se o backup é diário, o RPO pode ser de até 24 horas).
  - Quanto mais curto o RPO, mais frequente deve ser o backup.
- **Objetivo de Tempo de Recuperação (RTO - Recovery Time Objective)**:
  - Define o tempo máximo aceitável para restaurar operações após um desastre ou falha.
  - O plano deve incluir recursos e infraestrutura suficientes para atingir o RTO estabelecido, garantindo a continuidade dos negócios.

7. Política de Retenção de Backups

- **Período de retenção**: Definir por quanto tempo os backups serão mantidos antes de serem excluídos ou substituídos. Isso pode variar de acordo com os requisitos legais, como a retenção de dados financeiros por cinco anos.
- **Ciclo de vida dos backups**: Estabelecer um ciclo de retenção de backups (diários, semanais, mensais e anuais), mantendo uma combinação de backups recentes e antigos para garantir a recuperação em caso de necessidade futura.

8. Segurança de Backups

- **Acesso controlado**: Restringir o acesso aos backups para garantir que apenas pessoal autorizado possa visualizar ou restaurar dados.
- **Autenticação e auditoria**: Implementar autenticação multifator e trilhas de auditoria para monitorar quem acessou ou modificou os backups.
- **Proteção contra ransomware**: Implementar medidas de proteção contra ransomware, como backups offline (que não podem ser acessados ou criptografados por ransomware) e políticas de detecção e resposta a ameaças.

9. Monitoramento e Testes Regulares

- **Monitoramento automático de backups**: Usar ferramentas que monitorem os backups automaticamente para garantir que todos os processos sejam concluídos com sucesso, emitindo alertas em caso de falhas.
- **Testes de recuperação**: Agendar testes periódicos de recuperação para validar a eficácia dos backups e garantir que eles estejam disponíveis e funcionais quando necessário.
- **Revisão e aprimoramento**: Revisar regularmente a política de backup e recuperação de desastres para garantir que ela se mantenha atualizada com novas ameaças, tecnologias e requisitos organizacionais.

10. Política de Continuidade dos Negócios

- **Plano de continuidade**: A política de backup deve fazer parte de um plano mais amplo de continuidade dos negócios (BCP - Business Continuity Plan), garantindo que não apenas os dados

e sistemas sejam recuperados, mas também as operações essenciais sejam retomadas rapidamente.

- **Equipes de resposta**: Definir claramente as responsabilidades da equipe de TI e outros profissionais envolvidos na recuperação de desastres e continuidade dos negócios.

11. Conformidade com Regulamentos

- **Requisitos legais e regulamentares**: A política de backup deve estar em conformidade com os regulamentos de proteção de dados aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia, ou outras normas de setor.
- **Auditorias regulares**: Realizar auditorias regulares para garantir que os procedimentos de backup e recuperação estejam em conformidade com as normas e regulamentos aplicáveis.