**UC – Sistemas Computacionais e Segurança – Atividade 06**

**Integrantes : Nicholas, Tobias, Wendel**

**Politicas de acesso de uma pequena empresa**

**1. Políticas de Acesso e Controle de Usuários**

**Objetivo:** Estabelecer mecanismos de controle que garantam o acesso autorizado aos recursos informacionais da empresa, limitando o uso inadequado de dados e recursos críticos.

**Política Proposta:**

* **Autenticação e Autorização:** Todos os usuários devem ser autenticados através de credenciais únicas e seguras. Recomenda-se a adoção de senhas complexas e, quando possível, o uso de autenticação multifator para garantir maior segurança.
* **Privilégios de Acesso:** O acesso aos recursos da empresa será baseado no princípio do menor privilégio, no qual os usuários têm permissões apenas para os dados e sistemas necessários para a execução de suas funções.
* **Gerenciamento de Senhas:** As senhas devem ser alteradas regularmente, com um intervalo máximo de 90 dias, e o compartilhamento de credenciais entre usuários é estritamente proibido.
* **Desativação de Contas:** Contas de usuários inativos ou desligados da empresa devem ser desativadas imediatamente. O acesso temporário a sistemas deve ser concedido com uma data de expiração previamente definida.

**Justificativa:**  
A adoção de práticas de autenticação e controle de acesso tem como objetivo principal a prevenção de acessos não autorizados a sistemas críticos da empresa. A implementação de senhas fortes e de autenticação multifator minimiza o risco de credenciais comprometidas, enquanto o princípio do menor privilégio limita o potencial de danos em caso de vazamento de informações ou uso inadequado.

**2. Política de Uso de Dispositivos Móveis e Redes**

**Objetivo:** Estabelecer diretrizes para o uso seguro de dispositivos móveis e redes externas no acesso aos dados corporativos, visando proteger a empresa contra ameaças associadas ao trabalho remoto e ao uso de redes inseguras.

**Política Proposta:**

* **Criptografia de Dados:** Todos os dispositivos móveis utilizados para acessar sistemas da empresa devem ter criptografia habilitada, protegendo os dados em caso de perda ou roubo.
* **Acesso por VPN:** O acesso remoto aos sistemas corporativos deve ser realizado exclusivamente por meio de uma rede virtual privada (VPN), assegurando a criptografia do tráfego de dados.
* **Política de BYOD (Bring Your Own Device):** Caso a empresa permita o uso de dispositivos pessoais, eles deverão seguir as mesmas diretrizes de segurança dos dispositivos corporativos, incluindo a instalação de softwares de segurança e bloqueio por senha.
* **Proibição de Uso de Redes Públicas Não Seguras:** O acesso a dados da empresa via redes Wi-Fi públicas deve ser proibido, a menos que o funcionário utilize uma VPN para proteger as comunicações.

**Justificativa:**  
O uso de dispositivos móveis e redes externas expõe a empresa a novos vetores de ataque, como o roubo de dados em redes inseguras. A criptografia protege os dados em dispositivos perdidos ou roubados, enquanto o uso de VPN garante a segurança das comunicações em redes externas. Além disso, a política de BYOD permite flexibilidade sem comprometer a segurança da informação.

**3. Diretrizes para Resposta a Incidentes de Segurança**

**Objetivo:** Definir um conjunto de ações coordenadas para detectar, responder e mitigar incidentes de segurança, visando minimizar os impactos de eventos adversos sobre os sistemas e dados da empresa.

**Política Proposta:**

* **Monitoramento Contínuo:** Estabelecer sistemas de monitoramento contínuo para detectar comportamentos anômalos e possíveis violações de segurança.
* **Comunicação de Incidentes:** Ao identificar um incidente de segurança, os responsáveis devem notificar imediatamente a equipe de resposta, que será encarregada de investigar e mitigar o incidente.
* **Ações Corretivas:** Após a identificação de um incidente, medidas corretivas devem ser tomadas de forma imediata para conter a ameaça e mitigar seus efeitos.
* **Documentação e Aprendizado:** Todos os incidentes devem ser documentados detalhadamente, incluindo a descrição do evento, como foi identificado, quais medidas foram adotadas e recomendações para evitar recorrência. Posteriormente, será realizada uma análise pós-incidente para melhorar as políticas de segurança e prevenir novos eventos.

**Justificativa:**  
A resposta rápida e organizada a incidentes de segurança é crucial para minimizar os impactos negativos sobre a operação da empresa. O monitoramento contínuo possibilita a detecção precoce de ameaças, enquanto a comunicação eficaz e as ações corretivas garantem uma resposta imediata. A documentação completa dos incidentes fornece insights importantes para a melhoria contínua das políticas e sistemas de segurança.

**4. Política de Backup e Recuperação de Desastres**

**Objetivo:** Implementar uma estratégia robusta de backup e recuperação de desastres que garanta a integridade dos dados e a continuidade das operações em caso de falhas ou incidentes graves.

**Política Proposta:**

* **Backup Regular:** Os dados críticos da empresa devem ser submetidos a backups diários. Esses backups devem ser armazenados em local seguro, preferencialmente em um local externo ou na nuvem.
* **Teste de Recuperação:** Testes periódicos de recuperação de dados devem ser realizados para assegurar a eficácia dos processos e a integridade das cópias de segurança.
* **Plano de Recuperação de Desastres:** A empresa deve ter um plano formal de recuperação de desastres que identifique os sistemas críticos e defina as etapas necessárias para a retomada das operações em caso de incidentes que causem interrupção nos serviços.
* **Controles de Acesso aos Backups:** O acesso aos backups deve ser restrito a indivíduos autorizados, sendo implementados controles rigorosos para garantir a segurança dos dados armazenados.

**Justificativa:**  
A falha em realizar backups adequados pode resultar na perda irreversível de dados críticos, o que pode comprometer seriamente a continuidade dos negócios. O armazenamento seguro das cópias de segurança, aliado ao teste regular de recuperação, garante que a empresa possa retomar suas operações com a menor interrupção possível após um incidente. O plano de recuperação de desastres assegura que a empresa esteja preparada para enfrentar emergências de forma eficiente.