Atividade 17/04

Henrique Rosa da Silva - 82518188
Gabriel Luiz Vicente Soares - 825150671
Felipe Honorio de Sousa - 825134274
Vitor Bernardes - 825138944
Vitor de Souza Devicari - 825139110

São Paulo - 2025
São Judas

Desenvolvimento de Políticas de Segurança

Políticas de Acesso e Controle de Usuários

Medidas adotadas:

- Autenticação forte (MFA): Todos os colaboradores devem usar autenticação multifator para acessar os sistemas internos.

- Acesso mínimo necessário: Cada funcionário terá acesso somente às informações e ferramentas que precisa para realizar seu trabalho.

- Criação e exclusão de contas: A equipe de TI cria contas apenas mediante solicitação formal do gerente. Contas de ex-funcionários são desativadas imediatamente após seu desligamento.

- Troca periódica de senhas: As senhas devem ser atualizadas a cada 90 dias, seguindo critérios mínimos de complexidade.

Justificativas:

- Controlar quem acessa o quê reduz riscos de acesso não autorizado a informações sensíveis.

- O MFA reforça a segurança, dificultando acessos indevidos mesmo que a senha seja descoberta.

- Remover o acesso de ex-funcionários evita brechas de segurança.

- Trocar senhas com frequência reduz as chances de uso indevido por terceiros.

Política de Uso de Dispositivos Móveis e Redes

Medidas adotadas:

- Acesso somente por dispositivos autorizados: Apenas celulares e dispositivos registrados podem se conectar à rede da empresa.

- Criptografia e proteção obrigatória: Todos os dispositivos devem ter criptografia ativada e estar protegidos por senha ou biometria.

- Uso de VPN: Quem precisa acessar os sistemas da empresa remotamente deve fazer isso apenas via VPN corporativa.

- Proibição de Wi-Fi público: É proibido acessar os sistemas a partir de redes Wi-Fi públicas ou não seguras.

Justificativas:

- Dispositivos móveis são mais suscetíveis a perdas, roubos ou invasões via redes inseguras.

- Criptografia protege os dados mesmo em caso de perda ou roubo do aparelho.

- A VPN garante uma conexão segura entre o colaborador e a empresa.

- Evitar Wi-Fi público diminui o risco de ataques como “man-in-the-middle”.

Diretrizes para Resposta a Incidentes de Segurança

Medidas previstas:

- Plano de Resposta a Incidentes (PRI): Um documento oficial irá detalhar os procedimentos a seguir em casos como vazamento de dados ou falhas técnicas.

- Equipe de resposta: Um grupo interno será treinado para agir com agilidade diante de incidentes.

- Registro de incidentes: Cada ocorrência será registrada com detalhes sobre o que aconteceu, as ações tomadas e os impactos.

- Alerta imediato: Qualquer atividade suspeita deve ser comunicada imediatamente à equipe responsável.

Justificativas:

- Um plano claro acelera a resposta e reduz danos.

- Equipes treinadas sabem agir com eficiência.

- O registro ajuda a identificar padrões e prevenir novas ocorrências.

- Notificações rápidas evitam que pequenos problemas virem grandes crises.

Política de Backup e Recuperação de Desastres

Ações estabelecidas:

- Backups automáticos diários: Dados críticos serão copiados todos os dias para um servidor seguro.

- Cópias externas: Uma vez por semana, será feita uma cópia de segurança em local externo ou na nuvem.

- Testes frequentes: A equipe de TI fará testes mensais para garantir que os backups possam ser restaurados com sucesso.

- Plano de continuidade: Em caso de falhas graves, o plano orienta como retomar os serviços essenciais.

Justificativas:

- Backups frequentes protegem contra falhas técnicas, ataques de ransomware e desastres físicos.

- Armazenar cópias fora do local previne perdas em casos como incêndios ou enchentes.

- Testar os backups evita surpresas na hora de restaurar os dados.

- Um bom plano de continuidade garante que a empresa volte a funcionar rapidamente, com prejuízos mínimos.