Atividades Professor Calvetti- Davi Emanuel Silva Adriano 823149648

ATIVIDADE LAB6

Atividade 1

Manual de Políticas de Segurança da Informação – Empresa Fictícia: TechNova

1. Controle de Acesso e Usuários

Objetivo:

Garantir que apenas pessoas autorizadas tenham acesso aos sistemas e informações da empresa, de forma controlada e monitorada.

Políticas:

- Cada colaborador terá um usuário e senha exclusivos.
- O acesso será concedido conforme o nível de necessidade (mínimo necessário).
- Senhas fortes e renovadas a cada 90 dias.
- Autenticação em duas etapas (2FA) para acessos administrativos e financeiros.
- A conta de um colaborador será bloqueada após 5 tentativas falhas ou 30 dias de inatividade.

Justificativa:

Reduz o risco de acesso não autorizado, vazamento de informações e facilita a rastreabilidade em caso de incidentes.

2. Uso de Dispositivos Móveis e Conexões de Rede

Objetivo:

Evitar a exposição de dados e sistemas da empresa ao uso incorreto de dispositivos móveis e redes externas.

Políticas:

- Dispositivos pessoais só poderão ser usados com autorização da equipe de TI.
- Dispositivos usados no trabalho devem ter:
    - Antivírus atualizado
    - Criptografia ativada
    - Bloqueio automático por inatividade
- O acesso remoto aos sistemas só será feito por VPN oficial da empresa.
- Redes Wi-Fi públicas são proibidas, a menos que com VPN ativa.

Justificativa:

A mobilidade é útil, mas aumenta a superfície de ataque. Essas regras protegem o ambiente corporativo contra falhas humanas e conexões inseguras.

3. Resposta a Incidentes de Segurança

Objetivo:

Estabelecer um protocolo claro para lidar com falhas, ataques e violações de segurança.

Políticas:

- Todo incidente deve ser imediatamente reportado ao responsável de TI.
- O plano de resposta inclui 5 etapas:
    1. Identificação
    2. Contenção
    3. Erradicação
    4. Recuperação
    5. Análise e melhoria

Justificativa:

A preparação é a melhor forma de minimizar impactos e aprender com os erros. Ter um plano de ação evita o improviso em momentos críticos.

4. Backup e Recuperação de Desastres

Objetivo:

Assegurar que a empresa consiga recuperar suas informações em caso de falhas, perdas ou desastres.

Políticas:

- Backup completo semanal e incremental diário.
- Armazenamento em:
    - Local externo (offline)
    - Nuvem com criptografia
- Realização de testes de restauração a cada 3 meses.
- Tempo máximo de recuperação de sistemas críticos: 24 horas após o incidente.

Justificativa:

Em casos de ataque, falha física ou erro humano, o backup garante a continuidade do negócio. A existência de cópias seguras e testadas reduz os danos de forma significativa.

Atividade 2

NIST Cybersecurity Framework (CSF) é um conjunto de diretrizes criado pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) para ajudar organizações a gerenciar e reduzir riscos de cibersegurança.

COBIT (Control Objectives for Information and Related Technologies) é um framework de governança e gestão de TI, incluindo a segurança da informação. Desenvolvido pela ISACA.

Comparativo: NIST CSF vs COBIT

1. Requisitos para certificação:

- NIST CSF: Não exige certificação. É um framework gratuito e voluntário.

- COBIT: Exige certificação (ex: COBIT Foundation). Precisa fazer curso e prova pela ISACA.

2. Setores de atuação:

- NIST CSF: Usado por empresas de energia, saúde, governo, tecnologia e pequenas empresas.

- COBIT: Usado por grandes empresas, bancos, auditorias e setores que exigem governança de TI.

3. Benefícios:

- NIST CSF: Melhora a segurança cibernética, organiza processos e reduz riscos. Fácil de aplicar.

- COBIT: Ajuda na governança de TI, tomada de decisão e controle. Alinha TI aos objetivos do negócio.

4. Gestão de riscos:

- NIST CSF: Prático. Usa funções como identificar, proteger, detectar, responder e recuperar.

- COBIT: Estratégico. Foco em controles, políticas, auditoria e cumprimento de metas da empresa.