2.2 Política de Backup e Recuperação

1. Objetivo

Estabelecer diretrizes para execução, armazenamento e restauração de cópias de segurança de dados e sistemas críticos, garantindo a disponibilidade e integridade das informações conforme CIS Controls v8 IG1 (C11).

2. Escopo

Aplica-se a todos os sistemas, bancos de dados, arquivos e aplicações críticas definidos no inventário de ativos, abrangendo ambientes on-premises e serviços em nuvem.

3. Responsabilidades

- **Alta Direção**: Aprovar esta política e assegurar recursos para backup e recuperação.
- **Gestor de Segurança da Informação**: Definir estratégias de backup, revisar métricas de conformidade e aprovar testes de restauração.
- **Equipe de TI / Administradores de Sistemas**: Configurar rotinas de backup, executar restores e registrar evidências.
- **Gestores de Área**: Validar criticidade de sistemas e apoiar janelas de manutenção para testes.
- **Todos os Colaboradores**: Seguir procedimentos de backup local quando aplicável e reportar falhas.

4. Definições

- **Backup Full**: Cópia completa de todos os dados.
- **Backup Incremental**: Cópia de alterações desde o último backup.
- **Restore**: Processo de recuperação de dados a partir de backup.
- **Off-site / Offline**: Armazenamento de backup em local externo ou inacessível pela rede corporativa.

5. Referências e Pré-requisitos

- Inventário de ativos e criticidade de dados.
- Ferramenta de backup homologada.
- Acordos de nível de serviço (SLA) para RPO (Recovery Point Objective) e RTO (Recovery Time Objective).
- Acesso administrativo às plataformas de backup.

6. Diretrizes

- **Frequência e retenção de backups automatizados** (CIS C11)
- **Armazenamento offline ou off-site** (CIS C11)
- **Critérios de criptografia mínima para mídias de backup** (CIS C11)

- **Frequência de Backup**:
    - Full semanal (domingo às 02:00)
    - Incremental diário (02:00 de segunda a sábado)
- **Retenção**:
    - Backups diários por 30 dias
    - Backups semanais por 90 dias
- **Armazenamento Off-site**: Replicar backups completos semanalmente em local externo.
- **Criptografia de Backup**: Dados em backup devem ser criptografados em repouso e em trânsito.
- **Monitoramento e Alertas**: Configurar alertas para falhas de backup e espaço insuficiente.

7. Verificação e Auditoria. Verificação e Auditoria

- **Testes de Restore**: Realizar restauração mensal e trimestral, documentando sucesso e tempo de recuperação.
- **Auditoria de Backup**: Revisar logs de backup semanalmente para identificar falhas ou inconsistências.
- **Relatório de Conformidade**: Enviar métricas para o Gestor de Segurança mensalmente.

8. Registros e Relatórios

- Manter registro de todas as operações de backup e restore em repositório centralizado, incluindo:
    - Tipo de backup
    - Data, hora e responsável
    - Resultado (sucesso/falha)
- Gerar relatório trimestral de disponibilidade de restaurações para a Alta Direção.

9. Revisão da Política

Revisar anualmente ou sempre que houver alterações em sistemas, requisitos de negócio ou lições aprendidas de testes e incidentes.