Etapa 4 – Gestão de Continuidade de Negócio (PCN)

a. Esboço do Plano de Continuidade de Negócio (PCN)

Objetivo do PCN

Garantir que a MedClin seja capaz de continuar suas operações críticas, mesmo diante de eventos que comprometam a disponibilidade de sistemas, dados ou infraestrutura física.

Processos Críticos Identificados

PROCESSSO	DESCRIÇÃO
Sistema de Prontuário Eletrônico	Registro médico essencial para atendimentos presenciais e remotos
Aplicativo de Agendamento	Interface primária de marcação de consultas pelos pacientes.
Banco de Dados em Nuvem	Armazena dados sensíveis, históricos clínicos e administrativos.
Infraestrutura de Rede e Internet	Essencial para acesso a sistemas e comunicação entre unidades.
Comunicação com Pacientes	Notificações, lembretes e suporte em tempo real via canais digitais.

Estratégias de Resposta e Continuidade

CENÁRIO DE INTERRUPÇÃO	RESPOSTA IMEDIATA	TEMPO MÁXIMO DE RESTAURAÇÃO(RTO)
Queda do sistema de prontuário	Ativação do backup local + versão offline emergencial	2 horas
Falha no aplicativo de agendamento	Redirecionamento para agendamento por telefone com planilha de controle manual	4 horas
Ataque de ransomware	Isolamento dos sistemas afetados + recuperação via backup seguro na nuvem	6 horas
Perda de acesso à internet	Uso de link reserva (conexão secundária) e plano offline para registros temporários	1 hora
Invasão ou vazamento de dados	Acionamento do protocolo de resposta a incidentes + aviso à ANPD (LGPD)	24 horas (notificação)

b. Revisão de Cobertura das Ameaças/Vulnerabilidades

O PCN cobre diretamente as principais ameaças e vulnerabilidades listadas na Etapa 2:

AMEAÇA/VULNERABILIDADE	COBRE NO PCN?	OBSERVAÇÃO
Phishing	✅	Prevenção via treinamento; continuidade com equipe reserva
Ransomware	✅	Backup em nuvem e isolamento imediato do sistema afetado
Engenharia social	✅	Plano de contingência prevê comunicação e resposta centralizada
Acesso Indevido	✅	MFA e bloqueio remoto; substituição de credenciais comprometidas
Falha no app móvel	✅	Plano de atendimento alternativo por telefone
Atualizações não aplicadas	⚠️ Parcial	Planejado para ser incluído no ciclo de governança contínua
Ausência de criptografia	✅	Backup e comunicações protegidas via SSL e criptografia AES-256
Funcionário mal-intencionado	✅	Papéis bem definidos + monitoramento e plano de substituição
Falta de autenticação multifator	✅	MFA obrigatório nos acessos administrativos e médicos
Erro Humano	✅	Processos revisados e dupla verificação em comunicações críticas

c. Aspectos de Governança

Papéis e Responsabilidades

FUNÇÃO	RESPONSÁVEL	ATRIBUIÇÕES EM CASO DE INCIDENTE
Coordenação Geral do PCN	Diretor da MedClin	Tomada de decisão, acionamento do plano e comunicação externa/institucional
TI / Segurança da Informação	Analista de Infraestrutura de TI	Execução de planos de recuperação, restauração de sistemas e backups
Comunicação	Secretária-chefe	Notificação a pacientes, operadoras e fornecedores
Jurídico/Compliance	Assessor Jurídico	Comunicação com ANPD, registro do incidente, análise de impacto regulatório