ATIVIDADE 08

Docente: Robson Calvetti
UC: Sistemas Computacionais e Segurança – SCS

Beatriz Silva de Jesus – RA: 824219590
Christian Batista de Lima – RA: 824126605
Mariana Hildebrand Danta – RA: 824118462
Marinna Pereira Carneiro da Silva – RA: 824142121
Mayara Fernanda dos Santos – RA: 824227938
Victor Pinas Arnault – RA: 82215768

Sumário

ATIVIDADE 08

Objetivo: Os alunos deverão desenvolver um esboço de Plano de Continuidade de Negócios para uma empresa fictícia, levando em consideração os principais componentes de um BCP, identificando riscos, recursos críticos e definindo estratégias de recuperação;

Instruções: Formação de Grupos: Divida a turma em grupos de 4-6 alunos;

Contexto: Cada grupo deverá escolher ou criar um cenário fictício de uma empresa (pode ser uma startup de tecnologia, uma instituição financeira, um hospital, etc.);

Tarefas:

1. Identificação dos Recursos Críticos: Listar os recursos e sistemas que são essenciais para a operação da empresa;

2. Análise de Impacto nos Negócios (BIA): Identificar possíveis eventos disruptivos (ex.: falha de TI, desastre natural, ataque cibernético) e analisar o impacto de cada um no negócio;

3. Estratégias de Recuperação: Propor estratégias para garantir a continuidade dos negócios, como redundância de sistemas, backup de dados, plano de comunicação em caso de emergência, entre outros;

4. Plano de Ação: Definir um plano de resposta e recuperação, detalhando as etapas e prazos para a retomada das operações, designando responsabilidades e recursos necessários.

5. Teste do Plano: Sugerir uma forma de testar o plano de continuidade para garantir sua eficácia (ex.: simulação de cenário de crise).

INTRODUÇÃO DA EMPRESA E SEU CENÁRIO

Cada grupo deverá escolher ou criar um cenário fictício de uma empresa (pode ser uma startup de tecnologia, uma instituição financeira, um hospital etc.)

O hospital Vida Nova é uma unidade sanitária que faz parte do patrimônio da empresa HVida onde não são instituídas pelo Poder Público.

O Hospital Vida Nova tem diversos sistemas integrados sendo os principais:

- Prontuário Eletrônico do Paciente onde registra e armazena digitalmente o histórico médico do paciente, incluindo diagnósticos, tratamentos, exames e prescrições. cada paciente é identificado por uma pki única
- Sistema de Agendamento de Consultas e Cirurgias onde gerencia a marcação de consultas médicas, cirurgias e exames, otimizando o fluxo de pacientes.
- Sistema de Faturamento e Cobrança onde automatiza a geração de contas, envio de faturas para pacientes e convênios, além do controle de recebimentos e auditoria de contas médicas. A comunicação é protegida por uma endpoint protection

A empresa Hvida teve uma preocupação na instalação desses sistemas onde o Hospital Vida Nova fica localizado em uma zona de risco de alagamento e perca de energia em temporais. Contando que o sigilo médico é um direito do paciente, sendo um dever do médico mantê-lo, podendo, portanto, só ser quebrado mediante o consentimento por escrito do paciente ou mediante situações permitidas por lei. Logo, a regra geral é o sigilo médico. Nos termos do Código de Ética Médica, é vedado ao médico: Artigo 73. A empresa Hvida decidiu criar um Plano de Continuidade de Negócios – BCP visando ter um "plano B" para lidar com crises e possíveis riscos para não ocorrer interrupções significativas como roubo de dados ou não conseguir acessar os prontuários de cada paciente.

RECURSOS CRÍTICOS IDENTIFICADOS

Listar os recursos e sistemas que são essenciais para a operação da empresa;

Os recursos que são essenciais para a operação da empresa como falamos na introdução são:

- Prontuário Eletrônico do Paciente onde registra e armazena digitalmente o histórico médico do paciente, incluindo diagnósticos, tratamentos, exames e prescrições.
- Sistema de Agendamento de Consultas e Cirurgias onde gerencia a marcação de consultas médicas, cirurgias e exames, otimizando o fluxo de pacientes.
- Sistema de Faturamento e Cobrança onde automatiza a geração de contas, envio de faturas para pacientes e convênios, além do controle de recebimentos e auditoria de contas médicas.
- Sistema de Controle de Qualidade e Segurança onde garante o cumprimento das normas de qualidade e segurança hospitalar, monitorando indicadores como infecções, acidentes e boas práticas.
- Sistema de Manutenção Predial onde gerencia a manutenção preventiva e corretiva dos equipamentos hospitalares e da infraestrutura física do hospital.

ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)

Identificar possíveis eventos disruptivos (ex.: falha de TI, desastre natural, ataque cibernético) e analisar o impacto de cada um no negócio;)

Analisando a infraestrutura da empresa HVida dona do Hospital Vida Nova contando com os sistemas presentes, podemos verificar que com uma falha do TI, um desastre natural e um ataque cibernético pensando em um contexto geral muitas vidas irão se perder analisando os principais sistemas:

No Sistema de Prontuário Eletrônico do Paciente (PEP), que registra e armazena digitalmente o histórico médico do paciente, incluindo diagnósticos, tratamentos, exames e prescrições, um possível ataque cibernético que inviabilize o acesso a esses dados afetaria diretamente a vida do paciente. Sem o acesso às prescrições e tratamentos, haveria o risco de uso indevido de medicamentos, incluindo aqueles aos quais o paciente pode ser alérgico, podendo levar a graves complicações ou até à morte.

Além disso, em um cenário de desastre natural, como uma tempestade que comprometa a estrutura física do hospital, a falta de acesso a esses registros também colocaria em risco a vida dos pacientes. Por fim, em um ataque cibernético, conforme discutido na introdução, o sigilo médico é um direito do paciente e um dever do médico. Esse sigilo só pode ser quebrado com consentimento por escrito do paciente ou em situações previstas em lei. No caso de uma invasão cibernética, os dados dos pacientes poderiam ser comprometidos e expostos, violando a Lei Geral de Proteção de Dados (LGPD).

O Sistema de Agendamento de Consultas e Cirurgias gerencia a marcação de consultas médicas, cirurgias e exames, otimizando o fluxo de pacientes e a organização dos recursos médicos. Em um possível ataque cibernético, a indisponibilidade desse sistema causaria atrasos ou até cancelamentos nas consultas e procedimentos, impactando diretamente a saúde dos pacientes. Além disso, a falta de acesso a informações críticas como horários e prontuários pode comprometer a continuidade dos tratamentos. Em um cenário de desastre natural, como uma tempestade que afete a infraestrutura hospitalar, a perda de acesso ao sistema colocaria em risco a segurança e o bem-estar dos pacientes, pois comprometeria a organização dos atendimentos. Já em caso de uma invasão cibernética, dados

sensíveis dos pacientes, como horários de cirurgias e informações pessoais, poderiam ser expostos, violando a privacidade e a LGPD.

O Sistema de Faturamento e Cobrança automatiza a geração de contas, o envio de faturas para pacientes e convênios, além de controlar recebimentos e auditar contas médicas. Em um cenário de ataque cibernético, a paralisação desse sistema resultaria em graves problemas financeiros para o hospital, como o atraso na cobrança de procedimentos e pagamentos de convênios, o que afetaria a sustentabilidade da instituição. Além disso, a falta de acesso aos dados de faturamento poderia gerar erros em cobranças, prejudicando tanto os pacientes quanto o hospital. Em um desastre natural que comprometa a infraestrutura física, a falha no sistema poderia levar à perda de informações financeiras importantes. No caso de uma invasão cibernética, os dados financeiros dos pacientes e do hospital poderiam ser vazados, expondo informações sensíveis e causando sérios danos à privacidade e à conformidade com a LGPD.

ESTRATÉGIAS DE RECUPERAÇÃO PROPOSTAS

Propor estratégias para garantir a continuidade dos negócios, como redundância de sistemas, backup de dados, plano de comunicação em caso de emergência, entre outros;

Para anular os riscos nos sistemas de agendamento de consultas e cirurgias, bem como no sistema de faturamento e cobrança, é crucial implementar uma série de medidas de segurança. Manter backups automáticos e em tempo real dos dados, além de usar sistemas com alta disponibilidade, garante que as informações possam ser recuperadas rapidamente em caso de falha, ataque cibernético ou desastre natural. A criptografia dos dados sensíveis, é essencial para proteger informações confidenciais e evitar acessos não autorizados. Além disso, o uso de autenticação multifator onde os usuários forneçam mais do que uma senha para acessar contas, aplicativos ou redes assegura que apenas pessoas autorizadas possam acessar e modificar esses dados.

Além disso, o treinamento contínuo dos colaboradores em boas práticas de segurança da informação é essencial para prevenir erros humanos, que podem comprometer a segurança dos sistemas. Por fim, a proteção física dos servidores, com vigilância e controles de acesso restritos, complementa as medidas de segurança cibernética, garantindo a integridade dos dados em todos os níveis. Essas ações combinadas minimizam os riscos e garantem a proteção das informações e a continuidade das operações hospitalares.

PLANO DE AÇÃO DETALHADO

Definir um plano de resposta e recuperação, detalhando as etapas e prazos para a retomada das operações, designando responsabilidades e recursos necessários.

Implementação de Medidas de Segurança

Ações:

- Backup e Redundância: Estabelecer um sistema de backup automático diário para todos os dados sensíveis, com armazenamento em nuvem e local, garantindo a recuperação rápida em caso de falhas ou ataques.
- Criptografia e Controle de Acesso: Implementar criptografia de ponta a ponta para dados sensíveis e autenticação multifator (MFA) para todos os usuários que acessam os sistemas, reduzindo o risco de acessos não autorizados.
- Monitoramento em Tempo Real: Integrar ferramentas de monitoramento de segurança para detectar e responder a atividades suspeitas em tempo real.

Desenvolvimento de Planos de Contingência

Ações:

- Criação do Plano de Recuperação de Desastres: Elaborar um plano abrangente que detalhe procedimentos para a recuperação de dados, comunicação com pacientes e manutenção da continuidade dos serviços durante emergências.
- Simulações Regulares: Realizar testes semestrais do plano de recuperação de desastres para treinar a equipe e ajustar processos, garantindo que todos saibam como agir em situações críticas.

Treinamento e Conscientização da Equipe

Ações:

- Programa de Treinamento Contínuo: Desenvolver um programa de capacitação para funcionários sobre práticas de segurança da informação, uso seguro de senhas e conformidade com a LGPD.
- Campanhas de Conscientização: Implementar campanhas regulares para reforçar a importância da segurança da informação e manter todos os colaboradores informados sobre novas ameaças e melhores práticas.

SUGESTÃO DE TESTE DO PLANO

Sugerir uma forma de testar o plano de continuidade para garantir sua eficácia (ex.: simulação de cenário de crise).

Para testar se nosso plano de continuidade realmente funciona quando algo dá errado com a tecnologia dos sistemas e não conseguimos acessar os prontuários dos pacientes, podemos fazer uma simulação. Essa simulação vai nos ajudar a ver como a equipe reage a uma situação em que os prontuários eletrônicos estão fora do ar.

Primeiro, precisamos planejar a simulação. Vamos imaginar um cenário em que ocorre uma falha, como um problema no servidor ou na rede. É essencial que incluamos pessoas de várias áreas, como a equipe de TI, a administração, o atendimento ao paciente, médicos e enfermeiros, e que cada um saiba o que precisa fazer.

Durante a simulação, todos serão informados sobre a "falha" e que não poderão acessar os prontuários eletrônicos. A equipe precisará seguir os planos de emergência, como acessar informações importantes em registros físicos, ligar para os pacientes ou usar formulários em papel para registrar dados importantes. Enquanto isso, teremos observadores que vão acompanhar a resposta da equipe e anotar como tudo está acontecendo, se as diretrizes estão sendo seguidas e se a comunicação está fluindo bem.

Após a simulação, é fundamental reunir todos para discutir o que funcionou e o que pode ser melhorado. Com essas lições, o plano de continuidade deve ser atualizado para corrigir qualquer falha que tenha sido identificada. Também é importante marcar simulações regulares no futuro para garantir que a equipe esteja sempre pronta para lidar com problemas na tecnologia.

Esse tipo de prática ajuda a equipe a validar o plano de continuidade e a se preparar para situações reais em que o acesso aos prontuários dos pacientes possa ser afetado, garantindo que o atendimento aos pacientes continue sem interrupções.