**UNIVERSIDADE SÃO JUDAS TADEU- MOOCA**

**AMBIENTES COMPUTACIONAIS- SEGURANÇA**

**Emilly dos santos ferreira - 825153657**

**Rafaela Maria da Silva - 825134501**

**Douglas Evangelista - 82516629**

**Rafael Gomes Taiar - 825113488**

**Henrique Lima Cândido – 825156385**

**Larissa Oliveira dos Santos - 82516871  
Professor: Robson Calvetti**

**ELABORAÇÃO DO PLANO DE CONTINUIDADE DE NEGOCIOS- (BCP)**

**São Paulo**

**2025**

**Empresa:**

Uma empresa de E-commerce que faz a acessória ou consultoria de marketplaces, startup, com o total de 5 funcionários, esta empresa tem 2 pessoas que trabalham em home office e as demais presencial.

Como trabalhamos: O cliente contrata nossa empresa em 6 meses ou 12 meses para entrarmos no marketplace dela e alavancar suas vendas, com várias estratégias, temos acesso as senhas, contas, usuários e e-mail dos clientes através de contratos e dados sigilosos.

Os sistemas que são utilizados em hardware:  
2 **MacBook Air M2 (2022) 13.6" midnight 8GB de Ram - 256GB SSD - Apple M.**

3 **Notebook Samsung Galaxy Book4 Intel Core i3 8GB RAM SSD 256GB 15,6" Full HD Windows 11NP750XGJ-KG5BR.**

Os sistemas utilizados em software:

**Chrome e Pacote Office.**

**Recursos críticos identificados:**

* Infraestrutura física: Hardwares citados acima.
* Software: Google Chrome é utilizado para o acesso do marketplace e outras ferramentas e o Pacote office para comunicação interna, gestão dos documentos e planejamentos.
* Funcionários: Capturam clientes e implementam as estratégias para impulsionar as vendas.
* Acesso a dados sensíveis: Como senhas de acesso, contas de usuários, informações dos clientes e seus respectivos e-mails corporativos.

Alerta: Esses dados são essenciais para a realização dos serviços, ou seja, devem ser protegidos contra invasões e acessos não autorizados.

* Internet de alta velocidade: Pois garante a qualidade da comunicação entre os colaboradores e clientes além de melhor eficiência do trabalho remoto.
* Servidor e armazenamento em nuvem: Backup seguro de documentos e dados estratégicos.
* Sistemas de proteção: firewall, antivírus e autenticação multifatorial para evitar ataques cibernéticos.
* E-mails corporativos para comunicação com clientes e fornecedores.
* Plataformas de marketplace como a Amazon, Mercado Livre e Shopee.
* Softwares para avaliar os resultados e monitoramento de desempenho.

**Análise de Impacto nos Negócios (BIA)**

* Falha de TI/Hardware (MacBook, Notebooks, Internet): O impacto é alto. Paralisia nas operações diárias e acesso aos dados dos clientes.
* Falha de Software (Google Chrome, Pacote Office, Ferramentas de Monitoramento): Possui impacto médio. Interrupção em tarefas diárias e análise de desempenho
* Ataque Cibernético (Phishing, Ransomware): Nesse caso o impacto é crítico. Roubo de dados sensíveis e comprometimento da reputação.
* Desastres Naturais (Falta de Energia, Enchentes): o impacto é médio a alto. Danos à infraestrutura física e interrupção de trabalho presencial.
* Problemas de Conectividade de Internet: o impacto é alto. Atrasos em vendas e comunicação com clientes
* Falta de Funcionários (Doença, Saída Voluntária): o impacto é médio. Sobrecarga de tarefas e atrasos nas entregas.

**Estratégias de Recuperação**

Para garantir a continuidade dos negócios diante de falhas ou eventos imprevistos, foram definidas estratégias de recuperação:

* Redundância de Sistemas: Será garantida através da manutenção de equipamentos de backups, como notebooks e modens extras, instalação previa de software alternativos devem ser feitas, como Firefox em caso de falha do Chrome e LibreOffice para substituir temporariamente o Office.
* Backup de Dados: Fazer backups automáticos diários em serviços de nuvem confiáveis, esses backups devem ser criptografados para proteger informações dos clientes.
* Plano de Comunicação em Caso de Emergência: Criação de grupos internos em apps de mensagens, e-mails emergenciais para comunicação ágil entre os colaboradores, mensagens pré-programadas para informar clientes sobre a atual situação, nomear um responsável para atualizar os canais de atendimentos.
* Segurança da Informação: Utilizar de autenticação multifator (MFA) em todas as contas de sistemas e e-mails corporativos, Firewall ativo e antivírus atualizado em todos os dispositivos, restrição de acesso a dados conforme nível de responsabilidade de cada funcionário.
* Conectividade e Operação Remota: Contratação de internet móvel 4G como alternativa à rede fixa, Softwares baseados em nuvem acessíveis por todos os funcionários, incluindo os em home office, Equipamentos preparados para trabalho remoto imediato (com VPN e ferramentas necessárias instaladas),
* Gestão de Equipe e Continuidade Operacional: Praticar treinamento cruzado entre os funcionários para garantir que as funções essenciais possam ser realizadas por mais de uma pessoa.

**Plano de Ação Detalhado**

Para garantir a segurança da informação, será implementada a autenticação multifatorial em todas as contas e sistemas utilizados, além da instalação de antivírus e firewall atualizados nos cinco equipamentos da empresa. Será criada uma política interna de senhas fortes com trocas periódicas obrigatórias e adotado um gerenciador de senhas corporativo. A equipe passará por treinamentos mensais sobre segurança digital, como prevenção contra-ataques de phishing, ransomware e práticas de navegação segura. Para assegurar a continuidade dos negócios, será contratado um serviço de backup automático na nuvem, como Google Drive ou OneDrive, e configurado um plano de contingência para falhas na internet, incluindo a utilização de roteadores 4G de emergência. Os processos internos e acessos sensíveis serão documentados com controle de acesso, e testes periódicos de restauração de dados serão realizados. Na gestão de pessoas, será promovido o treinamento cruzado entre os colaboradores para que todos saibam realizar funções críticas, e um manual de procedimentos operacionais será criado para orientar em caso de ausências. A comunicação entre equipe remota e presencial será fortalecida com reuniões semanais. Quanto à infraestrutura de TI, haverá uma rotina de manutenção preventiva nos dispositivos, e um notebook reserva será adquirido como plano de contingência. Também será contratada internet com redundância para evitar falhas de conectividade. No aspecto operacional, será adotada uma ferramenta de gestão de tarefas como o Trello ou ClickUp, com padronização de relatórios de desempenho para os clientes. Canais de atendimento profissional, como e-mails corporativos com domínio próprio e WhatsApp Business, serão utilizados. Todos os colaboradores deverão assinar um código de conduta e termos de confidencialidade.

Plano de Ações por Área

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Área | Ação | Prazo | Responsável | Recursos |
| Segurança da Informação | Implementação de MFA | Dia 1 a 6 | Equipe de TI | Google/Microsoft Authenticator |
| Segurança da Informação | Instalação de Antivírus e Firewall | Dia 1 a 3 / Mensal | Suporte Técnico / TI | Kaspersky, Bitdefender |
| Segurança da Informação | Política de Senhas Fortes | Dia 1 a 4 | RH e TI | Gerenciador de senhas |
| Segurança da Informação | Treinamento de Segurança Digital | Mensal (início Semana 2) | RH / Consultor | Vídeos, simulações |
| Continuidade dos Negócios | Backup na Nuvem | Dia 1 a 4 | TI | Google Drive / OneDrive |
| Continuidade dos Negócios | Plano de Contingência de Internet | Semana 1 a 2 | TI | Roteador 4G |
| Continuidade dos Negócios | Testes de Restauração de Dados | A partir do mês 2, trimestral | TI | Sistema de backup |
| Gestão de Pessoas | Treinamento Cruzado | A partir da Semana 3 | Supervisores | Planos de aula, checklists |
| Gestão de Pessoas | Manual de Procedimentos | Semana 2 a 4 | Líderes de equipe | Documentos em nuvem |
| Gestão de Pessoas | Reuniões Semanais | A partir da Semana 1 | Coordenação | Google Meet, Teams |
| Infraestrutura de TI | Manutenção Preventiva | A partir do mês 2, bimestral | TI | Ferramentas de diagnóstico |
| Infraestrutura de TI | Notebook Reserva | Semana 2 a 3 | Administração / TI | Notebook sobressalente |
| Infraestrutura de TI | Internet com Redundância | Semana 3 a 4 | TI | Dois modens |
| Operações e Atendimento | Gestão de Tarefas (Trello/ClickUp) | Semana 1 a 2 | Gestão de Projetos | Ferramenta online |
| Operações e Atendimento | Relatórios Padronizados | Semana 2 a 3 | Comercial / Suporte | Modelos Excel/Docs |
| Operações e Atendimento | Canais Profissionais de Atendimento | Semana 2 a 3 | Comercial / Marketing | E-mail e WhatsApp Business |

**Teste do Plano de Continuidade de Negócios**

**Objetivo:**Avaliar a eficácia das estratégias definidas no BCP e garantir que a empresa consiga manter suas operações mesmo diante de falhas ou eventos críticos.

**1. Simulação de Falha de Internet (Conectividade)**

**Como testar:** Desligar a internet principal de forma controlada por 2 horas (fora do horário de pico). Ativar o roteador 4G configurado como contingência. Verificar se os colaboradores (presenciais e home office) conseguem acessar os sistemas via nuvem.

**Critério de sucesso:** Operações críticas continuam funcionando, sem perda de dados ou grandes atrasos.

**2. Simulação de Ataque Cibernético (Phishing)**

**Como testar:** Enviar um e-mail simulado de phishing para os colaboradores (com aviso prévio ao fim do teste). Verificar quem clicaria no link falso. Aplicar um mini treinamento logo após o teste.

**Critério de sucesso:** Baixo índice de cliques no link malicioso e boa adesão ao treinamento posterior.

**3. Teste de Restauração de Backup**

**Como testar:** Escolher um arquivo crítico salvo na nuvem. Simular sua exclusão e restaurá-lo a partir do backup.

**Critério de sucesso:** O arquivo deve ser recuperado em até 30 minutos com integridade garantida.

**4. Simulação de Ausência de Funcionário-chave**

**Como testar:** Um colaborador-chave “entra de férias fictícias” por um dia. Outro colaborador assume as tarefas dele com base no manual de procedimentos.

**Critério de sucesso:** As entregas e tarefas seguem sem grandes gargalos, mostrando que o treinamento cruzado está eficaz.

**5. Teste de Comunicação de Emergência**

**Como testar:** Simular um incidente e ativar os canais de comunicação de emergência (grupo interno, e-mails rápidos). Verificar o tempo de resposta da equipe e a clareza das instruções.

**Critério de sucesso:** Todos os membros são informados em até 15 minutos e sabem o que fazer.

**Conclusão**

Esses testes devem ser documentados com:  
- Data e hora  
- Responsável  
- Resultado  
- Lições aprendidas  
- Ações de melhoria  
  
Recomenda-se repetir esses testes a cada 3 ou 6 meses, ajustando o plano conforme as descobertas.