LISTA DE FIGURAS

SUMÁRIO

1 OBJETIVO

O presente Plano de Continuidade de Serviços de TIC (PCTIC) tem como objetivo o estabelecimento dos procedimentos necessários para assegurar a continuidade dos serviços tecnológicos considerados de caráter crítico para a [redacted] definindo as ações a serem tomadas em casos de incidentes ou desastres que resultem em indisponibilidade, incluindo acidentes naturais, intencionais, bem como falhas sistêmicas ou humanas que possam ocorrer durante o processo, tentando prever e mitigar os danos e riscos. Especificamente, este plano abrange ações a serem tomadas quando da ocorrência de incidentes relacionados à falta de energia, incêndio, ataque cibernético, inundação e indisponibilidade parcial ou total da infraestrutura.

2 RESPONSÁVEIS PELA CONTINUIDADE DE NEGÓCIO

A tabela abaixo apresenta as informações das pessoas responsáveis pelas ações de continuidade de negócios na Corretora, cujos papéis estão definidos ao longo deste documento para cada risco identificado.

[redacted]	Função	Telefone e Whatsapp	E-mail
[redacted]	Sócio Administrator	71 99999 9999	antonio.cerqueira@lagosseguros.com.br
[redacted]	Sócio	71 99999 9999	luiz.silva@lagosseguros.com.br
[redacted]	Funcionário	71 99999 9999	jorge.fraga@lagosseguros.com.br

3 ANÁLISE DE IMPACTO AOS NEGÓCIOS (BIA)

Foi realizada uma análise de impacto aos negócios (BIA), considerando as áreas de negócio da Corretora, concluindo-se que as áreas vitais e respectivos processos vitais estão contemplados no quadro abaixo. Nele também é possível identificar os sistemas dos quais cada processo vital depende e o tempo em que a empresa pode sobreviver com a infraestrutura de TI e serviços interrompidos (RTO).

Área	Processos Vitais	Classificação	Sistemas	RTO
Financeiro	Contas a receber	Vital	Teleport, link, e-mail e site do banco	2 DIAS
Vendas	Venda de seguro novo	Vital	Teleport, link e site de seguradoras	2H
Vendas	Renovação	Vital	Teleport, link, site seguradoras	12H

O negócio principal da [redacted] a venda de seguros, fazendo com que as áreas vitais da empresa sejam Vendas, que tem o maior fluxo de atividades indispensáveis e o departamento Financeiro, que o responsável por controlar receitas e despesas.

A tabela a seguir informa o nível de criticidade de cada sistema utilizado pelos processos críticos.

Ferramentas	Criticidade
Teleport	Alta
Link	Alta
Sites de Seguradoras	Alta
E-mail	Média
Site do banco	Média
Site da Corretora	Baixa
Whatsapp	Média

4 ANÁLISE DE RISCOS

Conforme item 8.2.3 Avaliação de riscos da norma ABNT NBR ISO 22301:2020, a organização deve implementar e manter um processo de avaliação de riscos, para identificar os riscos de disrupção das atividades priorizadas da organização e de seus requisitos de recursos, analisar e avaliar os riscos identificados e determinar quais riscos requerem tratamento. A análise apresentada a seguir detalha o risco, suas causas, consequências, probabilidade de ocorrência, impacto e controle a serem observados para garantir a continuidade de serviços de TI.

Interrupção de Energia Elétrica

Causa:	• Falha no sistema de distribuição de energia por parte do provedor do serviço • Curtos-circuitos • Falha humana • Defeito em algum dos componentes do circuito elétrico (disjuntores, fusíveis, etc.)
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos
Probabilidade:	Média
Impacto:	Médio
Controle:	Instalação de nobreaks
Ação:	• Utilizar a carga temporária do nobreak para priorizar atividades vitais • Migrar o trabalho para homeoffice (uma pessoa) • Contatar imediatamente a concessionária de energia para identificar previsão de retorno

Incêndio

Causa:	• Ações humanas • Curto circuito
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos
Probabilidade:	Baixa
Impacto:	Alto
Controle:	Presença de extintores de incêndio
Ação:	• Retirar as pessoas com segurança do lugar • Solicitar uso de extintores ao vigilante • Chamar os bombeiros • Retirar computadores, se possível

Ataque Cibernético

Causa:	• Falha humana relacionada a configuração das regras de segurança do G Suite • Falta de atualização do antivírus instalados nos endpoints • Manutenção de sistemas operacionais desatualizados • Falta de treinamento dos colaboradores em conscientização sobre segurança cibernética • Compartilhamento inseguro de credenciais
Consequência:	• Roubo ou perda de informações • Vazamento de informações críticas dos clientes e colaboradores • Indisponibilidade de recursos e serviços informatizados • Comprometimento da imagem institucional
Probabilidade:	Médio
Impacto:	Alto

Controle:	• Manutenção dos recursos de atualização automática do sistema operacional e seus aplicativos • Revisões periódicas nas regras de filtragem do e-mail • Plano de Capacitações periódicas relacionadas ao tema • Implementar rotinas de backup full e incremental em ferramenta contratada
Ação:	• Isolar o computador da rede • Rodar antivírus atualizado no equipamento e manter ameaças em quarentena para análise forense futura • Verificar se ataque pode atingir outros equipamentos e tentar impedi-lo • Substituir as credenciais de acesso ao Teleport, site das Seguradoras e e-mail • Acionar o suporte do G Suite, em caso de invasão ao e-mail ou console de administrador • Documentação, relatórios e registros sobre o incidente • Comunicar autoridades e partes interessadas, se necessário • Acionar backups • Acionar equipamento reserva • Utilizar estrutura de apoio técnico das Seguradoras via telefone, para atender as demandas de vendas dos clientes

Desastres Naturais

Causa:	• Chuvas • Alagamentos • Raios
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Dano físico nos equipamentos e instalações
Probabilidade:	Baixo
Impacto:	Médio
Controle:	• Adoção de infraestrutura remota redundante (própria ou contratada) • Instalação de para raio no prédio
Ação:	• Alugar computadores • Ligar para o provedor de internet para consertar equipamento ou sinal • Rotear dados móveis • Migrar o trabalho para homeoffice

Indisponibilidade de serviços de TI

Causa:	• Falha nos equipamentos de rede (modem) • Rompimento no cabeamento existente • Gestão ineficiente de antivírus • Queima de componentes eletrônicos dos equipamentos • Quedas ou oscilações de energia; • Falhas na execução dos Jobs de backup • Sistema Teleport fora do ar • Sites de Seguradoras fora do ar • Link de internet inoperante
Consequência:	• Indisponibilidade de recursos e serviços informatizados • Roubo ou perda de informações • Indisponibilidade do Teleport • Indisponibilidade dos sites das Seguradoras • Impossibilidade de acesso à internet • Interrupção das vendas, em função de não ter backup disponível
Probabilidade:	Baixa
Impacto:	Médio
Controle:	• Contratação de ferramenta de backup para informações de clientes e apólices em vigor, com monitoramento semanal e realização de testes periódicos de restauração • Implementar atualização automática de antivírus nas máquinas • Revisar o cabeamento

Ação:	• Realizar cotações e fechamento de seguros diretamente no site das Seguradoras, caso o Teleport esteja fora do ar • Utilizar estrutura de apoio técnico das Seguradoras via telefone, para atender as demandas de vendas dos clientes, caso os sites das Seguradoras estejam fora do ar • Acionar backup • Acionar equipamento reserva • Migrar o trabalho para homeoffice • Substituir cabo rompido • Manutenção corretiva imediata do equipamento

5 PLANOS DE AÇÃO

Interrupção de Energia Elétrica

Ação	Responsável	Quando
Utilizar a carga temporária do nobreak para priorizar atividades vitais	Automático	Imediato
Migrar trabalho para home office (uma pessoa)	Todos	1h após início do desastre
Contatar imediatamente a concessionária de energia para identificar previsão de retorno	Funcionária	2h após início do desastre

Incêndio

Ação	Responsável	Quando
Retirar as pessoas com segurança do lugar	Sócio	Imediato
Solicitar uso de extintores ao vigilante	Funcionária	Imediato
Chamar os bombeiros	Funcionária	Após chamar o vigilante
Retirar computadores, se possível	Todos	Quando possível

Ataque Cibernético

Ação	Responsável	Quando
Isolar o computador da rede	Funcionária	Imediato
Rodar antivírus atualizado no equipamento e manter ameaças em quarentena para análise forense futura	Funcionária	Após isolar computador da rede
Verificar se ataque pode atingir outros equipamentos e tentar impedi-lo	Funcionária	Após isolar computador da rede
Substituir as credenciais de acesso ao Teleport, site das Seguradoras e e-mail	Funcionária e Sócio	Imediato
Acionar o suporte do G Suite, em caso de invasão ao e-mail ou console de administrador	Sócio administrador	Imediato
Acionar backups	Funcionária	Após atividades de contenção da ameaça

Ação	Responsável	Quando
Acionar equipamento reserva	Sócio	Após atividades de contenção da ameaça
Utilizar estrutura de apoio técnico das Seguradoras via telefone, para atender as demandas de vendas dos clientes	Funcionária e Sócio	Caso haja indisponibilidade do backup, sistemas ou computador
Documentação, relatórios e registros sobre o incidente	Sócio administrador	Durante as fases da crise e após
Comunicar autoridades e partes interessadas, se necessário	Sócio administrador	De acordo com as regulamentações normativas

Desastres Naturais

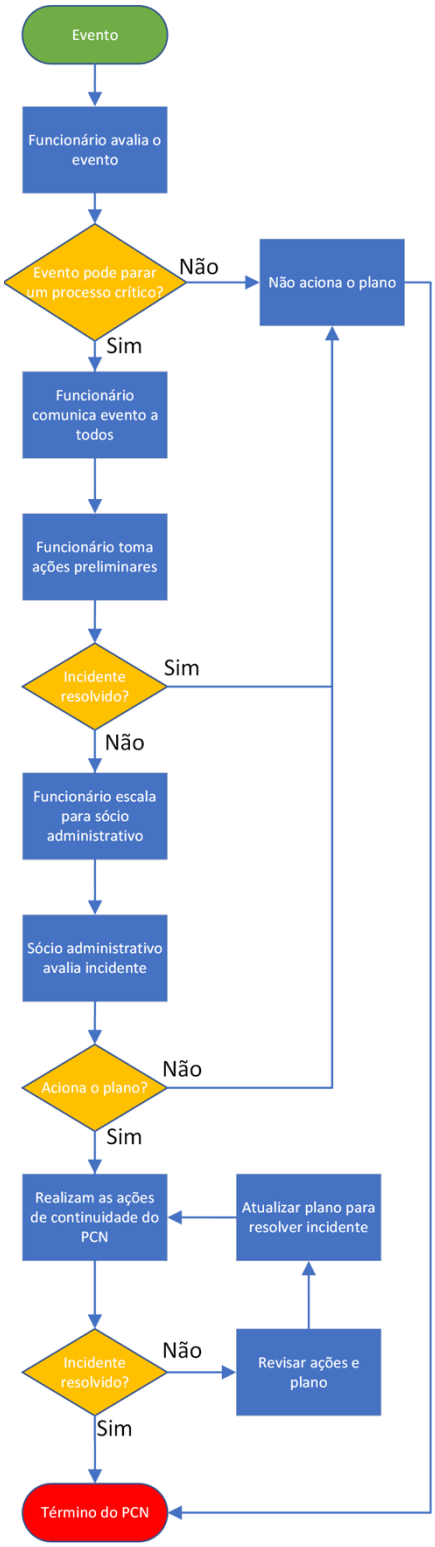
Ação	Responsável	Quando
Alugar computadores	Sócio administrador	Assim que verificada a indisponibilidade dos equipamentos atuais
Ligar para o provedor de internet para consertar equipamento ou sinal	Funcionária	Imediato
Rotear dados móveis	Funcionária e Sócio	Imediato
Migrar o trabalho para homeoffice	Todos	Imediato

Indisponibilidade de Serviços de TI

Ação	Responsável	Quando
Realizar cotações e fechamento de seguros diretamente no site das Seguradoras, caso o Teleport esteja fora do ar	Funcionária e Sócio	Imediato
Utilizar estrutura de apoio técnico das Seguradoras via telefone, para atender as demandas de vendas dos clientes, caso os sites das Seguradoras estejam fora do ar	Funcionária e Sócio	Imediato
Utilizar informações do backup	Funcionária e Sócio	Imediato
Migrar o trabalho para homeoffice	Funcionária e Sócio	Após 2h sem internet
Substituir cabo rompido	Funcionária e Sócio	Imediato
Solicitar manutenção corretiva do equipamento	Funcionária	Imediato

A Figura 1 representa o fluxo de atuação da equipe para resolver problemas gerados a partir de um evento relacionado aos riscos de continuidade descritos acima. Este fluxo será adotado na concretização de qualquer um dos riscos.

FIGURA 1 - ATIVAÇÃO DO PLANO



Fonte: Elaborado pelos autores, 2023

6 PONTOS DE CONTROLE

Pontos de controle em um Plano de Continuidade de Negócios (PCN) referem-se a marcos ou indicadores específicos que são estabelecidos para avaliar o progresso e a eficácia do plano. Eles desempenham um papel fundamental na gestão e na garantia de que o plano de continuidade de negócios está sendo implementado conforme o planejado e que a organização está preparada para lidar com situações de interrupção dos negócios.

Os pontos de controle do PCN devem incluir a garantia de que os recursos necessários, como equipamentos, pessoal, instalações e sistemas de backup, estejam prontos e disponíveis quando necessário, assim como investir na capacitação dos responsáveis pelo plano, buscando a avaliação da formação e do treinamento contínuo.

Também deve-se realizar testes regulares e exercícios simulados para verificar a eficácia do plano em cenários de interrupção, verificando a atribuição de responsabilidades e funções específicas para os membros da equipe de resposta a crises e continuidade de negócios.

Ainda, é importante avaliar a eficácia dos procedimentos de comunicação de emergência, sejam eles com partes interessadas internas e externas, bem como verificar a prontidão e atualização dos planos de recuperação de sistemas, aplicativos e processos críticos, para garantir que eles estejam alinhados com as mudanças na organização, as ameaças e as melhores práticas.

Por fim, deve-se realizar o monitoramento contínuo da avaliação de riscos para identificar novas ameaças e vulnerabilidades, estabelecer indicadores-chave de desempenho (KPIs) para medir a eficácia do plano e a recuperação de negócios, e realizar auditorias internas e revisões independentes para garantir a conformidade e a eficácia do plano.

Os pontos de controle estabelecidos neste plano são:

- Verificar a cada revisão do PCN que há um nobreak instalado e operacional;
- Verificar periodicamente se os extintores são adequados aos riscos e sua validade;
- Realizar manutenções preventivas dos recursos de atualização automática do sistema operacional e seus aplicativos;
- Realizar revisões periódicas nas regras de filtragem do e-mail;
- Revisar se as rotinas de backup full e incremental da ferramenta contratada estão funcionando corretamente;
- Atualizar a cada revisão do PCN a lista de escritórios de coworking disponíveis na região;
- Verificar as condições de instalação do para raio no prédio;

- Verificar periodicamente se os antivírus estão habilitados nas máquinas e com as assinaturas atualizadas;
- Revisar o cabeamento de rede a cada revisão do PCN;
- Plano de Capacitações periódicas relacionadas ao tema;
- Avaliar a eficácia do treinamento contínuo dos responsáveis pelas ações de continuidade;
- Realizar um teste de mesa com os responsáveis pela continuidade das atividades da Corretora para atualizar ou validar os processos estabelecidos no PCN, revisando suas políticas, procedimentos, responsabilidades e vulnerabilidades, verificando também as ações estabelecidas como pontos de controle;
- Verificar disponibilidade dos meios de comunicação;
- Elaborar um histórico mensal do funcionamento dos canais de comunicação da Corretora, relatando eventuais defeitos e indisponibilidade nos ativos computacionais e interrupção dos serviços das operadoras;
- Verificar se os canais de comunicação estão adequados;
- Atualizar o PCN anualmente para garantir que ele esteja alinhado com as mudanças na organização, nas ameaças e nas melhores práticas;
- Monitoramento contínuo da avaliação de riscos para identificar novas ameaças e vulnerabilidades, através da análise do contexto interno e externo da Corretora;
- Revisar os indicadores-chave de desempenho (KPIs): Tempo de Recuperação (RTO - Recovery Time Objective), Ponto de Recuperação (RPO - Recovery Point Objective), Taxa de Disponibilidade dos sistemas, Testes de Recuperação Bem-sucedidos, Tempo de Ativação dos Planos, Número de Incidentes de Recuperação, Avaliação de Impacto de Negócios (BIA - Business Impact Assessment), Taxa de Atualização do Plano;

Esses pontos de controle são fundamentais para garantir que o plano de continuidade de negócios seja dinâmico e eficaz, adaptando-se às mudanças nas circunstâncias e nas necessidades da organização, e garantindo que a empresa possa continuar operando de maneira eficaz, mesmo em face de interrupções inesperadas.

7 PROCEDIMENTO DE SIMULAÇÃO

Procedimento: instalação de códigos maliciosos

1. Escolha um computador que esteja fora da operação, que utilize o sistema operacional Windows e o antivírus Kaspersky para simular uma invasão de dispositivo, com execução de programas maliciosos, por um especialista em testes de invasão;
2. Apague os logs e informações de cache, referentes às senhas e acessos ao Teleport e sites de Seguradoras;
3. Estabeleça um momento para interromper a atualização das assinaturas de identificação de vírus;
4. Agende o dia da simulação e comunique previamente os funcionários e sócios da Corretora;
5. Realize a simulação com a instalação de programas maliciosos, que podem danificar o sistema e deixá-lo inoperante;
6. Execute um antivírus, atualize as assinaturas de identificação de vírus para prevenir novos ataques e coloque os vírus identificados em quarentena para análise forense;
7. Avalie os danos causados pela simulação;
8. Elabore um relatório com as lições aprendidas e os pontos que servirão de insumos para a revisão e atualização do plano de continuidade de negócios;
9. Comunique os resultados aos sócios e funcionários.

8 CONTATOS EM EMERGÊNCIA

Entidade	Contato
Bombeiro	Telefone
Polícia	Telefone
SAMU	Telefone
ANPD	Site
Defesa Civil	Telefone
Companhia de Energia Elétrica	Telefone
Seguradoras	Telefone, chat, site, gerente comercial
Segurados	Telefone, Whatsapp, e-mail
Teleport	Telefone, chat, site, gerente comercial
Técnico de Informática	Telefone, Whatsapp, e-mail
Vivo	Telefone, Whatsapp, e-mail
Fornecedor de Backup	Telefone, chat, site

9 CONTROLE DE VERSÃO

Versão	Data	Nome	Ação	Conteúdo
1.0	20/10/2023	[redacted]	Elaboração	Primeira versão do documento