Plano de Continuidade de Negócios e Gestão de Crises

Santos Bevilaqua Advogados

Sumário

1. Objetivo

Para garantir a integridade do Santos Bevilaqua Advogados, é fundamental focar nos seguintes objetivos em situações de crise:

Assegurar a continuidade das operações críticas, mantendo os serviços essenciais funcionando, mesmo diante de adversidades.

Minimizar os impactos negativos, reduzindo os danos a clientes, colaboradores e às operações em geral.

Garantir a proteção dos dados pessoais, cumprindo rigorosamente a Lei Geral de Proteção de Dados (LGPD) para salvaguardar as informações.

Cumprir as exigências regulamentares da OAB, conservando a conformidade com as normas e diretrizes da Ordem dos Advogados do Brasil.

Proteger a reputação e a integridade do escritório, preservando a imagem e a confiabilidade da organização no mercado.

Conceitos fundamentais:

Gestão de Crise: Qualquer situação que ameace interromper as operações do escritório ou comprometer a reputação da empresa e/ou de seus clientes.

Continuidade de Negócios: É a capacidade de manter as operações essenciais funcionando tanto durante quanto após uma crise.

2. Identificação e Avaliação de Riscos

O Santos Bevilaqua Advogados fará análises de risco periódicas para identificar possíveis ameaças às suas operações. Essas análises vão incluir, mas não se limitar a:

Riscos cibernéticos: Ameaças relacionadas a ataques virtuais, vazamento de dados etc.

Desastres naturais: Eventos como enchentes, terremotos ou vendavais que possam afetar a estrutura ou as operações.

Interrupções de infraestrutura: Problemas como falta de energia elétrica ou falhas nos sistemas de TI.

Pandemias e emergências de saúde pública: Situações que possam impactar a saúde dos colaboradores e a continuidade dos trabalhos.

Incidentes de segurança física: Eventos como roubos, furtos ou acessos não autorizados às instalações.

Conflitos internos e disputas legais: Situações que podem gerar instabilidade no ambiente de trabalho ou impactos jurídicos.

3. Análise de Impacto de Riscos

A avaliação dos riscos é conduzida em conformidade com as diretrizes do Disaster Recovery International Institute (DRII), para mitigar os riscos operacionais, identificamos as principais ameaças e as medidas preventivas adotadas para contê-las, detalhando os procedimentos que escritório utiliza para cada item mencionado.

Critério	Baixo (1 ponto)	Médio (3 pontos)	Alto (5 pontos)
Gravidade	Incidente menor, que não causa impacto significativo	Incidente com impacto moderado, que pode ser contido sem maiores danos	Impacto crítico para a organização, como perda de dados sensíveis ou interrupção de serviços essenciais
Urgência	Pode ser resolvido em prazo mais estendido	Deve ser tratado em curto prazo, mas não requer ação imediata	Necessita de ação imediata para evitar maiores danos
Impacto	Atinge uma pequena parte da organização com impacto restrito	Impacta uma parte significativa da organização, mas com danos limitados	Grande número de sistemas, usuários ou dados comprometidos
Probabilidade de Recorrência	Incidente isolado, com baixa probabilidade de repetição	Pode ocorrer novamente, mas de forma esporádica	Grande chance de ocorrer novamente se não for tratado adequadamente

Classificação	Pontuação
Criticidade Muito Alta	15 a 20 pontos
Criticidade Alta	10 a 15 pontos
Criticidade Média	5 a 10 pontos
Criticidade Baixa	0 a 5 pontos

Figura 1 A classificação de riscos deve ser realizada em conjunto pela Equipe Técnica de Resposta a Incidentes e pelo Encarregado de Dados Pessoais (DPO).

3.1.Avaliação de Impacto dos Serviços de TI

Recurso - Serviço	Criticidade	Backup	Restabelecer
Internet	Alta	8 horas	8 horas
E-mail	Alta	8 horas	8 horas
Site	Alta	24 horas	8 horas
Impressão e digitalização de documentos	Alta	-	8 horas
Rede cabeada	Alta	24 horas	8 horas
Rede Wi-Fi	Alta	24 horas	8 horas
Telefonia fixa	Alta	24 horas	8 horas

3.2.Suporte Técnico

O suporte técnico do escritório é de responsabilidade da empresa terceirizada 3A Plus Serviços de Informática Ltda que atua na manutenção e suporte técnico de equipamentos de informática, cobrindo os seguintes itens:

Atividades
Suporte remoto: Atendimento via telefone ou por mensageiro eletrônico.
Aquisição de equipamentos: Definição de compras emergenciais de equipamentos
Instalação de software: Instalação de sistemas operacionais
Configuração e suporte de rede: Configuração e suporte a controladores de domínio e servidores DNS
Administração de servidores: Instalação e administração de servidores
Recuperação de dados: Restauração de backups offline
Configuração de estações de trabalho: Instalação de equipamentos e periféricos aos colaboradores
Suporte a conectividade: Suporte a rede local e internet
Atualizações: Realização de atualizações de programas, drivers e sistemas operacionais
Gestão de backups: Definição e verificação da política de backups
Controle de ativos: Inventário de equipamentos

3.3. Levantamento de Ameaças

Risco	Causa	Resultado	Probabilidade
Incêndio	*Ações humanas; *Curtos-circuitos; *Queimadas.	Indisponibilidade de recursos, serviços e sistemas informatizados.	Média
Interrupção de energia elétrica	*Ações humanas; *Curtos-circuitos; *Queimadas; *Vendavais *Chuvas; *Tempestades.	Indisponibilidade de recursos, serviços e sistemas informatizados.- Dano físico nos equipamentos	Média
Desastres naturais	*Vendavais; *Chuvas; *Tempestades; *Alagamentos.	Indisponibilidade de recursos, serviços e sistemas informatizados	Média
Ataques cibernéticos	*Falha humana relacionada a configuração das regras de segurança dos Sistemas de detecção de intrusos *Desatualização de sistemas operacionais e softwares; *Vulnerabilidades ou erros de configuração em equipamentos, serviços e sistemas operacionais.	*Vazamento de informações críticas tais como: dados sensíveis como senhas e-mails, de sites autenticados, painéis administrativos; *Danos à reputação da empresa; *Perda de dados.	Média

Interrupção da comunicação com o provedor de internet	*Geralmente causado por obras públicas, desastres naturais ou acidentes. *Mau funcionamento de componentes eletrônicos. *Configuração incorreta de roteadores ou firewalls.	Parada na comunicação de dados entre servidores e serviços e sites externos.	Média
Falha na restauração de backups	*Erros de comunicação na rede; *Quedas ou oscilações de energia; *Queima de componentes eletrônicos	*Dados corrompidos; *Perda de dados; Indisponibilidade de Backup; *Indisponibilidade de sistemas informatizados.	Média
Ataques internos	*Falhas de sistema de monitoramento de vulnerabilidades; *Falhas nos mecanismos de proteção contra invasão; *Falhas no sistema de detecção de intrusão	*Roubo ou perda de informações; *Indisponibilidade recursos, serviços e sistemas informatizados.	Alta
Indisponibilidade de pessoas chave para a segurança da informação	*Ausência de capacitações na área de segurança da informação	*Indisponibilidade de serviços, recursos e sistemas informatizados; *Perda de dados. *Roubo de informações.	Alta

Falhas no acesso aos dados armazenados no banco de dados.	*Inexistência de conectividade de rede. -Falhas ou erros na configuração do serviço; *Comprometimento do sistema operacional; *Ataques internos e externos.	*Indisponibilidade de recursos, serviços e sistemas informatizados; *Perda de dados; *Roubo de informações.	Alta
Falhas de conexão com a rede lógica de dados.	Erros de configuração de ativos de rede. *Quedas ou oscilações de energia. *Queima ou falhas de componentes eletrônicos dos ativos de rede. -Falta de conhecimento sobre cabeamento estruturado. *Ausência de capacitações em redes de comunicação de dados. *Falha humana	*Indisponibilidade de recursos, serviços e sistemas informatizados.	Alta
Falhas de validação de credenciais no sistema de autenticação do usuário.	Falhas em componentes eletrônicos; *Falha humana.	*Indisponibilidade de recursos, serviços e sistemas informatizados	Alta
Falha de Hardware	*Queima de componentes eletrônicos.	*Indisponibilidade de recursos, serviços e sistemas informatizados	Média

Indisponibilidade de Informação	*Falha humana. - Erros de sistema; *Falhas em dispositivos de armazenamento; *Falhas na comunicação de dados	*Indisponibilidade de recursos, serviços e sistemas informatizados	Média

3.4. Dotação de Recursos

Para garantir a execução eficiente do Plano de Continuidade de Negócios e Gestão de Crises, diversos recursos são indispensáveis. Para facilitar a compreensão, esses recursos foram categorizados em: recursos humanos, sistemas de comunicação, infraestrutura tecnológica, energia, backups e locais de recuperação.

3.4.1. Recursos Humanos

O escritório Santos Bevilaqua Advogados garantirá a disponibilidade de recursos humanos com a capacitação mínima necessária por meio da contratação de uma empresa terceirizada. Esta empresa deverá possuir notório conhecimento e experiência no mercado, sendo habilitada para configurar recursos, serviços, sistemas e segurança da informação.

O profissional de TI designado para a execução do Plano de Continuidade precisa possuir, no mínimo, os seguintes conhecimentos:

- ⇒ Sistemas de proteção da informação;
- ⇒ Gerência de serviços, sistemas e redes de computadores;
- ⇒ Instalação, configuração e manutenção de sistemas operacionais;
- ⇒ Segurança da informação em infraestrutura de redes, sistemas operacionais e aplicações web.

Proteção contra Incêndio	Sistemas de proteção contra incêndio nas salas de equipamentos.
No-breaks	Nobreaks de grande porte com baterias para estabilizar os ativos de TI na sala de equipamentos.
Servidores	Servidores de rede.
Climatização	Sistema redundante de climatização do ambiente.
Conectividade	Um link de comunicação de dados principal e um link de comunicação de dados redundante.
Virtualização	Software para virtualização de servidores.
Backup	Software para automação de backups.
Gerenciamento de Rede	Software para gerenciamento de redes de computadores.

3.4.2. Sistemas de Comunicação

Para garantir a comunicação com outras entidades e entre suas próprias unidades, o Santos Bevilaqua Advogados necessita de um sistema de dados robusto. Dois links de internet para saída: um primário de 1 e um secundário, garantindo a continuidade da conexão. Internamente, para a troca segura de informações entre unidades será implementada uma Rede Virtual Privada (VPN). Este canal criptografado e seguro será dedicado exclusivamente a serviços e recursos de TI entre as unidades.

3.4.3. Infraestrutura e Segurança de TI – SBA

Para garantir a rápida restauração dos serviços de TI, a infraestrutura tecnológica do Santos Bevilaqua Advogados deve seguir os seguintes requisitos mínimos em cada unidade. Além da infraestrutura, o Santos Bevilaqua Advogados precisa manter seu sistema de gestão de segurança da informação atualizado, seguindo as normas vigentes. O escritório deve adotar, no mínimo, as seguintes recomendações:

Armazenamento Seguro de Dados: Dados sensíveis de colaboradores, prestadores terceirizados e informações institucionais devem ser armazenados em locais seguros, em conformidade com as normas de segurança da informação.

Prevenção de Ataques e Vazamentos: A prevenção contra-ataques e vazamentos de informações deve ser reforçada por meio de:

⇒ Política de segurança da informação.

⇒ Normas complementares sobre segurança da informação.

⇒ Lei Geral de Proteção de Dados (LGPD).

⇒ Firewall.

3.4.4. Energia

Para garantir a continuidade do fornecimento de energia, o Santos Bevilaqua Advogados conta com nobreaks próprios, que oferecem uma autonomia mínima de duas horas como fonte alternativa. Adicionalmente, o edifício em que o escritório está localizado dispõe de geradores movidos a combustível. Em momentos cruciais, o escritório Santos Bevilaqua Advogados assegura a operação ininterrupta de seus sistemas essenciais ao utilizar o suporte de uma empresa líder no mercado de locação de nobreaks. Esses equipamentos garantem uma autonomia de até 11 horas, fornecendo energia confiável sempre que necessário.

3.4.5. Backups e Locais de Recuperação

O Santos Bevilaqua Advogados implementou estratégias de backup local e em nuvem para assegurar a segurança dos dados institucionais. Essas rotinas especificam o tipo de backup a ser executado (completo, incremental e diferencial), a periodicidade do armazenamento dos dados (horária, diária, mensal e anual) e a forma de armazenamento.

Além das estratégias já existentes, novas rotinas automatizadas para a recuperação mensal de dados dos principais serviços de TI em infraestrutura em nuvem devem ser estabelecidas em breve. Essa configuração visa a retomada mais rápida possível dos serviços de TI. O comitê de segurança da Informação é a área encarregada de manter a matriz de acionamento (Plano de Continuidade) sempre atualizada, especialmente no que tange aos serviços de Tecnologia da Informação.

Responsável pela ativação	Comitê de segurança da Informação
Ambiente a ser contingenciado	Infraestrutura computacional- SBA
Quando acionar o Plano de Continuidade?	Na ocorrência de incidentes de interrupção com potencial superior a 24 horas
Quem executa o Plano de Continuidade?	Suporte TI
Qual o tempo de recuperação?	24 horas
Contato	comitesi@santosbevilaqua.com.br
Contato técnico	suporte@santosbevilaqua.com.br

4. Plano de Recuperação Ransomware

Um plano eficaz para recuperar-se de um ataque de ransomware envolve as seguintes etapas:

Identificação e Contenção: Primeiramente, é identificar a origem e o alcance do ataque, determinando quais arquivos e sistemas foram afetados. Em seguida, os dispositivos infectados devem ser isolados da rede, e os backups externos, desconectados para evitar que o malware se espalhe.

Restauração dos Dados: O próximo passo é restaurar os arquivos e sistemas a partir dos backups disponíveis, priorizando os mais críticos para a operação da empresa. Após a restauração, é fundamental verificar a integridade e a funcionalidade desses arquivos e sistemas por meio de testes.

Reforço da Segurança: Para evitar futuros ataques, é essencial reforçar as medidas de segurança. Isso inclui atualizar antivírus, aplicar correções de vulnerabilidades, revisar políticas de acesso e senha, e treinar os usuários sobre boas práticas de prevenção.

Análise Pós-Incidente e Comunicação: Por fim, deve-se elaborar um relatório detalhado do incidente, registrando causas, consequências, ações tomadas e lições aprendidas. A comunicação com clientes, fornecedores e autoridades competentes também é importante, informando sobre

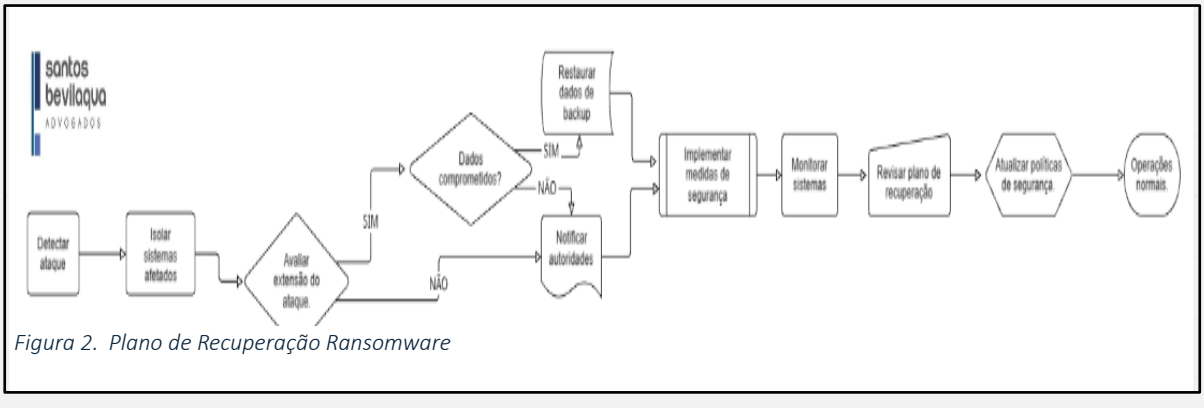

Figura 2. Plano de Recuperação Ransomware

4.1. Recuperação de Sistemas Específicos

No Santos Bevilaqua Advogados , os procedimentos foram mapeados para a recuperação dos principais sistemas em caso de desastre:

Gestão de Documentos Jurídicos (GED), Legal Doc e Legal Desk, assegurar o tipo de conexão e a garantia de segurança e disponibilidade do provedor de serviço impedindo que sejam afetados por ataques de ransomware.

Gestão Jurídica/Linha Sisjuri, conta com backup diário com histórico de 30 dias, o que permite a recuperação de dados perdidos ou corrompidos por um ataque de ransomware.

5. Gerenciamento de Crise de TI

5.1. Avaliação Pós-Incidente/Desastre

A avaliação pós-incidente/desastre é crucial para aprender com o ocorrido e fortalecer a resiliência da sua infraestrutura e equipe de TI. Incluir a equipe técnica de TI nesse processo é fundamental, pois eles possuem o conhecimento prático e a experiência direta com o incidente.

Atividade	Atribuição de Responsabilidade
1. Encaminhar comunicado aos membros do Comitê de sócios sobre o incidente ocorrido	Comitê de segurança da Informação
2. Informar as áreas afetadas sobre a crise ocorrida	
3. Redigir um release sobre o assunto, esclarecendo as condições da ocorrência e reforçando os aspectos favoráveis das medidas adotadas, bem como a idoneidade do escritório.	
4. Identificar o problema que ocasionou a crise	Suporte TI
5. Coletar o máximo de informações e provas possíveis	
6. Identificar o problema	
7. Registrar o motivo por que ocorreu.	
8. Registrar quando ocorreu o problema.	
9. Registrar as consequências em curto e médio prazos.	

10. Registrar quem são os responsáveis pelo ocorrido.	
11. Registrar se houve outras ocorrências.	

5.2. Plano de Comunicação em Situações de Crise

Para garantir transparência e a disseminação de informações corretas durante uma crise, será implementado um Plano de Comunicação abrangente, que contemplará as seguintes frentes:

Informações aos clientes	Será prioritário manter os clientes atualizados sobre o impacto da crise em suas demandas ou serviços e as medidas que estão sendo adotadas pelo escritório para mitigar os efeitos e restabelecer a normalidade.
Comunicação interna	Manter todos os colaboradores informados é crucial para alinhar a equipe, garantir a compreensão da situação e das ações em andamento, e evitar a propagação de informações desencontradas.
Relatórios para autoridades regulatórias	Serão preparados e submetidos relatórios às autoridades regulatórias competentes, conforme a necessidade e as exigências legais, garantindo o cumprimento das obrigações.
Estratégias de comunicação com a mídia	Se a natureza da crise exigir, serão desenvolvidas estratégias específicas para a comunicação com a mídia, visando gerenciar a percepção pública, controlar a narrativa e proteger a reputação do escritório.

5.3. Atividades de Retorno à Normalidade

Atividade	Responsável
Manter funcionando os sistemas de estabilização de energia (Grupo Gerador)	Área de Infraestrutura- TI
Manter funcionando os equipamentos de climatização da sala de equipamentos.	

Garantir a integridade dos ativos de rede para reconexão.	Área de TI- Suporte
Testar os equipamentos de processamento e armazenamento de dados	
Restaurar os serviços de acordo com uma sequência pré-definida de continuidade e restauração.	
Verificar a integridade dos dados e restaurar os backups caso necessário.	
Garantir o retorno dos sistemas de acordo com as demandas pontuais.	
Garantir a integridade dos dados, que podem estar corrompidos ou defasados.	
Garantir que as funcionalidades básicas de acesso estão funcionando novamente.	
Comunicar às partes interessadas o retorno da normalidade.	Comitê de Segurança da Informação

6. Plano de Retorno

6.1. Infraestrutura Local

Com o intuito de assegurar um retorno organizado e seguro ao ambiente de trabalho, este procedimento estabelece diretrizes para os colaboradores após a superação de eventos emergenciais que comprometam a infraestrutura local, tais como incêndios, inundações, quedas de energia ou outras ocorrências imprevistas.

Para garantir um retorno seguro e organizado ao ambiente de trabalho após uma emergência, siga estas etapas:

Autorização Oficial: A entrada no local da ocorrência só será liberada com a permissão das autoridades competentes (bombeiros, polícia ou defesa civil).

Comunicação: Informar o gestor imediato ou com o responsável pela área para receber as instruções detalhadas sobre quando e como retornar. Seguir essas orientações e respeitar a ordem de prioridade definida pelo escritório.

Avaliação das condições do Local: Antes de retomar as atividades, será inspecionado com uma equipe habilitada o ambiente de trabalho da ocorrência. Com intuito de identificar possíveis danos estruturais, equipamentos quebrados, fios expostos, vazamentos ou qualquer outro sinal de perigo.

Trabalho Remoto Temporário: Enquanto o retorno ao escritório não for liberado, todos os colaboradores devem trabalhar em regime de *home office*, seguindo as diretrizes do plano de continuidade de negócios.

6.2. Estações de Trabalho

As diretrizes a seguir detalha como o Santos Bevilaqua Advogados lida com situações de estações de trabalho indisponíveis, cobrindo dois cenários principais: quando apenas um computador falha e quando várias máquinas apresentam problemas simultaneamente.

6.2.1. Cenário de Única Falha em Estações de Trabalho

Se uma única estação de trabalho parar de funcionar, a política é substituí-la de imediato. A máquina com defeito será enviada para conserto, e o usuário receberá um computador substituto para que possa continuar suas tarefas sem interrupções.

6.2.2. Cenário de Múltiplas Falhas em Estações de Trabalho

Em casos em que vários equipamentos do escritório venham falhar ao mesmo tempo, implementaremos uma solução rápida para garantir que as operações não parem: alugaremos equipamentos de empresas parceiras.

Essas parceiras são escolhidas pela capacidade de fornecer computadores de alta qualidade em pouco tempo, além de serem confiáveis e terem um bom histórico em atender emergências.

Assim que a falha em múltiplos computadores for identificada, o suporte de TI entrará em contato com a parceira para iniciar o processo de aluguel. A quantidade de equipamentos alugados será a mesma do número de máquinas que falharam.

Nossa equipe de TI será responsável por configurar e instalar rapidamente os equipamentos alugados, garantindo assegurar a disponibilidade imediata, diminuindo o período de inatividade e permitindo que os colaboradores retornem às suas funções sem impactos significativos.

7. Papéis e Responsabilidades

A definição clara dos papéis envolvidos e de suas respectivas responsabilidades é fundamental para garantir a eficiência e a eficácia no tratamento de incidentes de segurança da informação. Cada ator desempenha um papel específico, alinhado às suas competências e funções, de modo a permitir uma resposta coordenada e ágil em situações críticas.

7.1.Encarregado de Dados Pessoais (DPO)

O Santos Bevilaqua Advogados, nomeou um Encarregado de Dados Pessoais, também conhecido como Data Protection Officer (DPO), para desempenhar um papel importante no processo de proteção de dados, principalmente na resposta a incidentes de segurança da informação. Esse colaborador será o elo de comunicação entre o escritório, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), garantindo a conformidade com a LGPD.

Suas principais responsabilidades relacionadas incluem:

Facilitar a comunicação: Atuando como um facilitador entre a equipe técnica de resposta a incidentes e os gestores. Isso garante que o plano seja seguido corretamente e que todas as ações estejam em conformidade com as exigências da LGPD.

O DPO assegura que os titulares de dados sejam informados de forma clara e transparente sobre quaisquer incidentes que possam afetar seus dados pessoais.

7.2. Assessoria de Comunicação

A Assessoria de Comunicação tem um papel essencial na coordenação das informações durante e após um incidente de segurança, trabalhando em conjunto com o Encarregado de Dados (DPO). Seu objetivo é garantir que toda a comunicação com o público e outras partes interessadas seja clara, transparente e consistente.

Suas principais atribuições são:

Comunicação com os Titulares de Dados: Junto com o DPO, a Assessoria colabora na notificação dos titulares de dados afetados. Isso inclui garantir que as informações sejam precisas, fáceis de entender e divulgadas dentro dos prazos exigidos pela LGPD.

Gestão da Reputação e Crise: A Assessoria de Comunicação cuidará para proteger a imagem do escritório. Cuidando das comunicações sensíveis e gerenciando possíveis crises de reputação que possam surgir em decorrência do incidente.

7.3. Equipe Técnica de Resposta a Incidentes

A Equipe Técnica de Resposta a Incidentes gerencia todos os aspectos técnicos de um incidente, desde a sua identificação até a implementação de medidas preventivas.

Suas principais atribuições incluem:

Detecção e Análise: Utilizam ferramentas de monitoramento e técnicas de investigação para identificar a origem e o alcance do problema, realizando a detecção e análise de incidentes.

Contenção e Erradicação: Garantem a contenção eficaz e a erradicação completa dos problemas, minimizando os danos.

Prevenção: Implementam medidas preventivas para evitar futuros eventos de segurança, fortalecendo a segurança da informação.

8. Exercícios e Testes

Serão testados regularmente por meio de exercícios simulados para assegurar sua eficácia e identificar áreas de melhoria. Os resultados dos testes serão documentados e revisados pelo Comitê.

8.1. Exercícios de Simulação

Discussões guiadas em grupo sobre um cenário de crise hipotético. Não há movimentação física de pessoas ou equipamentos.

Objetivo: Avaliar a compreensão dos planos, identificar lacunas, melhorar a comunicação e o processo de tomada de decisão.

Cenário 1: Falha tecnológica crítica (ex: servidor principal offline, ataque ransomware).

⇒ **Foco:** Tempo de recuperação, planos de backup, sistemas alternativos, comunicação com TI e usuários.

Cenário 2: Desastre natural (ex: enchente, incêndio no escritório principal).

⇒ **Foco:** Segurança da equipe, acesso a instalações alternativas, recuperação de dados, impacto na cadeia de suprimentos.

Cenário 3: Crise de imagem/reputação (ex: vazamento de dados de clientes, declaração polêmica de um executivo).

⇒ **Foco:** Plano de comunicação interna e externa, gestão de redes sociais, posicionamento da empresa.

Cenário 4: Pandemia/Crise de saúde pública (ex: alta taxa de absenteísmo, necessidade de trabalho remoto em massa).

⇒ **Foco:** Capacidade de trabalho remoto, comunicação com funcionários, políticas de saúde e segurança.

Periodicidade: Anual

9. Exercícios Funcionais

Tem como proposta testar componentes específicos do Plano de Continuidade de Negócios e Gestão de Crises em um ambiente mais próximo do real, mas sem afetar as operações diárias.

Objetivo: Validar procedimentos operacionais, testar sistemas e equipamentos específicos e treinar equipes em tarefas críticas, tais como:

Teste de Backup e Restauração de Dados: Restaurar dados de um backup para um ambiente de teste e verificar a integridade e completude.

Teste de Comunicação de Crise: Enviar mensagens de teste para a equipe de crise, clientes e parceiros para verificar a agilidade e a eficácia dos canais de comunicação.

Teste de Evacuação do Edifício: Realizar um simulado de incêndio para testar as rotas de fuga, pontos de encontro e o tempo de evacuação.

Periodicidade: Anual

10. Conformidade com a LGPD

O Santos Bevilaqua Advogados demonstra seu compromisso com a Lei Geral de Proteção de Dados (LGPD) ao implementar um conjunto robusto de medidas técnicas e administrativas para proteger os dados pessoais sob sua responsabilidade.

Essas medidas incluem:

Criptografia de dados sensíveis: Garante que informações cruciais sejam codificadas, dificultando o acesso não autorizado.

Controles de acesso: Restringe quem pode acessar determinados dados, assegurando que apenas pessoas autorizadas tenham permissão.

Monitoramento de sistemas: Permite a detecção e resposta rápida a atividades suspeitas ou tentativas de violação.

Treinamento contínuo de colaboradores: Capacita a equipe sobre as diretrizes da LGPD e as melhores práticas de segurança da informação, criando uma cultura de conscientização.

Políticas de uso de dispositivos pessoais e segurança da informação: Estabelece regras claras para o uso de equipamentos e a conduta em relação à segurança dos dados, mesmo fora do ambiente de trabalho direto.

Essas ações refletem um esforço para manter a confidencialidade, integridade e disponibilidade dos dados pessoais, alinhando-se com as exigências da LGPD.

11. Conformidade com as Normas da OAB

A aderência rigorosa às regras e diretrizes da Ordem dos Advogados do Brasil (OAB) é um pilar fundamental da atuação do escritório, especialmente em situações de crise.

Ética e Disciplina: Todas as ações e comunicações, internas e externas, serão pautadas pelos princípios éticos e disciplinares estabelecidos pela OAB, garantindo a conduta profissional e a integridade da advocacia.

Sigilo Profissional: Em qualquer cenário, a proteção do sigilo profissional e das informações confidenciais de clientes será mantida com a máxima prioridade, em estrita observância ao Código de Ética e Disciplina da OAB e legislação pertinente.

Transparência: A comunicação com clientes, colegas e autoridades será conduzida com total transparência e clareza, respeitando sempre as limitações impostas pelo sigilo e pelas determinações da OAB.

Regulamentação Específica: Quaisquer requisitos específicos da OAB relacionados a comunicações em momentos de instabilidade, notificação de incidentes ou manutenção da prestação de serviços jurídicos serão prontamente identificados e cumpridos.

Salvaguarda da Atividade Jurídica: Garantir que a continuidade dos serviços jurídicos oferecidos pelo escritório não seja comprometida de forma a violar os direitos dos clientes ou as prerrogativas da advocacia.

O Santos Bevilaqua Advogados prioriza a credibilidade e a confiança junto aos clientes e à comunidade jurídica. A atuação em conformidade assegura que o escritório manter sua licença para operar com ações responsáveis e éticas.

12. Referências

BRASIL. Departamento de Segurança da Informação e Comunicações / Gabinete de Segurança Institucional da Presidência da República. Norma Complementar Nº 06, de 11 de novembro de 2009. Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações. Brasília-DF, 2009. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf Acesso em: 09 de julho. 2025.

MANOEL, Sergio da Silva. Sistema de Gestão de Continuidade de Negócios: esteja preparado para salvar a sua vida e os seus negócios de um incidente ou desastre. Tenha um plano “B” profissional. Brasport, 2019.

Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados;

ISO/IEC 27035:2011- Tecnologias da Informação- Segurança- Gestão de Incidentes de Segurança da Informação;

Atuação do encarregado pelo tratamento de dados pessoais, Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/copy_of_guia_da_atuacao_do_encarregado_anpd.pdf acessado em 10 de julho. 2025.