



DIÁRIO OFICIAL DO ESTADO DE SÃO PAULO

Publicado na Edição de 28 de maio de 2026 | Caderno Executivo | Seção Atos Normativos

DELIBERAÇÃO DIRETORIA EXECUTIVA Nº 08, DE 8 DE MAIO DE 2026

Deliberação Diretoria Executiva nº 08, de 8 de Maio de 2026

Plano de Continuidade de Negócios

DELIBERAÇÃO DIREX Nº 08/2026

Assunto: Aprova o **Plano de Continuidade de Negócios** da Fundação de Previdência Complementar do Estado de São Paulo – SP-PREVCOM

A Diretoria Executiva da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM, em sua **697ª Reunião Ordinária**, realizada em **8 de maio de 2026**, resolve:

Artigo 1º. Fica aprovado o **Plano de Continuidade de Negócios** da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM, na forma do Anexo, que integra esta Deliberação para todos os fins.

Parágrafo único. Nos termos dos itens 2.2 e 2.3 da Política Interna de Elaboração e Gestão de Normativos da Prevcom este documento é classificado internamente como Regulamento.

Artigo 2º. Fica revogado o Plano de Continuidade de Negócios aprovado pela Diretoria Executiva em 29 de abril de 2021.

Artigo 3º. Esta Deliberação entra em vigor na data de sua publicação.

SUMÁRIO

1.Introdução

2.Objetivo

3.Escopo

4.Definições

5.Vigência

6.Responsabilidades

7.Monitoramento e Indicadores

8.Auditoria e Avaliação de Efetividade

9.Revisão e Atualização

10.Documentos Base e Diretrizes

11.Abrangência

12.Serviços Críticos

13.Classificação de Incidentes

14.Respostas aos Incidentes de Segurança da Informação por Serviço Crítico

14.2 Publicação e Centralização dos Planos de Continuidade

15.Vigência

16.Disposições Finais

1. Introdução

1.1. O planejamento da segurança da informação é essencial para a identificação, coleta e preservação adequada de evidências, bem como para a antecipação de potenciais incidentes e mitigação de riscos. Esse planejamento orienta o acionamento oportuno da equipe de Segurança da Informação, o direcionamento eficaz dos recursos e a execução dos procedimentos estabelecidos, assegurando uma resposta coordenada e eficiente.

1.2. O Plano de Continuidade de Negócios (PCN) da PREVCOM estabelece as diretrizes e os procedimentos necessários para assegurar a continuidade dos processos críticos da Entidade, a disponibilidade das informações e a mitigação de impactos operacionais, legais, regulatórios e reputacionais, integrando-se ao Sistema de Gestão da Segurança da Informação (SGSI).

1.3. O PCN contempla os seguintes planos complementares:

a. Plano de Resposta a Incidentes de Segurança da Informação: identifica ameaças relevantes, avalia impactos potenciais e define ações para a contenção, erradicação e recuperação, conforme requisitos do processo de gestão de incidentes.

b. Plano de Exercícios e Testes de Continuidade: especifica os recursos críticos, procedimentos e cronogramas necessários para validar a eficácia das estratégias de continuidade e assegurar o restabelecimento das funções essenciais dentro dos tempos de recuperação acordados (RTO/RPO).

c. Plano de Manutenção e Melhoria Contínua: estabelece critérios, periodicidade e gatilhos para a revisão e atualização do PCN, assegurando sua adequação contínua frente a mudanças organizacionais, tecnológicas e de contexto.

d. Plano de Comunicação em Situações de Disrupção: define as partes interessadas, fluxos de comunicação, canais, responsáveis e protocolos a serem seguidos durante a gestão de incidentes, em conformidade com o plano de comunicação de crise.

1.4. A alta direção demonstra seu compromisso com o PCN por meio da definição de políticas, da disponibilização de recursos necessários e da promoção da melhoria contínua do Sistema de Gestão da Segurança da Informação (SGSI) e do SGCN, assegurando sua eficácia e alinhamento com os objetivos estratégicos da organização.

1.5. A aplicação do PCN visa, ainda, assegurar o cumprimento das obrigações institucionais da PREVCOM perante participantes, patrocinadores, órgãos reguladores e demais partes interessadas.

2. Objetivo

2.1. Este documento tem como objetivo estabelecer diretrizes, responsabilidades e procedimentos para a gestão de situações de disrupção, assegurando a continuidade dos processos críticos, a disponibilidade das informações e a adequada resposta a incidentes relevantes da PREVCOM.

2.2. As respostas a incidentes têm por finalidade restabelecer a normalidade operacional dos ambientes críticos da PREVCOM, mediante o direcionamento coordenado das equipes responsáveis para a execução de procedimentos definidos, assegurando uma atuação eficaz, tempestiva e proporcional à severidade do evento, abrangendo os impactos operacionais, institucionais, jurídicos e regulatórios eventualmente decorrentes.

2.3. Os testes de continuidade validam a eficácia das estratégias implementadas, assegurando a capacidade de recuperação dos ambientes tecnológicos conforme os parâmetros estabelecidos.

2.4. O plano de comunicação especifica os responsáveis pelo acionamento em cada categoria de incidente, bem como os meios e protocolos de contato, com o objetivo de assegurar a celeridade no tratamento e na mitigação dos impactos decorrentes.

2.5. Adicionalmente, este documento reforça o compromisso da PREVCOM com a melhoria contínua do Sistema de Gestão da Segurança da Informação (SGSI) e do Sistema de Gestão de Continuidade de Negócios (SGCN), bem como com a conformidade às obrigações legais, regulamentares e contratuais aplicáveis, alinhando-se às melhores práticas internacionais em gestão de riscos e continuidade operacional.

3. Escopo

3.1. Este Plano de Continuidade de Negócios (PCN) aplica-se a todas as unidades organizacionais, processos críticos, sistemas de informação e ativos essenciais da PREVCOM que suportam a continuidade das operações e a entrega de produtos e serviços aos participantes, patrocinadores e demais partes interessadas, contemplando tanto os aspectos operacionais quanto os aspectos institucionais da Entidade, inclusive os impactos financeiros, reputacionais e de conformidade que possam decorrer de situações de disrupção.

3.2. O escopo inclui:

- a. Identificação dos processos críticos cujo comprometimento pode gerar impactos significativos na prestação de serviços ou no cumprimento de obrigações legais e contratuais.
- b. Eventual descumprimento de obrigações legais, regulatórias e contratuais, inclusive aquelas relacionadas ao regime de previdência complementar e à proteção de dados pessoais.
- c. Definição dos sistemas e ativos de informação que requerem estratégias específicas de continuidade e recuperação.
- d. Estabelecimento dos limites e interfaces com outros planos, como o Plano de Gestão de Incidentes de Segurança da Informação e o Plano de Recuperação de Desastres (PRD).

3.3. Este PCN não se aplica a processos, sistemas ou ativos cuja interrupção não cause impacto relevante à continuidade das operações da PREVCOM, conforme análise de impacto nos negócios (BIA — Business Impact Analysis) previamente realizada.

4. Definições

4.1. Para fins deste Regulamento de Continuidade de Negócios, aplicam-se as seguintes definições, siglas e expressões técnicas:

- a. Análise de Impacto nos Negócios (BIA – Business Impact Analysis): processo sistemático destinado a identificar e avaliar os impactos decorrentes da interrupção de processos, sistemas e serviços críticos, subsidiando a definição de prioridades, tempos de recuperação e estratégias de continuidade.
- b. Ativos Críticos: recursos tecnológicos, informacionais, humanos ou físicos considerados essenciais para a continuidade das operações da PREVCOM, cuja indisponibilidade compromete de forma significativa a execução dos processos críticos da entidade.
- c. Continuidade de Negócios: capacidade da PREVCOM de manter ou restabelecer suas operações essenciais em níveis aceitáveis após a ocorrência de incidentes ou eventos disruptivos.
- d. Incidente: evento ou conjunto de eventos que tenha potencial de causar impacto negativo à continuidade das operações, à segurança da informação ou ao cumprimento dos objetivos institucionais da PREVCOM.
- e. MTTR (Mean Time to Recovery – Tempo Médio de Recuperação): tempo médio necessário para restaurar um serviço, sistema ou ativo crítico após a ocorrência de um incidente.
- f. PCN (Plano de Continuidade de Negócios): conjunto de diretrizes, procedimentos, responsabilidades e estratégias documentadas destinadas a assegurar a continuidade ou o restabelecimento das operações críticas da PREVCOM em situações de interrupção.
- g. RTO (Recovery Time Objective – Objetivo de Tempo de Recuperação): tempo máximo aceitável para a recuperação de um serviço, processo ou sistema crítico após uma interrupção.

- h. RPO (Recovery Point Objective – Objetivo de Ponto de Recuperação): quantidade máxima tolerável de perda de dados, medida em tempo, antes da ocorrência de um incidente.
- i. Serviço Crítico: serviço ou processo cuja interrupção impacta diretamente a continuidade das operações, o cumprimento de obrigações legais, regulatórias ou contratuais, ou a prestação de serviços aos participantes, patrocinadores e demais partes interessadas.
- j. SGCN (Sistema de Gestão de Continuidade de Negócios): conjunto de políticas, processos, procedimentos e recursos que visam planejar, implementar, monitorar e melhorar continuamente a continuidade operacional da PREVCOM.
- k. SGSI (Sistema de Gestão da Segurança da Informação): sistema de gestão responsável por estabelecer, implementar, manter e melhorar a segurança da informação, assegurando a confidencialidade, integridade e disponibilidade das informações da PREVCOM.

5. Vigência

5.1. Este Regulamento entra em vigor na data de sua publicação, revogando integralmente a versão anterior do Plano de Continuidade de Negócios.

6. Responsabilidades

6.1. As responsabilidades relativas à implementação, manutenção, execução, monitoramento e aprimoramento do Regulamento de Continuidade de Negócios da PREVCOM são atribuídas da seguinte forma:

6.2. Diretoria Executiva

6.2.1. Compete à Diretoria Executiva:

- a. Aprovar o Regulamento de Continuidade de Negócios e suas revisões;
- b. Assegurar a disponibilização dos recursos humanos, tecnológicos e financeiros necessários à sua implementação e manutenção;
- c. Patrocinar e fomentar a cultura organizacional voltada à resiliência operacional, à gestão de riscos e à continuidade dos negócios;
- d. Deliberar sobre medidas estratégicas em situações de disrupção de alto impacto.

6.3. Equipe de Continuidade de Negócios

6.3.1. Compete à Equipe de Continuidade de Negócios:

- a. Supervisionar a implementação e a efetividade do Regulamento de Continuidade de Negócios;
- b. Acompanhar a execução de testes, simulações e exercícios de continuidade;
- c. Avaliar os resultados dos testes, incidentes ocorridos e indicadores de desempenho do PCN;

d. Propor melhorias, ajustes e revisões no Regulamento, com base em lições aprendidas e mudanças no contexto organizacional;

e. Atuar de forma integrada com as áreas de Gestão de Riscos, Segurança da Informação e Tecnologia da Informação.

6.3.2. A Equipe de Continuidade de Negócios será designada pela Diretoria competente, podendo ser composta por representantes das áreas de Tecnologia da Informação, Segurança da Informação e Gestão de Riscos, Controles Internos e Conformidade, bem como por representante(s) da(s) área(s) responsável(is) pelo(s) processo(s) crítico(s) envolvido(s), conforme a necessidade.

6.4. Diretoria de Tecnologia da Informação

6.4.1. Compete à Diretoria de Tecnologia da Informação:

- a. Elaborar, implementar e manter atualizado o Regulamento de Continuidade de Negócios;
- b. Assegurar a disponibilidade, integridade e recuperação dos sistemas e infraestruturas tecnológicas classificadas como críticas;
- c. Coordenar a execução dos procedimentos técnicos de resposta a incidentes e recuperação de serviços;
- d. Garantir a realização dos testes de continuidade e a documentação dos respectivos resultados;
- e. Manter registros atualizados de incidentes, ações corretivas e planos de melhoria.
- f. Apoiar a identificação, análise e tratamento de riscos relacionados à segurança da informação;
- g. Atuar de forma integrada nos processos de resposta a incidentes que afetem a confidencialidade, integridade ou disponibilidade das informações;
- h. Monitorar ameaças e vulnerabilidades que possam impactar a continuidade dos negócios;
- i. Contribuir para a definição e revisão dos controles de segurança associados aos ativos críticos.

6.6. Área de Gestão de Riscos, Controles Internos e Conformidade

6.6.1. Compete à Área de Gestão de Riscos, Controles Internos e Conformidade:

- a. Avaliar periodicamente a aderência do Regulamento de Continuidade de Negócios às normas internas, legislações aplicáveis e boas práticas de mercado;
- b. Apoiar a identificação e avaliação dos riscos operacionais, tecnológicos e reputacionais relacionados à continuidade dos negócios;
- c. Monitorar indicadores de efetividade do PCN e apoiar a definição de ações de melhoria;

d. Subsidiar processos de revisão e atualização do Regulamento.

6.7. Gestores de Processos e Serviços Críticos

6.7.1. Compete aos Gestores de Processos e Serviços Críticos:

- a. Identificar e manter atualizados os processos e serviços críticos sob sua responsabilidade;
- b. Assegurar a implementação das estratégias de continuidade e dos procedimentos operacionais definidos neste Regulamento;
- c. Participar dos testes, simulações e exercícios de continuidade;
- d. Comunicar tempestivamente incidentes ou situações que possam comprometer a continuidade das operações.

6.8. Empregados e Prestadores de Serviços

6.8.1. Compete aos Empregados e Prestadores de Serviços:

- a. Conhecer e cumprir as disposições deste Regulamento;
- b. Atuar de forma colaborativa na prevenção, comunicação e tratamento de incidentes;
- c. Participar de treinamentos, testes e exercícios de continuidade quando convocados;
- d. Comunicar imediatamente situações de risco ou incidentes que possam afetar a continuidade dos negócios.

7. Monitoramento e Indicadores

7.1. O Regulamento de Continuidade de Negócios será objeto de monitoramento contínuo, com o objetivo de avaliar sua efetividade, aderência aos objetivos institucionais e capacidade de resposta a incidentes que possam impactar a continuidade das operações da PREVCOM.

7.2. O monitoramento será realizado por meio de indicadores de desempenho e controles periódicos, contemplando, no mínimo:

- a. Tempo Médio de Recuperação (MTTR) dos serviços, sistemas e ativos classificados como críticos;
- b. Atendimento aos Objetivos de Tempo de Recuperação (RTO) definidos para cada serviço crítico;
- c. Resultados dos testes, simulações e exercícios de continuidade, incluindo taxa de sucesso e desvios identificados;
- d. Quantidade, natureza e recorrência de incidentes que afetem a continuidade dos negócios;
- e. Registro e acompanhamento das ações corretivas e preventivas decorrentes de incidentes, testes e auditorias;

f. Nível de aderência dos fornecedores críticos aos requisitos de continuidade estabelecidos pela PREVCOM.

7.3. Os indicadores deverão ser registrados, analisados e consolidados periodicamente, subsidiando a tomada de decisão pelas instâncias competentes, bem como a proposição de ações de melhoria contínua do Regulamento de Continuidade de Negócios.

7.4. A responsabilidade pelo monitoramento dos indicadores do PCN caberá às áreas designadas pela PREVCOM, observadas as atribuições previstas neste Plano.

7.5. Os resultados do monitoramento e da apuração dos indicadores servirão de base para a revisão periódica do Regulamento, para o aprimoramento das estratégias de continuidade e para o fortalecimento da governança, dos controles internos e da gestão de riscos da PREVCOM.

8. Auditoria e Avaliação de Efetividade

8.1. O Regulamento de Continuidade de Negócios poderá ser submetido a auditorias periódicas, internas ou independentes, com o objetivo de verificar sua conformidade com a legislação vigente, as normas internas da PREVCOM, os referenciais normativos aplicáveis e as boas práticas de governança.

8.2. A PREVCOM realizará auditorias internas relacionadas ao PCN para verificar a conformidade do Plano com os requisitos estabelecidos e sua efetiva aplicação.

8.3. A avaliação de efetividade deverá considerar, entre outros aspectos:

- a. O grau de atendimento aos objetivos de continuidade estabelecidos;
- b. A eficácia dos procedimentos de resposta a incidentes e recuperação de serviços;
- c. A consistência e atualidade das informações, registros e planos associados ao PCN;
- d. Os resultados dos testes, simulações e exercícios realizados;
- e. A implementação e a efetividade das ações corretivas e de melhoria contínua.

8.4. Os resultados das auditorias e das avaliações de efetividade do PCN deverão ser formalmente registrados e submetidos à análise crítica da Administração, para fins de deliberação e direcionamento estratégico, constituindo insumo para o aprimoramento contínuo do Regulamento, o fortalecimento dos controles internos e a mitigação de riscos operacionais e tecnológicos.

9. Revisão e Atualização

9.1. O Regulamento de Continuidade de Negócios deverá ser revisado, no mínimo, a cada dois anos, ou sempre que ocorrerem alterações relevantes no ambiente organizacional, tecnológico, regulatório ou de riscos da PREVCOM que possam impactar a continuidade das operações.

9.2. A revisão deverá considerar, entre outros fatores:

- a. Mudanças nos processos, serviços e ativos classificados como críticos;

- b. Resultados de testes, simulações, auditorias e avaliações de efetividade;
- c. Incidentes ocorridos e respectivas lições aprendidas;
- d. Alterações na legislação, normas internas e referenciais normativos aplicáveis;
- e. Recomendações das áreas de Tecnologia da Informação, Segurança da Informação, Gestão de Riscos, Controles Internos e Conformidade.

9.3. As atualizações do Regulamento deverão seguir o fluxo formal de elaboração, validação, aprovação e publicação previsto na Política Interna de Elaboração e Gestão de Normativos da PREVCOM.

10. Documentos Base e Diretrizes

10.1. Este Plano de Continuidade de Negócios (PCN) da PREVCOM baseia-se principalmente na ISO/IEC 22301:2019, que define requisitos para a gestão da continuidade operacional, bem como nas boas práticas da ISO/IEC 27001:2022 e ISO/IEC 27002:2022, que orientam a proteção de ativos de informação e o tratamento de incidentes.

10.2. A ISO/IEC 22301 estabelece um modelo sistemático para:

- a. Identificar, reportar e tratar incidentes e vulnerabilidades.
- b. Responder a eventos que comprometam a continuidade ou segurança da informação.
- c. Assegurar a melhoria contínua do Sistema de Gestão de Continuidade de Negócios (SGCN).

10.3. De acordo com a norma, define-se:

- a. Evento de segurança: ocorrência que pode indicar falha ou ameaça à segurança da informação.
- b. Incidente de segurança: evento ou combinação de eventos com potencial de causar impacto negativo nos negócios.

10.4. Nem todo evento caracteriza um incidente, mas ambos exigem tratamento estruturado.

10.5. A norma destaca que vulnerabilidades podem subsistir, mesmo com controles implementados, e recomenda processos robustos para garantir a resiliência organizacional.

10.6. O modelo da ISO/IEC 22301 é estruturado em cinco fases:

- a. Compreensão da organização — identificação de processos críticos e riscos.
- b. Estratégia de continuidade — definição de soluções para assegurar operações.
- c. Resposta a incidentes — procedimentos para mitigar impactos.
- d. Monitoramento e avaliação — acompanhamento da eficácia das ações.
- e. Melhoria contínua — ajustes com base em lições aprendidas.

10.7. Gestão de Fornecedores, Contratações e Continuidade de Serviços Essenciais

10.7.1. Para assegurar a efetividade do Plano de Continuidade de Negócios e a resiliência operacional da PREVCOM, aplicam-se as seguintes diretrizes relacionadas à gestão de fornecedores, contratações e serviços essenciais:

10.7.2. Contratações com requisitos de continuidade: os contratos administrativos que envolvam serviços ou ativos críticos deverão prever, obrigatoriamente, cláusulas específicas relacionadas à continuidade de negócios, incluindo, no mínimo: planos de contingência, níveis de serviço (SLA), objetivos de tempo de recuperação (RTO), responsabilidades das partes e medidas a serem adotadas em caso de interrupção ou degradação dos serviços.

10.7.3. Gestão de fornecedores críticos: os fornecedores que suportam processos ou serviços críticos deverão ser formalmente identificados e submetidos a critérios de avaliação periódica, contemplando aspectos de capacidade operacional, segurança da informação, resiliência, continuidade de negócios e aderência a requisitos contratuais.

10.7.4. Planos de contingência e substituição de fornecedores: deverão ser definidos, sempre que aplicável, planos de contingência que contemplem a substituição de fornecedores críticos, incluindo alternativas operacionais, mecanismos de transição e mitigação de riscos associados à descontinuidade de serviços.

10.7.5. Reequilíbrio econômico-financeiro: nos casos em que eventos de disrupção impactem contratos relacionados à continuidade dos negócios, poderá ser avaliada a necessidade de reequilíbrio econômico-financeiro, nos termos da legislação aplicável e das cláusulas contratuais estabelecidas.

10.7.6. Contratações emergenciais e prorrogações: em situações de disrupção que comprometam a continuidade das operações, poderão ser adotadas contratações emergenciais ou prorrogações contratuais, observadas as disposições legais vigentes e as diretrizes internas da PREVCOM, com o objetivo de assegurar a continuidade dos serviços essenciais.

10.7.7. Sistemas corporativos críticos e serviços de apoio: o Plano de Continuidade deverá contemplar, de forma explícita, estratégias de contingência para a indisponibilidade de sistemas corporativos utilizados pela PREVCOM, incluindo, mas não se limitando a sistemas de gestão documental, plataformas de armazenamento em nuvem e demais serviços essenciais ao funcionamento institucional.

10.7.8. Detalhamento operacional: os fluxos, procedimentos, responsáveis e instrumentos necessários à execução das ações de continuidade relacionadas a fornecedores e serviços críticos deverão ser detalhados em documentos complementares, assegurando sua aplicação prática, tempestiva e coordenada.

11. Abrangência

11.1. Este Regulamento de Continuidade de Negócios aplica-se aos ativos críticos da PREVCOM, compreendidos como aqueles indispensáveis à manutenção da continuidade das operações e ao cumprimento de suas obrigações institucionais.

11.2. A identificação dos ativos críticos decorreu da Análise de Impacto nos Negócios (BIA), considerando os processos essenciais da entidade, bem como suas dependências técnicas, físicas, humanas e lógicas, de modo a assegurar uma abordagem integrada e consistente da continuidade operacional.

11.3. O disposto neste Regulamento abrange, ainda, os serviços, sistemas de informação, infraestruturas tecnológicas e recursos de apoio que sustentam os processos críticos, bem como as interações com fornecedores e prestadores de serviços essenciais, na medida em que impactem a resiliência organizacional da PREVCOM.

12. Serviços Críticos

12.1. A classificação de criticidade dos serviços considera critérios de impacto operacional, institucional, legal e de segurança da informação, conforme análise de impacto no negócio.

12.2. A partir da delimitação do núcleo de funcionamento, foram definidos os serviços/processos abaixo como críticos, ou seja, que se tiverem sua funcionalidade interrompida comprometem inteiramente a operação. Com base na funcionalidade dos serviços de tecnologia, foram determinados os ativos críticos:

- a. SC 01 – MJ PREV – Criticidade: Muito Alto. Serviços de gestão dos planos dos participantes, comunicação e cadastro. Sites públicos, área restrita, ambiente corporativo.
- b. SC02 – GED - Criticidade: Muito Alto. Serviço de Gerenciamento Eletrônico de Documentos.
- c. SC03 – Link de Internet - Criticidade: Muito Alto. Serviço de link de Internet dedicada.
- d. SC04 – AWS - Criticidade: Alto. Provedor de serviços e servidores Cloud.
- e. SC05 – Operação da Sede Física – Criticidade: Muito Alto. Serviço relacionado à disponibilidade das instalações físicas da PREVCOM.
- f. SC06 – Condições de Trabalho Alternativas – Criticidade: Alto. Serviço relacionado à capacidade de operação da PREVCOM em regime alternativo, incluindo trabalho remoto, uso de instalações contingenciais ou realocação temporária de atividades.

13. Classificação de Incidentes

13.1. Análise de Impacto do Negócio é um componente essencial de um PCN. A análise tem por objetivo revelar vulnerabilidade e subsidiar o desenvolvimento de estratégias para minimizar os riscos.



Tabela 1 - Definição de métricas

NÍVEL DE IMPACTO	DESCRIÇÃO
Muito Baixo	Impacto insignificante nos objetivos, com dispensa de medida de reparação ou recuperação
Baixo	Impacto mínimo nos objetivos, com possibilidade de fácil reparação ou recuperação
Médio	Impacto mediano nos objetivos, com possibilidade de reparação ou recuperação
Alto	Impacto significativo nos objetivos, com possibilidade remota de reparação ou recuperação
Muito Alto	Impacto máximo nos objetivos, sem possibilidade de reparação ou recuperação
NÍVEL DE PROBABILIDADE	DESCRIÇÃO
Muito Baixo	Evento extraordinário, sem histórico disponível de ocorrência
Baixo	Evento casual, com histórico conhecido de ocorrência
Médio	Evento esperado, de frequência reduzida, com histórico conhecido pela maioria dos gestores e operadores do processo
Alto	Evento usual, de ocorrência habitual, com histórico conhecido amplamente por parte dos gestores e operadores do processo
Muito Alto	Evento repetitivo e constante, de ocorrência numerosa, com histórico disponível ou não, mas evidente para os que conhecem o processo

13.2. A matriz abaixo representa os possíveis resultados da combinação das escalas de Probabilidade X Impacto:

Impacto	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
	Probabilidade					
Muito Baixo	1	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).				
Baixo	2	Pequeno impacto nos objetivos.				
Médio	3	Moderado impacto nos objetivos, porém recuperável.				
Alto	4	Significativo impacto nos objetivos, de difícil reversão.				
Muito Alto	5	Alto Catastrófico impacto nos objetivos, de forma irreversível.				
Risco/Descrição		Probabilidade	Impacto	Criticidade		

Problema na Infraestrutura Tecnológica	4	4	16
Falta de Energia	2	3	6
Inacessibilidade à Sede da Organização	4	3	12

14. Respostas aos Incidentes de Segurança de Informação por Serviço Crítico

14.1. Na busca incessante pela resiliência organizacional, é imperativo estabelecer um sólido Plano de Continuidade de Negócios (PCN) que compreenda detalhadamente os ativos críticos da Prevcom. Neste contexto, apresentamos a seguir as tabelas que delineiam os planos de resposta a incidentes desses ativos, fornecendo uma visão abrangente das estratégias de mitigação de riscos, ações planejadas e os protocolos de comunicação associados.

14.2. O reconhecimento da natureza dinâmica do ambiente empresarial atual demanda uma abordagem proativa na identificação, análise e resposta aos riscos que possam ameaçar a continuidade operacional. Por meio da categorização criteriosa dos ativos críticos, este plano visa não apenas antecipar potenciais interrupções, mas também oferecer soluções robustas e eficazes para preservar a estabilidade do negócio.

14.3. Cada tabela apresentada é um guia detalhado que oferece insights sobre os riscos específicos associados a cada ativo crítico, acompanhados de estratégias concretas de mitigação. Além disso, os planos de ação delineados são complementados por protocolos claros de comunicação, essenciais para a coordenação eficiente durante incidentes inesperados.

14.4. Destacamos, ainda, a importância dos contatos de terceiros listados, que desempenham um papel fundamental na resposta rápida e eficaz a incidentes. A colaboração estreita com esses parceiros estratégicos fortalece a capacidade de recuperação da organização, proporcionando uma rede de apoio crucial em momentos críticos.

14.5. Ao abordar esses aspectos fundamentais, este documento visa capacitar a equipe responsável pela continuidade de negócios a tomar decisões informadas, agir com agilidade diante de adversidades e manter a integridade operacional mesmo em face de desafios imprevistos. Através da implementação rigorosa desses planos, a Prevcom reforça o compromisso com a resiliência e a sustentabilidade, consolidando a postura proativa da fundação diante do cenário dinâmico e complexo em que atuam.

14.1. Fases do Plano de Continuidade de Negócios

14.1.1. Fase de Contingência

14.1.1.1. A Fase de Contingência inicia-se com a instauração formal do PCN pela Diretoria Executiva e tem por finalidade estabelecer o comando estratégico, a coordenação inicial das ações e o enquadramento do nível de severidade do evento.

14.1.1.2. Nesta fase, caberá:

- a. Diretoria Executiva: instaurar formalmente o PCN, definir o nível de contingência aplicável, autorizar o acionamento das estruturas de apoio, priorizar processos críticos e deliberar sobre medidas e despesas excepcionais iniciais.

- b. Time de Resposta: promover o acionamento operacional inicial, mobilizar os responsáveis técnicos, levantar informações preliminares sobre o evento e preparar as condições para a atuação imediata nas fases subsequentes.
- c. Time de Comunicação: estruturar a comunicação institucional inicial, interna e externa, conforme diretrizes da Diretoria Executiva, controlando o fluxo, o conteúdo e a atualização das informações.
- d. Time de Segurança: apoiar tecnicamente a qualificação do evento e a avaliação preliminar de riscos, especialmente relacionados à segurança da informação e à proteção de dados, recomendando salvaguardas iniciais.

14.1.2. Fase de Resposta

14.1.2.1. A Fase de Resposta ocorre após a instauração do PCN e consiste na atuação imediata para contenção do incidente, proteção de pessoas, preservação de ativos essenciais e limitação de danos operacionais, institucionais e tecnológicos.

14.1.2.2. Nesta fase, caberá:

- a. Diretoria Executiva: deliberar sobre medidas emergenciais, validar ações de contenção, autorizar providências excepcionais e acompanhar a evolução do evento.
- b. Time de Resposta: atuar diretamente no evento, realizar o levantamento detalhado dos impactos, conter a propagação do incidente e executar as ações técnicas imediatas necessárias à estabilização da situação.
- c. Time de Comunicação: divulgar informações institucionais tempestivas e alinhadas às deliberações da Diretoria Executiva, mantendo os públicos estratégicos informados.
- d. Time de Segurança: assessorar tecnicamente a resposta, avaliando riscos emergentes e orientando quanto a medidas de contenção, segurança da informação e proteção de dados.

14.1.3. Fase de Recuperação

14.1.3.1. A Fase de Recuperação tem por objetivo retomar os processos considerados essenciais, restabelecendo gradualmente as funções críticas de negócio e assegurando a estabilidade operacional sob a vigência do PCN.

14.1.3.2. Nesta fase, caberá:

- a. Diretoria Executiva: priorizar recursos, autorizar despesas e validar medidas necessárias à recuperação dos processos essenciais.
- b. Time de Resposta: preparar e implementar os procedimentos de recuperação, com apoio de empregados e terceiros, assegurando a continuidade dos processos críticos, inclusive mediante adoção de teletrabalho seguro, quando aplicável.
- c. Time de Comunicação: manter os públicos internos e externos informados sobre a evolução da recuperação e as expectativas de normalização.

- d. Time de Segurança: avaliar riscos residuais, apoiar tecnicamente o reforço dos controles e monitorar a integridade das informações e dos dados.

14.1.4. Fase de Restauração

14.1.4.1. A Fase de Restauração consiste no retorno gradual e seguro à normalidade operacional, incluindo a recomposição da infraestrutura, dos sistemas e dos ambientes permanentes de trabalho, culminando no encerramento do PCN.

14.1.4.2. Nesta fase, caberá:

- a. Diretoria Executiva: coordenar e deliberar sobre o encerramento do PCN, autorizar despesas finais e validar o retorno à normalidade operacional.
- b. Time de Resposta: executar os procedimentos necessários à restauração plena das operações, incluindo migração ou retorno aos ambientes definitivos.
- c. Time de Comunicação: comunicar formalmente aos públicos internos e externos o retorno à normalidade operacional.

14.2. Publicação e Centralização dos Planos de Continuidade

14.2.1. Todos os Planos de Continuidade de Negócios deverão ser formalmente registrados e disponibilizados em repositório institucional indicado pela área de Tecnologia da Informação, destinado ao armazenamento, controle e gestão dos documentos relacionados à continuidade dos negócios da PREVCOM.

14.2.2. Os planos já elaborados na data de publicação deste Regulamento deverão ser devidamente revisados, quando aplicável, e inseridos no repositório no prazo máximo de 30 (trinta) dias corridos, contados a partir da sua entrada em vigor.

14.2.3. A manutenção, atualização e controle de versões dos planos serão de responsabilidade das áreas gestoras dos respectivos processos críticos, observadas as diretrizes estabelecidas neste Regulamento e nos instrumentos complementares aplicáveis.

15. Vigência

15.1. Este Regulamento de Continuidade de Negócios entra em vigor após o prazo de 120 (cento e vinte) dias corridos, contados a partir da data de sua publicação, período destinado à adaptação dos processos, à divulgação interna e à capacitação das áreas envolvidas, revogando, ao final desse prazo, as disposições em contrário, em especial a versão anterior do Plano de Continuidade de Negócios da PREVCOM.

16. Disposições Finais

16.1. O cumprimento deste Regulamento é obrigatório para todas as áreas, empregados e prestadores de serviços que, direta ou indiretamente, participem de processos, serviços ou atividades classificados como críticos para a continuidade dos negócios da PREVCOM.

16.2. Os procedimentos operacionais, fluxos, formulários e demais instrumentos complementares necessários à execução deste Regulamento poderão ser detalhados em documentos específicos, aprovados conforme o fluxo interno aplicável, sem prejuízo da observância das disposições aqui estabelecidas.

16.3. A indicação dos responsáveis operacionais, bem como a designação de equipes e pontos focais relacionados à execução do Regulamento, será formalizada por meio de atos administrativos ou processos próprios no SEI, vedada a indicação nominal neste instrumento normativo.

16.4. Este Regulamento integra o Sistema de Gestão de Continuidade de Negócios (SGCN) e o Sistema de Gestão da Segurança da Informação (SGSI) da PREVCOM, devendo ser aplicado de forma integrada às demais políticas, normas e regulamentos institucionais.