



Plano de Continuidade de Negócio

Versão 1.0

Novembro de 2024

COLABORAGOV

MINISTÉRIO DA
GESTÃO E DA INovaÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Sumário

Mensagem da alta gestão.....	4
Histórico de revisões	5
Conceitos.....	6
Siglas	9
Objetivos de um Plano de Continuidade de Negócio.....	10
Escopo deste Plano de Continuidade de Negócio.....	11
Alinhamento com a Estratégia.....	12
Processo de construção do Plano de Continuidade de Negócio	13
Equipe de Resposta a Incidentes	14
Implementação do Plano de Continuidade de Negócio.....	15
Protocolo de Comunicação em Situações de Crise	16
Protocolos de incidentes críticos.....	17
Revisão do Plano de Continuidade de Negócio.....	18
Anexo 01 - Protocolo de Comunicação em Situações de Crise	20
Anexo 02 - Pagamento de Folha.....	26
Mitigação	26
Resposta	28
Avaliação do Incidente.....	33
Classificação da Crise para efeito de Comunicação.....	34
Pós-Incidente	34
Anexo 03 - Incidentes Contratuais	36
Mitigação	36
Resposta	39
Avaliação do Incidente.....	42
Pós-Incidente	43
Anexo 04 - Indisponibilidade de recursos tecnológicos críticos - CompartilhaServiços	44
Mitigação	44
Resposta	46
Avaliação do Incidente.....	47
Pós-Incidente	48
Anexo 05 - Indisponibilidade de recursos tecnológicos críticos - Sistema SEI	49
Mitigação	49
Resposta	51

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Avaliação do Incidente	54
Pós-Incidente	55
Anexo 06 - Infraestrutura – Alagamento	56
Mitigação	56
Resposta	59
Avaliação do Incidente	63
Pós-Incidente	64
Anexo 07 – Infraestrutura - Incêndio	65
Mitigação	65
Resposta	70
Avaliação do Incidente	74
Pós-Incidente	75
Anexo 08 – Queda de energia	77
Mitigação	77
Resposta	82
Avaliação do Incidente	86
Pós-Incidente	88
Anexo 09 – Ocupação de prédio público	90

Mensagem da alta gestão

Prezados Colaboradores,

É com grande responsabilidade que nos dirigimos a todos vocês para destacar a importância fundamental do Plano de Continuidade de Negócio – PCN da Secretaria de Serviços Compartilhados – SSC. O PCN é uma ferramenta estratégica indispensável para garantir que as atividades essenciais à prestação dos serviços no âmbito do [ColaboraGov](#) permaneçam operacionais em momentos de crise ou interrupções inesperadas. Ele assegura a capacidade de responder de forma eficaz a incidentes que possam comprometer a continuidade de nossos serviços, preservando a nossa missão de atender à sociedade com eficiência, mesmo diante de adversidades.

A criação e implementação do PCN não podem ser encaradas como uma tarefa isolada ou apenas de um grupo específico. Pelo contrário, sua eficácia depende do comprometimento de todos e de cada um. Para que este plano seja verdadeiramente eficaz, é essencial que ele seja amplamente divulgado em todas as áreas do ColaboraGov. Todos devem conhecer seus papéis e responsabilidades, compreendendo como suas ações individuais e coletivas contribuem para a prevenção de incidentes e para o sucesso do PCN em momentos críticos.

A aplicação prática e constante do PCN também é indispensável. O plano precisa ser incorporado ao nosso dia a dia, sendo exercitado e testado por meio de simulações e treinamentos regulares, para que todos estejamos preparados para agir com prontidão e segurança.

Reafirmamos ainda a necessidade de manter o PCN atualizado. Sabemos que a realidade de nossas operações é dinâmica, com novos desafios surgindo constantemente. Por isso, o nosso compromisso é garantir que o PCN seja revisado periodicamente, ajustado conforme necessário, para que esteja sempre adequado às mudanças no ambiente interno e externo. Esta atualização contínua é essencial para garantir que estamos sempre à frente dos riscos e preparados para enfrentá-los.

A alta gestão do Ministério da Gestão e da Inovação em Serviços Públicos – MGI reafirma seu compromisso com todas as etapas do desenvolvimento, implementação, manutenção e aplicação do Plano de Continuidade de Negócios. Enxergamos o PCN como uma prioridade estratégica, e nosso envolvimento será constante para garantir que este plano seja eficaz e alcance seus objetivos.

Neste momento, o documento que apresentamos representa apenas o início de um projeto maior. É o ponto de partida de uma jornada contínua, que evoluirá gradualmente abrangendo mais disciplinas e adaptando-se às novas demandas e outras necessidades emergentes. O PCN, à medida em que evolui, vai se tornando cada vez mais robusto e completo, garantindo a resiliência do ColaboraGov em tempos de incerteza.

Agradecemos a todos pela dedicação e compromisso. Contamos com o empenho de cada um de vocês para o sucesso desta iniciativa, que não só protege a SSC, mas também garante a qualidade e continuidade dos serviços que prestamos à população.

Histórico de revisões

Data	Versão	Descrição	Unidade
05/08/2024	0.0	Versão inicial do documento	CGPRO/DGE/SSC
30/11/2024	1.0	Versão aprovada pela SSC/MGI na reunião 5ª reunião ordinária do Comitê de Governança e Estratégia da SSC/MGI (SEI nº 47238242)	CGPRO/DGE/SSC

Conceitos

Com a finalidade de padronizar o entendimento dos principais conceitos adotados em um PCN, apresentamos, a seguir, uma relação com a definição dos principais termos utilizados em um plano como este:

Ações de correção e prevenção de falhas: medidas técnicas ou operacionais adotadas a curto prazo, logo após o incidente, que tenham o objetivo de corrigir a falha e prevenir que incidentes da mesma natureza ocorram.

Ameaça: refere-se a eventos, circunstâncias ou condições que podem causar interrupções significativas nas operações críticas de uma organização.

Análise de Impacto nos Negócios – BIA: Processo utilizado para identificar e avaliar o impacto de uma possível interrupção nas operações críticas da organização, estabelecendo as prioridades de recuperação.

Atividades Críticas: São as operações ou funções que devem ser priorizadas para garantir a continuidade mínima dos negócios, cuja paralisação causaria impactos graves ao funcionamento da organização.

Continuidade de Negócio: Refere-se à capacidade da organização de manter suas funções críticas operacionais e entrega de produtos e serviços em um nível aceitável, com capacidade predefinida, durante e após uma interrupção ou crise.

Encarregado pelo tratamento de dados pessoais: servidor indicado pelo Ministério da Economia para atuar como canal de comunicação entre o Órgão, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados.

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e às atividades relacionadas a incidentes de segurança em redes de computadores (NC nº 05/IN01/DSIC/GSIPR).

Estratégia de mitigação: Conjunto de ações e medidas desenvolvidas para reduzir ou eliminar o impacto potencial de uma ameaça identificada à continuidade das operações da organização. As estratégias buscam minimizar os riscos, seja prevenindo que a ameaça ocorra, seja atenuando seus efeitos caso ela se concretize.

Gestão da Continuidade de Negócios: conjunto de elementos de gestão que estabelece, implementa, opera, monitora, analisa criticamente, mantém e aprimora a continuidade de negócios.

Gestor de Continuidade: Pessoa ou equipe responsável por coordenar a execução do PCN, garantir sua atualização e responder a incidentes que necessitem ativação do plano.

Incidente: Qualquer evento ou situação inesperada que pode causar uma interrupção nas operações normais, perda, emergência ou crise.

Incidente crítico: evento que pode causar a interrupção na provisão dos serviços ou que resulte na necessidade de ações emergenciais para o restabelecimento da normalidade da provisão dos serviços.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais (Autoridade Nacional de Proteção de Dados – ANPD).

Informações de Incidente com Dados Pessoais: documento registrado pela ETIR em processo SEI sigiloso, utilizando o tipo de documento de mesmo nome, contendo informações sobre o incidente com dados pessoais.

Infraestrutura: sistema de instalações, equipamentos e serviços necessários para a operação de uma organização.

Interrupção: evento, previsível ou imprevisível, que cause um desvio negativo, não planejado, das expectativas de entrega de produtos ou execução de serviços em relação aos objetivos do ColaboraGov.

Interrupção máxima aceitável: tempo para que os impactos adversos que possam surgir como resultado do não fornecimento de um produto ou serviço ou realização de uma atividade se tornem inaceitáveis.

Notificador: qualquer pessoa física ou jurídica que comunique, mesmo que anonimamente, um evento adverso incidente de segurança com dados pessoais. Também pode ser representado por tecnologias de detecção de incidentes, como sistema de detecção de intrusão, soluções de *Security Information and Event Management* (SIEM), *Data Loss Prevention* (DLP), entre outras.

Período máximo de interrupção: tempo necessário para que os impactos adversos se tornem inaceitáveis, que pode surgir como resultado de não fornecer um produto/serviço ou realizar uma atividade;

Plano de Ação de Emergência: Conjunto de procedimentos imediatos para proteger vidas e minimizar danos à infraestrutura da organização antes de uma eventual ativação completa do PCN.

Plano de Comunicação de Crise: Estratégias de comunicação interna e externa para garantir que todas as partes interessadas sejam informadas de maneira oportuna e precisa durante um incidente.

Ponto de Recuperação de Dados (POR): Refere-se à quantidade máxima de dados que pode ser perdida em caso de falha, com base no último backup realizado, e o impacto que isso terá na organização.

Processo: agregação de atividades e comportamentos executados por seres humanos ou máquinas para alcançar um ou mais resultados organizacionais;

Recuperação de Desastres: Conjunto de estratégias e ações focadas na recuperação da infraestrutura física, segurança e bem-estar dos colaboradores, documentos físicos, equipamentos, de sistemas de TI e dados críticos, após uma interrupção, para restaurar a operação normal no menor tempo possível.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Registro Geral de Incidentes com Dados Pessoais – RGI-DP: base de dados contendo informações de todos os incidentes de segurança com dados pessoais, ocorridos no âmbito do Ministério da Economia e comunicados ao encarregado.

Relatório Final de Tratamento de Incidente com Dados Pessoais: documento elaborado pelas ETIRs após o término do tratamento do incidente com dados pessoais, contendo todas as informações relativas ao incidente.

Sala de Crise é um ambiente físico ou virtual utilizada para gerenciar e coordenar a resposta a uma situação crítica que possa impactar as operações, a reputação ou a segurança de uma organização. A sala deve ser equipada com os recursos e tecnologias necessários à facilitação da comunicação e do tratamento de crises.

Tempo Objetivo de Recuperação – RTO: O período máximo aceitável de inatividade após uma interrupção, antes que as operações críticas precisem ser retomadas.

Testes e Exercícios: Definição dos diferentes tipos de atividades usadas para verificar a eficácia do PCN, como simulações, testes práticos e auditorias.

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Siglas

Sigla	Definição
ABIN	Agência Brasileira de Inteligência
ANPD	Autoridade Nacional de Proteção de Dados
BIA	<i>Business Impact Analysis</i>
BPM	<i>Business Process Management</i>
CGC	Comitê de Gerenciamento de Crise
Dataprev	Empresa de Tecnologia e Informações da Previdência Social
DLP	<i>Data Loss Prevention</i>
EAP	Estrutura Analítica do Projeto
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
ERI	Equipe de Resposta a Incidentes
GSI	Gabinete de Segurança Institucional
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
PCN	Plano de Continuidade de Negócio
PF	Polícia Federal
PGCN	Política de Gestão de Continuidade de Negócio
PGCN	Política de Gestão de Continuidade de Negócio
PM	Polícia Militar
POSIC	Política de Segurança da Informação e Comunicações
SEI	Sistema Eletrônico de Informações
RGI-DP	Registro Geral de Incidentes com Dados Pessoais
RTO	Tempo Objetivo de Recuperação
SGD	Secretaria de Governo Digital
SRA	Superintendência Regional de Administração
Serpro	Serviço Federal de Processamento de Dados
SIEM	<i>Security Information and Event Management</i>
SSC	Secretaria de Serviços Compartilhados
TI	Tecnologia da Informação

Objetivos de um Plano de Continuidade de Negócio

Um PCN emerge como uma ferramenta estratégica essencial para fortalecer a resiliência institucional e a capacidade de resposta da instituição em momentos de crise.

Com ambientes cada vez mais complexo e sujeito a riscos diversos, tais como desastres naturais, falhas tecnológicas, ameaças cibernéticas, falhas de infraestrutura as organizações enfrentam a necessidade de adotar práticas que garantam a continuidade de suas operações em situações adversas.

Nessa linha, a SSC decide lançar o seu PCN visando não apenas preservar as atividades essenciais à prestação dos serviços de suporte administrativo no âmbito do ColaboraGov, mas, também, minimizar os impactos de um incidente, proteger ativos, garantir a segurança de colaboradores e os interesses de todos que utilizam esses serviços.

O conjunto de ações previstas no PCN permitem que a SSC responda rapidamente a incidentes e restabeleça seus processos críticos com eficiência, para que se mantenha a confiança nos seus serviços e para que seja assegurada a conformidade com normas regulatórias.

A seguir, detalharemos alguns dos principais objetivos que orientam a estrutura e a implementação de um Plano de Continuidade de Negócios.

- 1 Minimizar os impactos de interrupções:** Reduzir o impacto operacional e reputacional causado por eventos inesperados, como desastres naturais, falhas tecnológicas, ameaças cibernéticas, falhas de infraestrutura, ataques ou intrusões nas instalações do Ministério, dentre outras.
- 2 Assegurar a continuidade das operações críticas:** Identificar processos críticos e garantir que eles permaneçam funcionais ou sejam rapidamente restaurados após uma interrupção.
- 3 Preservar a segurança de colaboradores e visitantes:** Proteger a integridade física e a saúde das pessoas envolvidas, criando estratégias claras de evacuação, comunicação e suporte.
- 4 Reduzir o tempo de recuperação:** Estabelecer procedimentos claros e colaborativos para restaurar as operações o mais rápido possível, reduzindo o tempo de inatividade e, consequentemente, o impacto para aqueles que utilizam os serviços prestados pelas unidades do Ministério para o público interno e externo.
- 5 Manter a conformidade legal, com normas e regulamentos:** Garantir que o Ministério atenda a requisitos legais, regulamentares e contratuais relacionados à gestão de riscos e continuidade do negócio.
- 6 Proteger ativos e informações:** Garantir a segurança de ativos físicos, dados pessoais, confidenciais e de sistemas de TI, protegendo-os contra perda, roubo ou danos.
- 7 Mitigar riscos e promover resiliência organizacional:** Identificar e abordar vulnerabilidades para fortalecer a capacidade do Ministério de resistir a interrupções.
- 8 Assegurar a comunicação eficaz:** Definir estratégias de comunicação internas e externas para manter interessados em serviços prestados pelo Ministério, suas unidades internas, e colaboradores informados durante uma crise.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

- 9 **Divulgar, disseminar, testar e treinar continuamente:** Divulgar o Plano, disseminar sua importância, realizar simulações e treinamentos, garantindo que todos saibam como agir em emergências.
- 10 **Proteger a imagem e a reputação do Ministério:** Demonstrar aos interessados e à sociedade que o MGI está preparado para lidar com crises de maneira eficiente, evitando prejuízos à sua credibilidade e às demais instituições que formam o Governo.

Escopo deste Plano de Continuidade de Negócio

Ao estruturar e implementar um PCN, a SSC busca proteger a sua capacidade em cumprir sua missão institucional, preservando seus processos de entrega de serviços e resultados, a confiança pública e a eficiência operacional, em prol do serviço público e da sociedade.

O PCN da SSC, ora apresentado, chega como o primeiro passo rumo a documento mais completo que será continuamente aprimorado de forma colaborativa. Chega, também, como uma proposta de estruturação que poderá ser adotada por outros órgãos de governo.

Optamos por uma estratégia de desenvolvimento por ondas evolutivas em lugar de estender o tempo de construção para uma entrega mais completa. Entendemos que é possível cobrir os riscos de indisponibilidade de serviços de forma paulatina.

Assim sendo, nesta primeira onda do PCN foram mapeados e elaboradas ações de prevenção e tratamento para oito incidentes:

1. Pagamento de Folha
2. Incidentes Contratuais
3. Indisponibilidade de recursos tecnológicos críticos
 - a. Sistema CompartilhaServiços
 - b. Sistema SEI
4. Infraestrutura
 - a. Alagamento
 - b. Incêndio
 - c. Queda de Energia
5. Ocupação de Prédio Público

Em ondas posteriores será possível acrescentar tratamento para outros incidentes não cobertos no momento da construção desta versão do PCN. Também é possível aprimorar o plano atual, construir planos complementares, com destaque para os planos que garantam o pleno funcionamento dos sistemas e serviços essenciais de TI em momentos de crise.

Neste contexto, **planos complementares** são documentos ou estratégias que apoiam e detalham aspectos específicos do PCN, de forma a garantir que a SSC consiga gerenciar e responder adequadamente a interrupções. Esses planos são projetados para abordar áreas críticas específicas e se integram a este PCN principal.

Alinhamento com a Estratégia

O alinhamento com a estratégia busca para garantir que o PCN não apenas responda a incidentes e crises, mas também dê o suporte necessário aos objetivos estratégicos da organização. Ao assegurar que os recursos e esforços dedicados à continuidade do negócio estejam direcionados para a proteção dos ativos mais críticos e para a garantia das operações essenciais para a concretização da estratégia, busca-se fortalecer a resiliência organizacional, permitindo uma recuperação mais rápida e eficiente e sem comprometer seus objetivos de médio e de longo prazo.

A oferta de serviços de suporte administrativo consta do Planejamento Estratégico do MGI 2023-2027, especialmente no “Objetivo Estratégico 13 - Prover serviços de suporte compartilhados e difundir soluções de alta qualidade para toda administração pública federal”.



Figura 1 – Mapa estratégico MGI 2023-2027

A importância de um PCN já havia sido identificada na Estrutura Analítica do Projeto – EAP de 2023 do Projeto ColaboraGov, na qual previu ações a serem realizadas em 2024 para a criação de uma Política de Gestão de Continuidade de Negócio – PGCN e de um PCN.

Também cabe destacar que a falha na confecção de um Plano de Continuidade de Negócios foi um dos riscos levantados do Projeto ColaboraGov, tendo como consequências a interrupção de atividades relevantes e impacto negativo na imagem ou reputação da SSC, enquanto prestadora de serviço. Para fazer frente a esse risco, foi incluída a EAP do Projeto ColaboraGov 2024 a entrega “Elaboração do Plano de Continuidade de Negócio”, prevista para junho a dezembro de 2024.

Na perspectiva das operações do ColaboraGov, em 2023, foram considerados como processos de negócio priorizados àqueles relacionados a Compras e Contratações, Execução Orçamentária e Financeira, Logística (Gestão de Espaços Físicos Inteligentes e Patrimônio),

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Pessoas (Gerir pagamento da folha). Esses processos de negócio passaram por ciclos de análise e de transformação de processos, conforme a disciplina *Business Process Management* (BPM).

Os incidentes críticos priorizados neste PCN relacionam-se a esses processos de negócio priorizados.

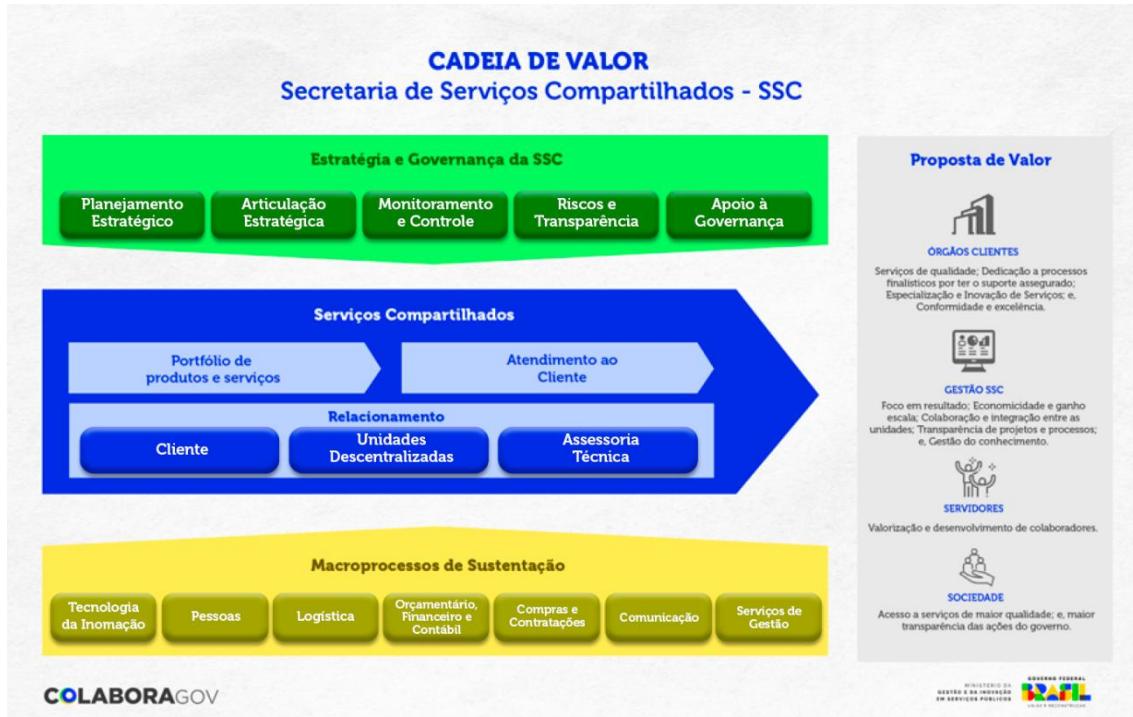


Figura 2 – Cadeia de valor da Secretaria de Serviços Compartilhados (SSC)

Também cabe destacar que as medidas para garantir a continuidade de negócio do MGI, especialmente a ausência de PCN instituído, fizeram com que o desempenho desse quesito tenha sido considerado inicial ou inexpressivo (0% a 39,99%) no [Levantamento iESGo 2024](#), promovido pelo TCU. Essa avaliação reforçou a necessidade de se priorizar a elaboração do PCN no âmbito do MGI para o fortalecimento da governança ministerial.

Processo de construção do Plano de Continuidade de Negócio

A elaboração do PCN foi possível, em primeiro lugar, pelo patrocínio da alta gestão, que indicou o conjunto de incidentes que deveriam compor esta primeira onda do Plano e disponibilizou equipe especialista nos temas para fornecer informações necessárias e construir este PCN.

A partir da definição do conjunto de incidentes a serem tratados, a equipe do projeto solicitou às áreas, por meio de processo no Sistema Eletrônico de Informações - SEI, a indicação de pontos focais para atuar fornecendo as informações essenciais para a construção do Plano.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Em seguida, para alinhamento dos diversos atores, foi realizado o *Kick-off* do projeto em 1º de agosto de 2024.

Na sequência, foi elaborada metodologia, em ferramenta CANVAS, que propiciou interação mais dinâmica em cada uma das oficinas realizadas para a coleta de informações sobre os incidentes.

Concluída a fase de levantamento relativas aos incidentes, as informações recebidas foram consolidadas e organizadas no formato em que se apresentam neste Plano, formando protocolos que projetam cenários, medidas preventivas, definem as ações em momento de crise, identificam responsáveis pelas ações de resposta aos incidentes, além de estipular ações que devem ser tomadas após a ocorrência de incidentes.

Ressalta-se que esta é a primeira versão do PCN. Objetiva-se que gradualmente o tratamento de outros incidentes críticos seja incorporado e que haja periódica atualização.

Equipe de Resposta a Incidentes

A **Equipe de Resposta a Incidentes – ERI** é responsável por **gerenciar incidentes críticos** que possam comprometer a continuidade dos serviços prestados pela Secretaria de Serviços Compartilhados (SSC). O objetivo é assegurar o funcionamento das operações em nível adequado até o restabelecimento completo da normalidade como também assegurar que não haja ruídos de comunicação no curso do tratamento de incidentes.

A ERI não se confunde com a Equipe de Tratamento e Resposta a Incidentes – ETIR, que tem a prerrogativa de atuar no tratamento de incidentes específicos, de acordo com normativos existentes. Assim, se o tratamento de determinado incidente compõe a ETIR devido a seu objeto, este PCN não será ativado.

A ERI será composta pelas pessoas titulares das diretorias da SSC, por membro do gabinete do Secretário e da Coordenação de Comunicação Interna. As pessoas membros podem delegar representantes ou suplentes e, quando necessário, convidar especialistas externos para reuniões específicas.

A ERI será responsável por:

1. Gerenciar riscos associados aos incidentes.
2. Analisar informações para diagnóstico da crise.
3. Coordenar o trabalho das equipes operacionais e propor ações corretivas.
4. Monitorar a execução do plano de comunicação em situações de crise e validar comunicados públicos.
5. Avaliar o tratamento dos incidentes e propor revisões nos protocolos existentes.

A ERI terá **Reuniões Extraordinárias** convocadas, a qualquer momento após a tomada de ciência do incidente, pela pessoa líder da diretoria responsável por seu tratamento.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Obrigatoriamente, membro do gabinete da SSC e da Coordenação de Comunicação devem ser convocados para a reunião.

Sempre que convocadas, as reuniões serão secretariadas pela Diretoria de Gestão Estratégica – DGE, cuja função será elaborar atas de reunião, manter o arquivo da documentação relativa às atividades de tratamento de incidentes, comunicar, encaminhar e fazer publicar informações relacionadas ao PCN.

A pessoa líder da diretoria responsável pelo tratamento do incidente designará **técnicos** de sua área para executar ações práticas relacionadas ao tratamento do incidente. Esta equipe deverá:

- Implementar ações previstas neste PCN.
- Coletar informações e planejar medidas para mitigar os impactos dos incidentes.
- Garantir alinhamento com protocolos de segurança.
- Criar relatório informando as principais ocorrências relacionadas ao tratamento do incidente.

Em caso de necessidade, a pessoa líder da diretoria responsável pelo tratamento do incidente ativará e coordenará **Sala de Crise**.

Atividades da Sala de Crise:

- Centralizar a gestão de informações e decisões.
- Mitigar incidentes e assegurar a retomada normal das operações.
- Apresentar relatório acerca do gerenciamento de incidentes.
- Garantir que as ações tomadas no tratamento de incidentes estejam alinhadas aos protocolos gerais e de segurança existentes no âmbito no Ministério da Gestão e da Inovação em Serviços Públicos;
- Propor atualizações no Plano de Continuidade de Negócios

A ERI deve avaliar as medidas tomadas durante incidentes, identificando oportunidades de melhoria nos procedimentos e protocolos para fortalecer a resiliência da SSC em situações futuras.

A Sala de Crise será desativada após a normalização das atividades e apresentação de relatório final.

Implementação do Plano de Continuidade de Negócio

A eficácia do PCN pressupõe adoção de ações que corroborem para o conhecimento do Plano e para o fomento da cultura de gestão de riscos no âmbito da SSC. A capacitação das equipes é um dos pilares do PCN, porque garante o reconhecimento da criticidade das ocorrências, a

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

assertividade das ações durante incidentes e sua devida comunicação. A capacitação deve envolver simulações de exercícios práticos e programas de reciclagem periódica.

Ações de comunicação também são fundamentais para estimular o conhecimento acerca das principais diretrizes do Plano. Assim, como extensão do Plano serão criadas e divulgadas cartilhas físicas e virtuais acerca do tratamento de incidentes críticos, elaborados informes sobre a importância do Plano, de forma a levar ao conhecimento de todos como cada equipe e colaboradores deve fazer em momentos de crise.

As comunicações acerca do Plano serão divulgadas por sítio na internet ou, quando conveniente, por meio físico.

Não menos importante é a necessidade de alinhamento deste Plano com o Plano de Gestão de Incidentes com Dados Pessoais. É importante que as ações previstas no PCN estejam integradas com os demais planos existentes.

Protocolo de Comunicação em Situações de Crise

Um Protocolo de Comunicação em Situação de Crise tem como objetivo estabelecer diretrizes e procedimentos a serem seguidos pelo Núcleo de Comunicação do Comitê de Gerenciamento de Crise (CGC) durante o gerenciamento de incidentes críticos. É desenvolvido para garantir uma comunicação clara, eficaz e coerente em todas as fases da gestão de crises, minimizando impactos e preservando a confiança e a imagem institucional.

Detalha procedimentos específicos que devem ser seguidos ao longo das diferentes fases de uma crise, desde sua identificação e contenção, passando pela gestão ativa do incidente, até o período de pós-crise.

Orienta que a comunicação em situações de crise deve abordar princípios fundamentais como transparência, agilidade, consistência e sensibilidade às partes interessadas.

Neste sentido, a SSC desenvolveu um protocolo que, além de atender as recomendações citadas acima, alinha suas diretrizes com outros documentos ou normas de comunicação existentes, tendo caráter subsidiário. Assim sendo, ele complementa e não substitui protocolos previamente estabelecidos, criando uma abordagem integrada e abrangente para a gestão comunicacional em situações críticas.

O Protocolo de Comunicação em Situação de Crise, para efeito deste PCN, compõe este documento no seu **Anexo 01**.

Protocolos de incidentes críticos

Os protocolos de incidentes críticos são componentes projetados para garantir uma resposta rápida, coordenada e eficaz a eventos que podem comprometer a operação da organização. Esses protocolos servem como guias práticos e padronizados para lidar com situações adversas, ajudando a minimizar impactos negativos e a proteger os recursos mais valiosos, como pessoas, ativos, informações e a reputação institucional.

Este item apresenta os procedimentos necessários para identificar, classificar e responder a diferentes tipos de incidentes críticos, abrangendo desde interrupções tecnológicas até desastres naturais ou falhas significativas de processos.

Na composição destes procedimentos temos a definição clara de papéis e responsabilidades e o alinhamento entre equipes como elementos fundamentais para o sucesso na gestão de crises. Além disso, os protocolos estabelecem ações específicas para a comunicação, contenção, mitigação e recuperação durante e após a ocorrência de incidentes.

A implementação desses protocolos exige não apenas o planejamento prévio, mas também a divulgação do Plano, treinamento contínuo, testes e simulações, além do comprometimento de todos os níveis organizacionais da SSC.

As práticas aqui documentadas e testadas, preparam a SSC para enfrentar adversidades de maneira estruturada, fortalecendo sua resiliência e garantindo a continuidade de suas operações em cenários de crises e alta pressão.

Neste item serão detalhados os incidentes críticos tratados neste documento, e os mecanismos de comunicação e coordenação, assegurando uma abordagem abrangente e integrada para lidar com as situações crises de forma alinhada ao ciclo de resposta a incidentes representado na figura abaixo



Figura 3 – Ciclo de resposta a incidentes

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

INCIDENTE	DESCRIÇÃO	ANEXO
Pagamento de Folha	Trata de evento que possa ocasionar em atraso no pagamento da folha de pagamento dos servidores.	02
Incidentes Contratuais	Trata de incidentes relacionados à descontinuidade contratual, especialmente os relacionados ao funcionamento mínimo dos órgãos (manutenção predial, CPD e datacenter).	03
Indisponibilidade de recursos tecnológicos críticos	Sistema CompartilhaServiços	04
	Sistema SEI	05
Infraestrutura	Alagamento	06
	Incêndio	07
	Queda de Energia	08
Ocupação de Prédio Público	Trata de incidente relacionado à ocupação de prédio público.	09

Revisão do Plano de Continuidade de Negócio

A revisão periódica do PCN é essencial para garantir sua eficácia e alinhamento às mudanças estratégicas, organizacionais, tecnológicas e regulatórias. A rotina deve incluir:

- Periodicidade:** Realizar revisões completas pelo menos semestralmente, com revisões adicionais após eventos críticos ou mudanças significativas na estrutura ou processos da organização.
- Atualização de Informações:** Verificar se os contatos, recursos, responsabilidades e procedimentos descritos no PCN permanecem atualizados e relevantes.
- Avaliação de Riscos:** Revisar a análise de riscos para identificar novos cenários que possam impactar a continuidade do negócio, ajustando estratégias conforme necessário.
- Testes e Simulações:** Incorporar resultados de testes e exercícios práticos para identificar lacunas e propor melhorias ao plano.
- Feedback dos Interessados:** Coletar sugestões de colaboradores, gestores e partes interessadas para ajustar o PCN às necessidades reais da organização.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

- **Documentação e Aprovação:** Formalizar todas as alterações realizadas, garantindo que a versão revisada seja distribuída e aprovada pelos responsáveis pela governança do PCN.

Essa rotina assegura que o PCN permaneça funcional, atualizado e preparado para responder de forma eficaz a incidentes que possam comprometer as operações críticas.

Anexo 01 - Protocolo de Comunicação em Situações de Crise

1. Apresentação

Este protocolo estabelece instruções a serem consideradas e procedimentos a serem adotados pelo núcleo de comunicação do Comitê de Gerenciamento de Crise – CGC no curso do gerenciamento de incidentes críticos. A primeira parte do protocolo apresenta instruções gerais acerca da forma que a comunicação deve ser realizada em um cenário de crise. A segunda parte expõe procedimentos específicos que devem ser observados no curso de um incidente, englobando as fases do gerenciamento da crise e o pós-crise. Ressalta-se que este protocolo tem caráter subsidiário, não afastando protocolos de comunicação eventualmente existentes.

2. Forma de Comunicação no Comitê

A comunicação entre os membros do CGC deverá ser preferencialmente realizada por meio de correio eletrônico sobretudo pela utilização da **lista de e-mail de crise (XXXXXXX)**. Outros meios de comunicação de caráter particular deverão ser utilizados apenas em situações de exceção. Entretanto, por segurança, contatos pessoais dos titulares de unidades organizacionais deverão estar disponíveis à Secretaria Executiva do Comitê.

As informações relevantes sobre o gerenciamento da crise, tais como contatos pessoais e funcionais de todos os envolvidos, relatórios do desempenho da Secretaria e lições aprendidas, serão mantidas no **ambiente de colaboração (XXXXX)**, gerenciado pela Secretaria Executiva do Comitê.

Em caso de ameaça de crise identificada pelo próprio gabinete de Comunicação, seja por questionamentos da imprensa ou contato feito pela mídia ou pela sociedade, a Coordenação de Comunicação Interna, deverá informar prontamente ao Presidente/Secretário do Comitê de Crise e este deverá seguir o protocolo definido no Plano de Continuidade de Negócio.

3. Orientações sobre vocabulário a ser adotado em situações de crise

Sem desconsiderar orientações de comunicação de crise existentes no Ministério, no curso do tratamento de incidentes críticos, é essencial que seja adotado vocabulário padronizado para melhorar a eficiência da Secretaria na resposta a incidentes e garantir que todos os envolvidos compreendam claramente a situação.

3.1. Princípios

São três os princípios de uma comunicação que lide adequadamente com situações de crise:

- **Transparência:** Ser transparente, sem expor informações sensíveis.
- **Empatia e Compreensão:** Utilizar uma linguagem que demonstre sensibilidade com as partes impactadas.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

- **Foco na Solução:** Promover uma linguagem voltada para a ação e solução, que tranquilize o público sobre o controle e os próximos passos.

Diretrizes de Estilo:

- **Tom e Voz:** É desejável que o tom seja calmo, confiante e humano, deve-se evitar linguagem excessivamente técnica ou jargões internos.
- **Linguagem Positiva:** Mesmo ao comunicar informações difíceis, deve-se buscar a adoção de termos positivos.
- **Evitar Exageros e Promessas Incertas:** Expressões que impliquem garantias absolutas (ex: "100% seguro") devem ser evitadas.

3.2. Sugestões de Vocabulário:

Expressões Recomendadas:

- Ao invés vez de "problema", "transtorno", opte por "desafio" ou "situação delicada".
- Para "falha", usar "interrupção temporária" ou "dificuldade técnica".
- Para "erro", usar "inconsistência" ou "desvio não planejado".
- Em respostas a perguntas, sugerir frases como "Estamos trabalhando ativamente para resolver isso" ou "Estamos comprometidos em fazer o melhor possível".

Expressões a Serem Evitadas:

- Evitar expressões como "não é culpa nossa", "não podemos fazer nada", "sempre" e "nunca", ou outras expressões defensivas ou inflexíveis.
- **Não use "sem comentários".** Parece que se tem algo a esconder. Em vez disso, utilize "entendemos que há uma situação e não estamos preparados para compartilhar informações adicionais neste momento". Também é possível direcionar os demandantes de informações a uma autoridade externa, se aplicável.

Vocabulário Alternativo para Comunicação Delicada:

- Para expressões negativas, como "cancelado", usar "adiado" ou "reprogramado".
- Em vez de "não podemos" usar "neste momento, estamos avaliando opções".

3.3. Exemplos de Frases para Situações Específicas:

- **Pedido de desculpas:** "Lamentamos sinceramente a situação e estamos empenhados em sua solução."
- **Esclarecimentos de Status:** "Estamos monitorando a situação de perto e informaremos assim que tivermos atualizações significativas."

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

- **Informar sobre próximas etapas:** "Nosso próximo passo será [ação] e manteremos todos informados.

3.4. Orientações adicionais sobre comportamentos adequados para uma comunicação assertiva em um contexto de crise:

O que fazer:

- Informar assertivamente os *stakeholders* acerca da gravidade do incidente tão logo existir diagnóstico preciso.
- Selecionar os comunicadores certos para a situação, bem como para cada fase do ciclo de vida do incidente. Realizar testes sob condições simuladas para garantir que os comunicadores desenvolvam a habilidade de lidar com pressão.
- Sempre demonstrar empatia por eventuais vítimas.
- Quando não souber de alguma informação específica, comunicar que não dispõe da informação no momento, mas que está buscando.
- Acompanhe a Internet e as redes sociais em busca de informações incompletas ou equivocadas, que possam prejudicar a reputação da secretaria no tratamento do incidente.
- Forneça informações básicas sobre o incidente crítico para todos os membros da força de trabalho, especialmente sobre como lidar com dúvidas do público sobre o incidente. Lembre-se que fora da equipe de comunicação de crise, nenhum membro da força de trabalho deveria se pronunciar sobre o incidente crítico. Eles precisam saber a quem encaminhar as perguntas recebidas.

O que não fazer?

- Ainda que reações iniciais geralmente sejam baseadas em emoções, não se deve comunicar de forma impulsiva. O plano de gerenciamento de crise ajudará a moderar o medo e a incerteza da situação.
- Evitar buscar por culpados pelo incidente. Focar na em sua resolução e sanar possíveis fragilidades.
- Não comunicar de forma arrogante ou impaciente. Buscar sempre que possível um tom conciliatório.
- Não especular sobre coisas fora do alcance de controle da Secretaria.
- Nunca mentir ou exagerar. No mundo atual de mídias sociais e de trilhas de auditoria, é preciso priorizar a reputação da organização.
- Não se deve fazer promessas que não se pode cumprir.
- Não deixe que a alta gestão saia do script.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

- Não declare que o problema está resolvido se ainda não estiver.

3.5. Modelos padrões para comunicação de crise.

Modelo para mensagens de baixa gravidade:

A Secretaria de Serviços Compartilhados informa que em XX/XX ocorreu um incidente de segurança relacionado a XXXXXXXXXXXX. Prezando pela transparência, o Comitê de Gerenciamento de Crise informa que a situação já está sendo tratada e envolve os seguintes aspectos: XXXXXX. Nesta fase, não é possível fornecer detalhes mais precisos sobre a situação, porém garantimos que nossas equipes técnicas estão trabalhando para a pronta resolução do incidente, de modo que o serviço XXXXX retorne à normalidade o mais rápido possível.

Modelo para mensagens de alta gravidade:

A Secretaria de Serviços Compartilhados (SSC) lamenta confirmar a situação XXXX ocorrida em XXXX. As autoridades XXXX foram notificadas e estamos trabalhando em estreita colaboração para controlar o impacto deste incidente, de modo a restaurar a provisão adequada dos serviços para nossos usuários o mais rápido possível. Ainda é cedo para entender com precisão quais ativos foram comprometidos. O incidente XXXX não significa automaticamente que XXXXXX. O Comitê de Gerenciamento de Crise está tomando todas as precauções para diagnosticar a ocorrência com precisão, mas neste momento não temos motivos para acreditar que o cenário XXXXXX se materialize. A SSC está comprometida em trabalhar nesta investigação de modo a dirimir as preocupações de nossos usuários. A confiança de nossos usuários em relação à qualidade de nossos serviços é nosso maior ativo. Prezando pela transparência, informamos que nossa próxima atualização estará disponibilizada em nosso site às [horário]. Enquanto isso, se houver alguma dúvida adicional, entre em contato [nome], por meio de [telefone ou e-mail].

3.6. Material complementar para comunicação de incidentes

A Coordenação de Comunicação Interna da SSC preparou material específico sobre a comunicação de incidentes que pode ser acessado na seguinte página: [Comunicação em Ação](#).

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

4. Procedimentos específicos para comunicação de crise

4.1. Check list

Ações básicas (Ameaça de crise)	Tempo previsto
Tomar ciência sobre a ameaça de crise e identificar partes diretamente interessadas.	
Realizar análise inicial acerca do risco de imagem e reputação do incidente específico e comunicar impressões ao CGC.	30 min
Se necessário, início do monitoramento da imprensa e das mídias sociais e manutenção do Comitê de Crise informado sobre essa repercussão.	
A partir do exame do protocolo de avaliação do incidente, elencar informações necessárias para a construção do posicionamento para público interno. Se necessário contatar coordenador da equipe operacional para coleta de informações adicionais.	
Se necessário, contatar assessoria de comunicação do MGI para a construção do posicionamento para público externo e para definir estratégia.	
Elaborar mensagem-chave e posicionamento oficial para público interno e externo (alinhar com ASCOM) (stakeholders diretamente afetados).	
Se necessário, sugerir posicionamento oficial, porta-voz e forma de divulgação para a imprensa para aprovação do Comitê.	
Se necessário, preparar publicação no Portal da SSC, enviar para <i>mailing list</i> da imprensa e preparar divulgação na Intranet.	
Informar sobre a repercussão na imprensa e nas mídias sociais até o momento e definir demais estratégias de comunicação com o Presidente do Comitê de Crise.	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

5. Caracterização de crise finalizada ou controlada (pós-crise)

5.1. Check list

Ações básicas	Tempo previsto
Elaborar e divulgar comunicado informando o encerramento da crise	
Análise do conteúdo veiculado pela imprensa desde o início da crise e da repercussão nas mídias sociais	
Divulgação sobre as ações tomadas no pós-crise (conforme estratégia).	
Envio de relatório sobre as ações de comunicação interna, a repercussão e as oportunidades de melhoria para o comitê.	

6. Referências

- GARTNER. Top Strategic Technology Trends for 2023. Disponível para assinantes Gartner. Gartner, 2022.
- GARTNER. Quick Answer: 3 Communicationtatics for Change Management Success. Disponível para assinantes Gartner. Gartner, 2024.
- GARTNER. Build Your Security Incident Crisis Communications. Disponível para assinantes Gartner. Gartner, 2022.
- GARTNER. Business Continuity Plan Template for Midsize Enterprises. Disponível para assinantes Gartner. Gartner, 2023.
- GARTNER. Tips to Bolter Your Disaster Recovery Program. Disponível para assinantes Gartner. Gartner, 2024.

Anexo 02 - Pagamento de Folha

Um incidente na folha de pagamento refere-se a qualquer situação que comprometa a exatidão, pontualidade ou integridade dos processos relacionados à remuneração dos servidores públicos. Isso pode incluir erros no cálculo de salários, insuficiência orçamentária ou financeira, falhas na rede de acesso aos sistemas, falhas sistêmicas, acesso não autorizado a dados sensíveis ou inconsistências nas deduções obrigatórias, provocando inconsistências ou atrasos no pagamento.

Esses incidentes podem gerar impacto direto no bem-estar dos servidores e na conformidade legal do órgão, exigindo resposta imediata e ações corretivas eficazes.

Para combatê-lo, deve-se seguir o Protocolo abaixo.

Mitigação

PAGAMENTO DE FOLHA			
Gestor	Diretoria de Gestão de Pessoas		
Responsável	DGP, CGPAG. Telefone: 61 2031-6458.		
Contratos Relacionados	Convênios firmados entre as instituições bancárias e o órgão central do SIPEC		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
SSC	CGPAG	2021-5810 ssc@gestao.gov.br	Imediato
SGP	CGPAG	2020-1943 Sgp.desin@gestao.gov.br	Imediato
DTI - Se for problema de internet	CGPAG	2021-5330 dti.ssc@gestao.gov.br	Imediato
Consequências secundárias			
Demandas judiciais e contencioso administrativo. Dano reputacional.			

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Medidas preventivas		
Ameaça	Resposta	Responsável
Paralização de servidores - tesouro, FOF, SERPRO e demais que operacionalizam a folha	Alertar as instâncias superiores das instituições sobre a paralização	CGPAG
Insuficiência Orçamentaria	Fazer pedido de suplementação orçamentária	CGPAG
Insuficiência Financeira	Pedir a complementação financeira	CGPAG
Indisponibilidade de rede - SEI, SIAPE	Acionar a DTI	CGPAG
Sistemas lentos - SIAFI ocorre com frequência	Acionar a DTI para a DTI acionar o tesouro	CGPAG
Rotatividade da equipe responsável pela apropriação	Estender horários de trabalho/capacitar mais servidores	CGPAG
Problemas nos bancos conveniados	Acionar os bancos	CGPAG
Treinamentos		
Escopo	Público-alvo/alcance	Responsável
Gestão orçamentária e financeira	Servidores da CGPAG/DGP	CGPAG/DGP
Apropriação da folha de pagamento	Servidores da CGPAG/DGP	CGPAG/DGP

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Resposta

PAGAMENTO DE FOLHA			
Gestor	Diretoria de Gestão de Pessoas (DGP)		
Responsável	<ul style="list-style-type: none">• DGP, CGPAG.• Telefone: 61 2031-6458.		
Contratos Relacionados	Convênios firmados entre as instituições bancárias e o órgão central do SIPEC		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
SSC	CGPAG	2021-5810 ssc@gestao.gov.br	Imediato
SGP	CGPAG	2020-1943 Sgp.desin@gestao.gov.br	Imediato
DTI - Se for problema de internet	CGPAG	2021-5330 dti.ssc@gestao.gov.br	Imediato
Resposta a incidentes por cenários			
Cenário 1: Paralisação de servidores (Tesouro, SOF, SERPRO e demais órgãos com interface com a folha)			
Responsável		Atribuição	
DGP		<ul style="list-style-type: none">• Acionar a instância superior (SSC) para indicação de medidas decididas pela Alta Administração.• Acionar o órgão central do SIPEC (SGP) e (SSC) para conhecimento, acompanhamento e, se possível, indicação da providência a ser adotada.	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

PAGAMENTO DE FOLHA	
Alternativas para a continuidade do negócio	
Responsável	Atribuição
SGP	Indicação de medidas operacionais de contorno
SSC	Indicação das medidas administrativas a serem adotadas
Cenário 2: Insuficiência Orçamentária	
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DGP	Verificar, junto à DFC, as opções disponíveis para a execução das despesas.
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DGP	Verificar, junto à DFC, as opções disponíveis para a execução das despesas.
Cenário 3: Insuficiência Financeira	
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DGP	Formalizar pedido de descentralização para que a unidade setorial responsável envie os recursos adicionais
DGP	Acionar a instância superior (SSC) para acompanhamento e, se necessário, gestão junto aos órgãos envolvidos.
Alternativas para a continuidade do negócio	
Responsável	Atribuição

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

PAGAMENTO DE FOLHA	
SGP	Indicação de medidas operacionais de contorno
SSC	Indicação das medidas administrativas a serem adotadas
Cenário 4: Indisponibilidade ou lentidão de Rede: SEI, SIAPE e SIAFI	
Responsável	Atribuição
DGP	Acionar a DTI para verificar se o problema é na rede interna do MGI ou rede SERPRO.
DGP	Acionar o órgão central do SIPEC (SGP) e (SSC) para conhecimento e solução, caso o problema seja na rede SERPRO/SIAPE.
DGP	Acionar a instância superior (SSC) para acompanhamento e, se necessário, gestão junto aos órgãos envolvidos.
DGP	Acionar a STN para conhecimento e solução, caso o problema seja na rede SERPRO/SIAFI.
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DGP	Colocar a equipe responsável em trabalho remoto, caso o problema seja na rede interna do MGI
SGP	Indicação de medidas operacionais de contorno, caso o problema seja no SIAPE
STN	Indicação de medidas operacionais de contorno, caso o problema seja no SIAFI
Cenário 5: Lentidão de sistemas em dias críticos (SIAFI)	

Plano de Continuidade de Negócios
 Ministério da Gestão e Inovação em Serviços Públicos

PAGAMENTO DE FOLHA	
Responsável	Atribuição
DGP	Acionar a DTI para verificar se o problema é na rede interna do MGI.
DGP	Acionar a instância superior (SSC) para acompanhamento e, se necessário, gestão junto aos órgãos envolvidos.
DGP	Acionar a STN para conhecimento e solução, caso o problema seja na rede SERPRO/SIAFI.
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DGP	Colocar a equipe responsável em trabalho remoto, caso o problema seja na rede interna do MGI
STN	Indicação de medidas operacionais de contorno, caso o problema seja no SIAFI
Cenário 6: Rotatividade Equipe responsável pela apropriação	
Responsável	Atribuição
DGP	Acionar a instância superior (SSC) para acompanhamento e indicação de medidas de apoio.
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DGP	Ampliar a disseminação de conhecimento para que outros agentes possam atuar nos processos de apropriação da folha de pagamento.

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

PAGAMENTO DE FOLHA	
DGP	Requisitar servidores de outros órgãos.
DGP	Conferir boa estrutura de funções/gratificações para viabilizar a retenção dos servidores.
Cenário 7: Problemas com bancos conveniados	
Responsável	Atribuição
DGP	<ul style="list-style-type: none">• Acionar a instância superior (SSC) para acompanhamento; e• Se necessário, gestão junto aos bancos envolvidos e estabelecer rotina para resolução
DGP	
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DGP	Ajustar os dados do convênio no SIAPE
DGP	<ul style="list-style-type: none">• Reenviar a Ordem Bancária da Folha; e• Solicitar prazo D+0 para a STN.
DGP	Liberar o financeiro em D+0

Avaliação do Incidente

AVALIANDO O INCIDENTE - PAGAMENTO DE FOLHA					
	1	2	3	4	5
O incidente afeta a entrega de serviços públicos em que escala? 1 se não afeta; 5 se afeta para todos os usuários do serviço.					
O incidente interrompe as atividades de suporte? 1 se não interrompe; 5 se interrompe para todos os servidores do órgão					
Quantos órgãos são afetados pelo incidente? 1 = 1 órgão afetado; 2 = entre 2 e até 5 órgãos afetados; 3 = entre 5 e até 8 órgãos afetados; 4 = entre 9 e até 12 órgãos afetados; 5 = acima de 12 órgãos afetados;					
O incidente afeta a imagem/reputação da organização? 1 = não afeta; 5 = afeta.					
O incidente compromete ou coloca em riscos ativos de informações (em meios digitais ou físicos)? Se sim, acionar ETIR e POSIC.					
CONSEQUÊNCIAS SECUNDÁRIAS:					
Consequência 2:					
Consequência 3:					
Consequência 4:					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião)					
Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação)					

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).

Classificação da Crise para efeito de Comunicação

1. Não é necessário comunicar
- 2.

AVALIANDO O INCIDENTE - PAGAMENTO DE FOLHA					
	1	2	3	4	5
CONSEQUÊNCIAS SECUNDÁRIAS:					
Consequência 2:					
Consequência 3:					
Consequência 4:					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião)					
Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação)					
Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).					

Pós-Incidente

PAGAMENTO DE FOLHA

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Documentação do Incidente	Responsável
Ofício	Detalhar o incidente, apontar as instâncias envolvidas e, se for possível, indicar solução para correção.
Atualização da política, contratos e protocolo	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável
Fluxograma da Folha de Pagamento	DGP

Anexo 03 - Incidentes Contratuais

Um incidente contratual com empresas contratadas de um ministério ocorre quando há descumprimento de cláusulas contratuais, atrasos na entrega de serviços ou produtos, falhas de qualidade, interrupções na execução contratual ou conflitos jurídicos. Essas situações podem comprometer projetos e atividades essenciais do órgão, gerando riscos financeiros, administrativos e operacionais. A gestão adequada desses incidentes é crucial para mitigar impactos e garantir a continuidade dos serviços contratados.

Para combater incidentes contratuais, deve-se seguir o Protocolo abaixo.

Mitigação

CONTRATOS DE MANUTENÇÃO PREDIAL			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	<ul style="list-style-type: none">• CGERP- Coordenação Geral de Infraestrutura Predial.• Telefone: 61 2021-5055.		
Contratos Relacionados	<ul style="list-style-type: none">• Manutenção predial, CPD – data center e serviço de dados (DTI),• manutenção de elevadores,• manutenção de telefonia fixa,• manutenção de ar-condicionado,• manutenção de rede de dados – Cabos.		
Contatos Úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
CGERP	Unidade de Manutenção predial		
Órgãos ColaboraGov	Gabinete		
SSC	Central de atendimento CB		
Consequências secundárias			

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

<ul style="list-style-type: none"> • Datacenter; • Risco de vida; • Avaria de equipamentos; e • Estrutura da edificação - elétrica, hidráulica, estrutura física. 		
Medidas Preventivas		
Ameaça	Resposta	Responsável
Falência da empresa contratada ou inexecução total	Contratação emergencial	CGERP
Recusa de prorrogação de contrato pela empresa	<ul style="list-style-type: none"> • 1^a - Negociação com a empresa • 2^a - Nova Contratação • 3^a - Emergencial quando o tempo para nova contratação é insuficiente - não se consegui negociar prorrogação por poucos meses 	CGERP/CGCAF
Atraso no planejamento de contratações (tempestividade)	Iniciar o planejamento com prazo suficiente para ele conclusão compatível com cada necessidade	CGERP
Falta de orçamento	<ul style="list-style-type: none"> • 1^a - Programação orçamentária • 2^a - Restrição orçamentária - reduzir o contrato 	CGERP/Equipe de manutenção
Rateio - Descentralização de recursos	<ul style="list-style-type: none"> • Oficializar o órgão que não descentralizou, • Reduzir o contrato, • Realizar suplementação própria 	CGERP
Greve dos terceirizados	Negociação com a empresa para continuidade dos serviços	CGERP
Inexecução parcial do contrato	Nova contratação	CGERP
Treinamentos		
Escopo	Público-alvo/alcance	Responsável

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Cursos de gestão contratual	Servidores, Fiscais e gestores dos contratos e Equipes técnicas	CGERP e DGP
--------------------------------	--------------------------------------------------------------------	-------------

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Resposta

CONTRATOS DE MANUTENÇÃO PREDIAL			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	CGERP- Coordenação Geral de Infraestrutura Predial. Telefone: 61 2021-5055.		
Contratos Relacionados	<ul style="list-style-type: none">• Manutenção predial, CPD – data center e serviço de dados (DTI),• Manutenção de elevadores,• Manutenção de telefonia fixa,• Manutenção de ar-condicionado,• Manutenção de rede de dados – Cabos.		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Ministérios suportados pelo ColaboraGov	Coordenação-Geral de Relacionamento em Serviços Tecnológicos Compartilhados	<ul style="list-style-type: none">• WhatsApp,• E-mail	20 minutos
Resposta a incidentes por cenários			
Cenário 1: Encerramento do contrato - necessidade de contrato emergencial			
Responsável		Atribuição	
CGERP		<p>Iniciar contratação emergencial</p> <p>Análise do risco: avaliar o que manter e como manter enquanto a nova contratação não ocorrer - necessidade de contratação específica? Possível empréstimo de profissional de outros</p>	
Alternativas para a continuidade do negócio			

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Responsável	Atribuição
N/A	N/A
Cenário 2: Inexecução parcial do contrato (Empresa não prorroga o contrato)	
Responsável	Atribuição
Gestor de contrato	<ul style="list-style-type: none"> • Sugerir de nova licitação; e • Avaliar o tempo de sobrevida do contrato
CGERP	Análise do risco: avaliar o que manter e como manter enquanto a nova contratação não ocorrer - necessidade de contratação específica? Possível empréstimo de profissional de outros
Alternativas para a continuidade do negócio	
Responsável	Atribuição
CGERP	Realizar contratação emergencial
Cenário 3: Atraso na licitação/ contratação	
Responsável	Atribuição
CGERP	<ul style="list-style-type: none"> • 1^a avaliar prorrogação excepcional do contrato • 2^a contratação emergencial • Análise do risco: avaliar o que manter e como manter enquanto a nova contratação não ocorrer - necessidade de contratação específica? Possível empréstimo de profissional de outros
Alternativas para a continuidade do negócio	
Responsável	Atribuição
CGERP	prorrogação excepcional do contrato ou contratação emergencial.

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Avaliação do Incidente

AVALIANDO O INCIDENTE - CONTRATOS DE MANUTENÇÃO PREDIAL					
	1	2	3	4	5
O incidente afeta a entrega de serviços público em que escala? 1 se não afeta; 5 se afeta para todos os usuários do serviço.					
O incidente interrompe as atividades de suporte? 1 se não interrompe; 5 se interrompe para todos os servidores do órgão					
Quantos órgãos são afetados pelo incidente? 1 = 1 órgão afetado; 2 = entre 2 e até 5 órgãos afetados; 3 = entre 5 e até 8 órgãos afetados; 4 = entre 9 e até 12 órgãos afetados; 5 = acima de 12 órgãos afetados;					
O incidente afeta a imagem/reputação da organização? 1 = não afeta; 5 = afeta.					
O incidente a compromete ou coloca em riscos ativos de informações (em meios digitais ou físicos)? Se sim, acionar ETIR e POSIC.					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião)					
Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação)					
Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).					

Pós-Incidente

CONTRATOS DE MANUTENÇÃO PREDIAL	
Documentação do Incidente	Responsável
Análise de risco / nota técnica de sanção	Gestor de contrato
Atualização da política, contratos e protocolo	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável
Mapa de risco	Gestor de contrato

Anexo 04 - Indisponibilidade de recursos tecnológicos críticos - CompartilhaServiços

A indisponibilidade de recursos tecnológicos críticos, no contexto de compartilhamento de serviços, afeta sistemas, plataformas ou infraestruturas compartilhadas entre órgãos ou departamentos do Ministério.

Isso pode afetar diretamente a execução de processos interdependentes, como acesso a bases de dados, sistemas de gestão ou ferramentas colaborativas, interrompendo atividades essenciais.

Uma resposta rápida e coordenada é necessária para restabelecer os serviços e minimizar impactos operacionais e institucionais. Para combater este tipo de incidente, deve-se seguir o Protocolo abaixo.

Mitigação

COMPARTILHA SERVIÇOS			
Gestor	Diretoria de Tecnologia da Informação (DTI)		
Responsável	Coordenação-Geral de Relacionamento em Serviços Tecnológicos Compartilhados. Telefone: 61 2021-5055.		
Contratos Relacionados	Central IT 12/2022 - SEI nº XXXXX		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Ministérios suportados pelo ColaboraGov	Coordenação-Geral de Relacionamento em Serviços Tecnológicos Compartilhados	<ul style="list-style-type: none">WhatsApp,E-mail	20 minutos
Consequências secundárias			

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Clientes do ColaboraGov deixam de registrar as solicitações de serviços.		
Medidas preventivas		
Ameaça	Resposta	Responsável
Falhas no ambiente computacional.	Uso de meios alternativos para solicitação de serviços. Exemplos: <ul style="list-style-type: none">• Canal 0800,• Telefone,• E-mail,• WhatsApp.	Coordenador-Geral de Relacionamento em Serviços Tecnológicos Compartilhados
Falhas de conectividade de rede.	Uso de meios alternativos para solicitação de serviços. Exemplos: <ul style="list-style-type: none">• Canal 0800,• Telefone,• E-mail,• WhatsApp	Coordenador-Geral de Relacionamento em Serviços Tecnológicos Compartilhados
Ataque cibernético.	Uso de meios alternativos para solicitação de serviços. Exemplos: <ul style="list-style-type: none">• Canal 0800,• Telefone,• E-mail,• WhatsApp.	Coordenador-Geral de Relacionamento em Serviços Tecnológicos Compartilhados
Treinamentos		
Escopo	Público-alvo/alcance	Responsável

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Resposta

COMPARTILHA SERVIÇOS			
Gestor	Diretoria de Tecnologia da Informação (DTI)		
Responsável	<ul style="list-style-type: none">Coordenação-Geral de Relacionamento em Serviços Tecnológicos Compartilhados.Telefone: 61 2021-5055.		
Contratos Relacionados	Central IT 12/2022 - SEI nº XXXXX		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Ministérios suportados pelo ColaboraGov	Coordenação-Geral de Relacionamento em Serviços Tecnológicos Compartilhados	WhatsApp, e-mail	20 minutos
Resposta a incidentes por cenários			
Cenário 1:			
Responsável	Atribuição		
Alternativas para a continuidade do negócio			
Responsável	Atribuição		

Avaliação do Incidente

AVALIANDO O INCIDENTE					
	1	2	3	4	5
O incidente afeta a entrega de serviços públicos em que escala? 1 = se não afeta; 5 = se afeta para todos os usuários do serviço.					
O incidente interrompe as atividades de suporte? 1 = se não interrompe; 5 = se interrompe para todos os servidores do órgão					
Quantos órgãos são afetados pelo incidente? 1 = 1 órgão afetado; 2 = entre 2 e até 5 órgãos afetados; 3 = entre 5 e até 8 órgãos afetados; 4 = entre 9 e até 12 órgãos afetados; 5 = acima de 12 órgãos afetados;					
O incidente afeta a imagem/reputação da organização? 1 = não afeta; 5 = afeta.					
O incidente a compromete ou coloca em riscos ativos de informações (em meios digitais ou físicos)? Se sim, acionar ETIR e POSIC.					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião)					
Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação)					
Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).					

Pós-Incidente

COMPARTILHA SERVIÇOS	
Documentação do Incidente	Responsável
Plano de Continuidade de Negócios	DTI
Plano de resposta a incidentes	DTI
Plano de backup	DTI
Atualização da política, contratos e protocolo	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável

Anexo 05 - Indisponibilidade de recursos tecnológicos críticos - Sistema SEI

A indisponibilidade do Sistema Eletrônico de Informações (SEI) representa uma falha crítica que impacta a gestão documental e os processos administrativos do Ministério e demais órgãos do ColaboraGov.

O SEI é uma ferramenta essencial para a tramitação de processos eletrônicos no âmbito dos Ministérios, sua inoperância pode paralisar atividades, atrasar decisões e comprometer prazos legais.

Restaurar o acesso ao SEI de forma rápida é essencial para garantir a continuidade das operações e a eficiência administrativa. Nesse sentido, para combater os incidentes no SEI, deve-se seguir o Protocolo abaixo.

Mitigação

SISTEMA ELETRÔNICO DE INFORMAÇÕES (SEI)			
Gestor	Diretoria de Administração e Logística (DAL)		
Responsável	<ul style="list-style-type: none">Coordenação de Gestão de Documentação e Informação da Diretoria de Administração e Logística.Telefone: 61 XXXXXX.		
Contratos Relacionados			
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
<ul style="list-style-type: none">SGDGSIPFSerproDataprevGestor de Segurança	DTI/SSC	Relatório criptografado para a área criminalística da PF	De acordo com a gravidade e extensão dos fatos
Consequências secundárias			

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

- Perda de prazo processual;
- eventual perda de dados e informações;
- confiabilidade dos órgãos do ColaboraGov em utilizar sistemas;
- Prejuízo aos sistemas que atuam integrados ao SEI para recuperar ou inserir informações. Dentre eles:
 - ProtocoloGov.BR,
 - TramitaGov.BR,
 - SPUNET,
 - Balcão Digital,
 - E-processos,
 - Sistema de Gestão de Carreiras (SGC), e outros,
- Prejuízo para o público externos que dão entrada em serviços, acompanham processos ou recebem respostas pelo SEI ou por sistemas que se utilizam dele
- Atrasos em processos de contratação e gestão e pagamento de contratos, publicação de portarias e demais atos normativos

Medidas preventivas

Ameaças	Resposta	Responsável
<ul style="list-style-type: none">• Falha de comunicação• Indisponibilidade de infraestrutura• Inclusão de conteúdos com formato incompatível• Atualização de versão. incidente de segurança.• Ambiente ou banco do sei corrompido.	<ul style="list-style-type: none">• Plano de redundância de canal.• Monitoramento e uso de ações de segurança (backup, ambiente protegido).• Uso de ferramentas de análise e varredura de documentos e conteúdos.	DTI/SSC.

Treinamentos

Escopo	Público-alvo/alcance	Responsável

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Resposta

SISTEMA ELETRÔNICO DE INFORMAÇÕES (SEI)			
Gestor	Diretoria de Administração e Logística (DAL)		
Responsável	Coordenação de Gestão de Documentação e Informação da Diretoria de Administração e Logística. Telefone: 61 XXXXXX.		
Contratos Relacionados	NA		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Resposta a incidentes por cenários			
Cenário 1: Falhas de conectividade com a rede			
Responsável		Atribuição	
DTI		Contatar: <ul style="list-style-type: none">• Fornecedores• Infovia• Equipe responsável pela sustentação	
Alternativas para a continuidade do negócio			
Responsável		Atribuição	
DTI		Redundância de conectividade	
Cenário 2: Falhas no ambiente computacional			
Responsável		Atribuição	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

DTI	Contatar equipe responsável pela operação de TI
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DTI	Redundância de conectividade
Cenário 3: Inclusão de conteúdos com formato malicioso	
Responsável	Atribuição
DTI	Prover ferramentas de verificação de conteúdo.
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DTI	Redundância de conectividade
Cenário 4: Ataques cibernéticos	
Responsável	Atribuição
DTI	Monitoramento técnico 24/7
Alternativas para a continuidade do negócio	
Responsável	Atribuição
DTI	Redundância de conectividade
Cenário 5: indisponibilidade prolongada do sistema ou que possa gerar prejuízos em razão da urgência (Instrução Normativa DAL/ME nº 23, de 9 de maio de 2022)	
Responsável	Atribuição
Alternativas para a continuidade do negócio	

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Usuário	Praticar os atos processuais seguindo as regras aplicáveis aos processos em meio físico, utilizando-se numeração manual sequencial provisória e, posteriormente, digitalizado e incluído no processo SEI correspondente (Instrução Normativa DAL/ME nº 23, de 9 de maio de 2022)
---------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Avaliação do Incidente

AVALIANDO O INCIDENTE					
	1	2	3	4	5
O incidente afeta a entrega de serviços públicos em que escala? 1 se não afeta; 5 se afeta para todos os usuários do serviço.					
O incidente interrompe as atividades de suporte? 1 se não interrompe; 5 se interrompe para todos os servidores do órgão					
Quantos órgãos são afetados pelo incidente? 1 = 1 órgão afetado; 2 = entre 2 e até 5 órgãos afetados; 3 = entre 5 e até 8 órgãos afetados; 4 = entre 9 e até 12 órgãos afetados; 5 = acima de 12 órgãos afetados;					
O incidente afeta a imagem e reputação da organização? 1 = não afeta; 5 = afeta.					
O incidente a compromete ou coloca em riscos ativos de informações (em meios digitais ou físicos)? Se sim, acionar ETIR e POSIC.					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião)					
Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação)					
Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).					

Pós-Incidente

SISTEMA ELETRÔNICO DE INFORMAÇÕES (SEI)	
Documentação do Incidente	Responsável
Relatório criptografado, o qual, somente as equipes citadas possuem acesso, pois se trata de conteúdo forense para a área criminalística da PF.	DTI
Atualização da política, contratos e protocolo	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável
Plano de Continuidade de Negócios	DAL/DTI
Plano de resposta a incidentes	DTI
Plano de backup	DTI

Anexo 06 - Infraestrutura – Alagamento

Um incidente de infraestrutura por alagamento ocorre quando chuvas intensas, problemas de drenagem ou vazamentos d'água de grandes proporções resultam na inundação de instalações físicas do Ministério.

Esse evento pode danificar equipamentos, arquivos, sistemas elétricos, estruturas, colocam risco ativos de informações além de comprometer a segurança dos servidores e a continuidade das operações.

A resposta imediata deve ser dada seguindo o Protocolo abaixo.

Mitigação

Infraestrutura – Alagamento			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	<ul style="list-style-type: none">• Diretoria de Administração e Logística - DAL,• Coordenação geral de Segurança, Administração, Terceirização e Transporte – CGSAT,• CGERP.• Telefone: 61 2021-5055.		
Contratos Relacionados	<ul style="list-style-type: none">• Contrato de Manutenção predial,• Contrato de segurança predial,• Contrato de Brigada de Incêndio,• Contrato de limpeza,• Contrato de CFTV.		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
CAESB	CGERP	Ofício	N/A
MGI (Brigadista de plantão)	CGERP	Telefone - ramal da brigada de cada prédio	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Representante indicado por cada Órgãos ColaboraGov	CGERP	Telefone	
Consequências secundárias			
<ul style="list-style-type: none"> • Equipamento molhados; • Perda de imobiliário; • perda de ativos em geral; • perda de bens próprios, de terceiros e de contratados; • elevadores, • rede elétrica em geral, • Data Center, • Indisponibilidade de ambiente tecnológico • CFTV. 			
Medidas Preventivas			
Ameaça	Resposta	Responsável	
<ul style="list-style-type: none"> • Elevadores, • rede elétrica em geral, • Data Center, • Indisponibilidade de ambiente tecnológico • CFTV 	Limpeza de ralos e calhas	CGERP/Equipe de manutenção	
Colapso de equipamento da estrutura hidráulica	Treinar equipe para conhecer prédio, rede hidráulica.	CGERP/Equipe de manutenção	
Colapso de bombas hidráulicas	Manutenção preventiva	CGERP/Equipe de manutenção	
Tempestades	Acompanhar o site de INMET	CGERP/Equipe de manutenção	
Chuvas de vento que provocam alagamentos	Rondas	CGSAT/Equipe de segurança	
Treinamentos			
Escopo	Público-alvo/alcance	Responsável	

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Plano de prevenção e combate a incêndio e abandono PPCIA - Administração predial	Colaboradores	CGSAT – Brigada de Incêndio
----------------------------------------------------------------------------------	---------------	-----------------------------

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Resposta

Infraestrutura – Alagamento			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	Diretoria de Administração e Logística - DAL, Coordenação geral de Segurança, Administração, Terceirização e Transporte – CGSAT, CGERP. Telefone: 61 2021-5055.		
Contratos Relacionados	Manutenção predial, Contrato de segurança predial, Contrato de Brigada de Incêndio, Contrato de limpeza, Contrato de CFTV.		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
CAESB	CGERP	Ofício	N/A
MGI (Brigadista de plantão)	CGERP	Telefone (ramal da brigada de cada prédio)	
Órgãos ColaboraGov (Indicados de cada órgão)	CGERP	Telefone	
Resposta a incidentes por cenários			
Cenário 1: Alagamento externo sem afetar a edificação			
Responsável		Atribuição	
Equipe de segurança		Detecção visual e comunicação inicial	
Encarregado de manutenção		Identificação do problema e proteção dos ativos mais vulneráveis, construção de barricadas e ações para escoamento, acionar grupo no WhatsApp	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Qualquer pessoa pode detectar visualmente o problema alertar sobre o problema	N/A
-------------------------------------------------------------------------------	-----

Alternativas para a continuidade do negócio

Responsável	Atribuição
	Deslocamento da força de trabalho
	Home Office
	Realizar reparos

Cenário 2: Alagamento externos afetando a cobertura e andares superiores da edificação

Responsável	Atribuição
Equipe de Segurança	Avaliar situação, reunir com líderes, orientar vigilantes e brigadistas
Encarregado de manutenção	<ul style="list-style-type: none">• Desligar a energia• Combater com a brigada• Acionar corpo de bombeiros• Esvaziar o ambiente
Servidores	Proteger os ativos em sua propriedade

Alternativas para a continuidade do negócio

Responsável	Atribuição
	Deslocamento da força de trabalho
	Home Office
	Realizar reparos

Cenário 3: Alagamentos externo afetando o subsolo da edificação

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Responsável	Atribuição
Equipe de segurança	<ul style="list-style-type: none"> • Detecção visual e comunicação inicial, • Proteger: os elevadores em risco, quadros e QGBT, quadro geral de baixa tensão, • orientar evacuação dos locais afetados.
Encarregado de manutenção	<ul style="list-style-type: none"> • Identificação do problema e proteção dos ativos mais vulneráveis, • Construção de barricadas e ações para escoamento, • Acionar grupo no WhatsApp, • Proteger elevadores em risco.
Qualquer pessoa pode detectar visualmente o problema alertar sobre o problema	<ul style="list-style-type: none"> • Desligar a energia nos quadros internos da edificação ou • Acionar a NEOENERGIA para desligar a edificação.
Alternativas para a continuidade do negócio	
Responsável	Atribuição
Equipe de manutenção	Fazer reparos
Chefe da unidade/equipe engenharia	Alocar as pessoas em outras salas/postos de trabalho
Chefias imediatas	Orientar as equipes a dar continuidade dos trabalhos de forma remota
Cenário 4: Chuva de vento	
Responsável	Atribuição
Equipe de segurança	Fechamento das janelas
Encarregado de manutenção	Verificar a qualidade da manutenção

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Cenário 5: Falha de rede hidráulica/ rede esgoto

Responsável	Atribuição
Equipamento de segurança	<ul style="list-style-type: none">• Fechar registros,• Desligar bombas,• Se água gelada desligar a refrigeração do prédio,• Proteção dos ativos em riscos
Encarregado de manutenção	Proteção dos ativos em riscos
Servidores	Proteção dos ativos de sua responsabilidade

Avaliação do Incidente

AVALIANDO O INCIDENTE INFRAESTRUTURA – ALAGAMENTO					
	1	2	3	4	5
O incidente afeta a entrega de serviços públicos em que escala? 1 se não afeta; 5 se afeta para todos os usuários do serviço.					
O incidente interrompe as atividades de suporte? 1 se não interrompe; 5 se interrompe para todos os servidores do órgão					
Quantos órgãos são afetados pelo incidente? 1 = 1 órgão afetado; 2 = entre 2 e até 5 órgãos afetados; 3 = entre 5 e até 8 órgãos afetados; 4 = entre 9 e até 12 órgãos afetados; 5 = acima de 12 órgãos afetados;					
O incidente afeta a imagem/reputação da organização? 1 = não afeta; 5 = afeta.					
O incidente a compromete ou coloca em riscos ativos de informações (em meios digitais ou físicos)? Se sim, acionar ETIR e POSIC.					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião)					
Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação)					
Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).					

Pós-Incidente

INFRAESTRUTURA – ALAGAMENTO	
Documentação do Incidente	Responsável
Relatório de incidente CGSAT/CGERP	CGSAT/CGERP
Atualização da política, contratos e protocolo	
Documentos a atualizar, aprimorar ou criar no pós-incidente.	Responsável

Anexo 07 – Infraestrutura - Incêndio

Mitigação

INFRAESTRUTURA - INCÊNDIO (DAL)			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	<ul style="list-style-type: none">Coordenação geral de Segurança, Administração, Terceirização e Transporte – CGSAT.Coordenação Geral de Infraestrutura Predial- CGERP.Telefone: 61 XXXXXX.		
Contratos Relacionados	<ul style="list-style-type: none">Manutenção predial,Contrato de segurança predial,Contrato de Brigada de Incêndio,Contrato de limpeza,Contrato de CFTV.		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Corpo de bombeiros-combate	CGSAT	Telefone	Imediato
Corpo de Bombeiros - perícia	CGSAT	Telefon	Automático junto com o chamado para o combate
Brigada de incêndio	CGSAT	Telefone	Imediato
Consequências secundárias			
<ul style="list-style-type: none">Risco à vida,Perda de imobiliário,Perda de ativos em geral,			

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

<ul style="list-style-type: none">• Perda de bens próprios, terceiros e de contratados,• Elevadores,• Rede elétrica em geral.	Medidas Preventivas	
Ameaça	Resposta	Responsável
Curto-circuito - rompimento de cabo, própria manutenção, aquecimento de instalações elétricas, bus-way	Termografia dos quadros elétricos; Desligamento geral e Manutenção preventiva e corretivas.	CGERP
Vazamento de GLT - provoca explosão	Teste de estanqueidade; Proibição de colocar reservatório de gás no interior do prédio (restaurante) e Projetos de instalações com conformidade com normas ABNT.	CGERP/ CGSAT
Explosão em ativos ou subestação de gestão da concessionária	Acompanhamento junto a concessionária	CGERP
Risco de incêndio em reservatórios de diesel	profissional específico para monitoramento semanal	CGERP
Ação humana - proposital ou acidental	<ul style="list-style-type: none">• Treinamento da brigada,• campanhas de conscientização,• rondas periódicas da brigada de incêndio	CGSAT
Estocagem de material de fácil combustão - papel, por exemplo	Implementação de exaustores, ventilação mais adequada para reduzir a temperatura	CGERP
Incêndio nos arredores	Acionar o GDF para limpar a parte externa aos prédios	CGSAT

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Serviços de soldagem e outros equipamentos com emissão de calor	Deslocar extintor para o local onde está sendo feito a soldagem acompanhado da brigada de incêndio	CGSAT
Bateria estacionária	Monitoramento profissional	CGERP
Treinamentos		
Escopo	Público-alvo/alcance	Responsável
Plano de prevenção e combate a incêndio e abandono PPCIA - Administração predial	Colaboradores	CGSAT - Brigada
Projetos de prevenção combate a incêndio - manutenção predial	Colaboradores	CGERP - Engenharia

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

INCÊNDIO - Superintendência Regional de Administração						
Gestor	Superintendência Regional de Administração de cada estado					
Responsável	<ul style="list-style-type: none"> • Superintendência Regional de Administração de cada estado • Telefone: 61 2021-5055. 					
Contratos Relacionados	N/A					
Contatos úteis						
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação			
CBM (Tel)	Superintendência Regional de Administração de cada estado	<ul style="list-style-type: none"> • Telefone; • Ofício. 	Imediatamente após a confirmação do incêndio e início dos procedimentos de evacuação			
PM (Tel)						
Defesa Civil (Tel)						
Companhias de água e energia. (Tel)						
Consequências secundárias						
<ul style="list-style-type: none"> • Risco à vida, • Perda de imobiliário, • Perda de ativos em geral, • Perda de bens próprios, de terceiros, e inclusive contratados, • Elevadores, • Rede elétrica em geral. 						
Medidas Preventivas						
Ameaça	Resposta	Responsável				
Sobrecarga de quadros elétricos	<ul style="list-style-type: none"> • Acionamento da brigada de incêndio do edifício; • Evacuação do edifício; • Acionamento do CBM/MS; acionamento da concessionária de energia. 	Superintendência Regional de Administração de cada estado.				
Curto-circuito em instalações elétricas						
Vazamento de gás						
Defeito em algum equipamento elétrico						
Descargas atmosféricas						

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Incêndios externos		
incêndios externos		
Manuseio de fontes de calor		
Treinamentos		
Escopo	Público-alvo/alcance	Responsável
Treinamento de uso de extintores	Brigada voluntária	SRA
Simulação de evacuação	Todos os funcionários	
Curso de primeiros socorros	Equipe de manutenção	
Treinamento em segurança elétrica	Líderes de departamento	
Workshop de prevenção de incêndios	Todos os funcionários	
Teste dos sistemas de alarme e sprinklers	Equipe de manutenção	SRA
Treinamento em comunicação de emergência	Líderes de departamento	

Plano de Continuidade de Negócios
 Ministério da Gestão e Inovação em Serviços Públicos

Resposta

INCÊNDIO (DAL)			
Compartilha serviços			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	<ul style="list-style-type: none"> • Coordenação geral de Segurança, Administração, Terceirização e Transporte – CGSAT. • Coordenação Geral de Infraestrutura Predial- CGERP. • Telefone: 61 XXXXXX. 		
Contratos Relacionados	<ul style="list-style-type: none"> • Manutenção predial, • Contrato de segurança predial, • Contrato de Brigada de Incêndio, • Contrato de limpeza, • Contrato de CFTV. 		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Corpo de bombeiros- combate	CGSAT	Telefone	Imediato
Corpo de Bombeiros - perícia	CGSAT	Telefone	Automático junto com o chamado para o combate
Brigada de incêndio	CGSAT	Telefone	Imediato
Resposta a incidentes por cenários			
Cenário 1: Incêndio externo com fumaça em direção à edificação			
Responsável	Atribuição		
Equipe de segurança - CGSAT	<ul style="list-style-type: none"> • Fechar janelas e • Acionar Corpo de Bombeiros 		
Alternativas para a continuidade do negócio			
Responsável	Atribuição		
	Deslocamento da força de trabalho Home Office		

Plano de Continuidade de Negócios
 Ministério da Gestão e Inovação em Serviços Públicos

	Realizar reparos
Cenário 2: Foco de incêndio	
Responsável	Atribuição
Equipe de manutenção - CGERP	<ul style="list-style-type: none"> • Avaliar situação, • Reunir com líderes, • Orientar vigilantes e brigadistas
Equipe de segurança - CGSAT	<ul style="list-style-type: none"> • Desligar a energia • Combater com a brigada • Acionar corpo de bombeiros • Esvaziar o ambiente
Alternativas para a continuidade do negócio	
Responsável	Atribuição
	Deslocamento da força de trabalho Home Office
Cenário 3: Incêndio Generalizado	
Responsável	Atribuição
Equipe de manutenção - CGERP	Acionamento automático dos equipamentos de combate a incêndio
Equipe de segurança - CGSAT	evacuamento das instalações
CGSAT	Acionamento de corpo de bombeiros
CGERP	Desligar a energia nos quadros internos da edificação ou acionar a NEOENERGIA para desligar a edificação
Alternativas para a continuidade do negócio	
Responsável	Atribuição
	Deslocamento da força de trabalho para outra edificação até restaurar o prédio
	Home Office
	Manutenção

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

INCÊNDIO - Superintendência Regional de Administração			
Gestor	Superintendência Regional de Administração de cada estado		
Responsável	<ul style="list-style-type: none"> • Superintendência Regional de Administração de cada estado • Telefone: 61 2021-5055. 		
Contratos Relacionados	N/A		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
CBM (Tel)	Superintendência Regional de Administração de cada estado	Telefone; Ofício.	Imediatamente após a confirmação do incêndio e início dos procedimentos de evacuação
PM (Tel)			
Defesa Civil (Tel)			
Companhias de água e energia. (Tel)			
Resposta a incidentes por cenários			
Cenário 1: Incêndio externo			
Responsável	Atribuição		
Agente interno ou externo que identifique o incidente	Informar a um Servidor, portaria ou segurança do prédio, ou qualquer pessoa que se identifique com vínculo com o Ministério		
Equipe de segurança;	<ul style="list-style-type: none"> • Avaliar situação, • Reunir com líderes, • Orientar vigilantes e brigadistas 		
Equipe de manutenção e segurança	<ul style="list-style-type: none"> • Utilizar extintores, • Acionar alarme, • Evacuar área imediata 		
Alternativas para a continuidade do negócio			

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Responsável	Atribuição
Equipe de manutenção	<ul style="list-style-type: none"> • Realocar equipamentos e documentos, • Adaptar espaços não afetados
Cenário 2: Incêndio interno	
Responsável	Atribuição
<ul style="list-style-type: none"> • Equipe de segurança; • Qualquer pessoa que possa detectar visualmente o problema. 	<ul style="list-style-type: none"> • Detecção visual; • Comunicação inicial; • Orientação e • Evacuação dos locais afetados.
<ul style="list-style-type: none"> • Equipe de segurança e • Corpo de Bombeiros 	<ul style="list-style-type: none"> • Acionar Corpo de Bombeiros, • Evacuar prédio, • Isolar área afetada
Alternativas para a continuidade do negócio	
Responsável	Atribuição
Superintendência Regional de Administração de cada estado	<ul style="list-style-type: none"> • Estabelecer postos de trabalho temporários em áreas secas, • Iniciar trabalho remoto parcial
Cenário 3: Incêndio de Grandes Proporções	
Responsável	Atribuição
<ul style="list-style-type: none"> • Corpo de Bombeiros e • Defesa Civil 	<ul style="list-style-type: none"> • Evacuação total, • Combate ao incêndio, • Resgate, • Contenção de danos
Alternativas para a continuidade do negócio	
Responsável	Atribuição
Superintendência Regional de Administração de cada estado	<ul style="list-style-type: none"> • Estabelecer postos de trabalho temporários em áreas secas, • Iniciar trabalho remoto parcial

Avaliação do Incidente

AVALIANDO O INCIDENTE INCÊNDIO - Superintendência Regional de Administração					
	1	2	3	4	5
O incidente afeta a entrega de serviços públicos em que escala? 1 se não afeta; 5 se afeta para todos os usuários do serviço.					
O incidente interrompe as atividades de suporte? 1 se não interrompe; 5 se interrompe para todos os servidores do órgão					
Quantos órgãos são afetados pelo incidente? 1 = 1 órgão afetado; 2 = entre 2 e até 5 órgãos afetados; 3 = entre 5 e até 8 órgãos afetados; 4 = entre 9 e até 12 órgãos afetados; 5 = acima de 12 órgãos afetados;					
O incidente afeta a imagem/reputação da organização? 1 = não afeta; 5 = afeta.					
O incidente a compromete ou coloca em riscos ativos de informações (em meios digitais ou físicos)? Se sim, acionar ETIR e POSIC.					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião) Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação) Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).					

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Pós-Incidente

INCÊNDIO (DAL)	
Documentação do Incidente	Responsável
Relatório de incidente CGSAT/CGERP	CGSAT/CGERP
ATUALIZAÇÃO DA POLÍTICA, CONTRATOS E PROTOCOLO	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

INCÊNDIO (DCD)	
Documentação do Incidente	Responsável
Relatório detalhado do incidente	Superintendência Regional de Administração de cada estado e Equipe de Manutenção
Registro de acionamento do corpo de bombeiros	
Relatório de danos e perdas	
Registro de evacuação	
Relatório de investigação da causa do incêndio	
Plano de ação corretiva	
Registro de comunicações internas e externas	
Relatório de impacto nas operações	
ATUALIZAÇÃO DA POLÍTICA, CONTRATOS E PROTOCOLO	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável
Plano de Prevenção e Combate a Incêndio	SRA
Protocolo de Evacuação de Emergência	
Política de Segurança Elétrica	
Contrato com empresa de manutenção elétrica	
Plano de Continuidade de Negócios	
Política de Armazenamento de Materiais Inflamáveis	

Anexo 08 – Queda de energia

Mitigação

QUEDA DE ENERGIA (DAL)			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	<ul style="list-style-type: none">Coordenação geral de Segurança, Administração, Terceirização e Transporte – CGSAT.Coordenação Geral de Infraestrutura Predial- CGERP.Telefone: 61 XXXXXX.		
Contratos Relacionados	<ul style="list-style-type: none">Manutenção predial,Contrato de segurança predial,Contrato de Brigada de Incêndio,Contrato de limpeza,Contrato de CFTV,Contrato com Neoenergia.		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Neoenergia	CGERP	Telefone, e-mail ou ofício -a depender da urgência	N/A
MGI	Brigadista de plantão/Empresa de manutenção predial	ramal da brigada de cada prédio	N/A
Órgãos ColaboraGov	Representantes indicados de cada órgão	Telefone, e-mail ou ofício -a depender da urgência	N/A
Consequências secundárias			
Interrupção e/ou perda de trabalho; Descontinuidade dos sistemas de TI; Perda de bens próprios ou de terceiros (inclusive contratados) e Desconfiguração do sistema de refrigeração.			
Medidas Preventivas			
Ameaças	Resposta	Responsável	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Falta de manutenção preventiva	Manutenção preventiva (paradas programadas)	CGERP
Incêndio e Alagamento	Tratados na avaliação dos incidentes de alagamentos e incêndio	CGERP
Interrupção de serviço pela Neoenergia	Manter equipamentos de emergência	CGERP
Furto de cabo	<ul style="list-style-type: none"> • Manter equipamentos de emergência; • Interno e externo: rondas, • Monitoramento pelo sistema de CFTV; • Não deixar cabos expostos (proteger equipamentos); 	CGSAT/CGERP
Curto-circuito	Manutenção preventiva (paradas programadas)	CGERP
Ação humana - vandalismo, desligamento inadvertido	<ul style="list-style-type: none"> • Manter equipamentos de emergência; • Interno e externo: rondas, • monitoramento pelo sistema de CFTV; • Não deixar cabos expostos (proteger equipamentos); 	CGSAT/CGERP
Sobrecarga	<ul style="list-style-type: none"> • Conscientização, • Controle das demandas por novos pontos 	CGERP
Utilização indevida de sistema- tomadas T, extensão	<ul style="list-style-type: none"> • Avaliação de prédios, • Campanhas educativas 	CGERP
Intermitência/Variação no fornecimento - qualidade da energia	<ul style="list-style-type: none"> • Aquisição de equipamentos bi-volt; • Equipamentos de segurança nos quadros 	CGERP
Não sustentação dos serviços TI	Mapear o que geradores e nobreaks cobrem em cada bloco	DTI/DAL
Treinamentos		
Escopo	Público-alvo/alcance	Responsável
Teste de desligamento de energia e dos sistemas nobreak e grupo Moto-Gerador	Equipamento do sistema elétrico	CGSAT - Brigada

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

QUEDA DE ENERGIA (DCD)			
Gestor	Superintendência Regional de Administração de cada estado		
Responsável	Superintendência Regional de Administração de cada estado.		
Contratos Relacionados	<ul style="list-style-type: none"> • Manutenção predial; • Brigada de incêndio; • Segurança predial; • Contratos de limpeza; • Administrativo. 		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
MGI-SRA	Indicados de cada órgão	Telefone/ofício	Imediato
Companhia de energia de cada estado.	Central de atendimento	Telefone/ofício.	Imediato
Consequências secundárias			
<ul style="list-style-type: none"> • Interrupção de serviços eletrônicos; • Perda de dados não salvos; • Falha nos sistemas de segurança; • Impacto na produtividade; • Possível dano a equipamentos sensíveis. 			
Medidas Preventivas			
Ameaça	Resposta	Responsável	
Problemas na rede de alimentação externa; intempéries; problemas em equipamentos elétricos; circuitos elétricos mal dimensionados; sobrecarga do sistema elétrico.	Manutenção preventiva e corretiva das instalações elétricas. Ativação de geradores de emergência. Desligamento ordenado de equipamentos não essenciais. Comunicação com a concessionária de energia.	Superintendência Regional de Administração de cada estado	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Treinamentos		
Escopo	Público-alvo/alcance	Responsável
Treinamento em operação de geradores de emergência	Equipe de manutenção	Teste de sistemas de backup de energia
Simulação de falha de energia	Todos os funcionários	Teste de sistemas de backup de energia
Curso de segurança em instalações elétricas	Equipe de manutenção	Teste de sistemas de backup de energia
Workshop de economia de energia	Todos os funcionários	Teste de sistemas de backup de energia
Treinamento em procedimentos de desligamento seguro	Equipe de TI	Teste de sistemas de backup de energia
Exercício de continuidade de negócios	Equipe de Gestão	Teste de sistemas de backup de energia

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Resposta

QUEDA DE ENERGIA (DAL)			
Gestor	Diretoria de Administração e Logística - DAL		
Responsável	<ul style="list-style-type: none"> Coordenação geral de Segurança, Administração, Terceirização e Transporte – CGSAT. Coordenação Geral de Infraestrutura Predial- CGERP. Telefone: 61 XXXXXX. 		
Contratos Relacionados	<ul style="list-style-type: none"> Manutenção predial, Contrato de segurança predial, Contrato de Brigada de Incêndio, Contrato de limpeza, Contrato de CFTV, Contrato com Neoenergia. 		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
Neoenergia	CGERP	Telefone, e-mail ou ofício – a depender da urgência	N/A
MGI	Brigadista de plantão/Empresa de manutenção predial	Ramal da brigada de cada prédio	N/A
Órgãos ColaboraGov	Representantes indicados de cada órgão	Telefone, e-mail ou ofício – a depender da urgência	N/A
Resposta a incidentes por cenários			
Cenário 1: Interrupção de fornecimento da Neoenergia e gerador não funcionar			
Responsável	Atribuição		
Equipe de manutenção - CGERP	<ul style="list-style-type: none"> Verificar a causa e Tomar as providências. 		
Alternativas para a continuidade do negócio			
Responsável	Atribuição		

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

Autoridade do órgão	Trabalho em home office se o grupo gerador não funcionar
CGERP - equipe de engenharia	Acionamento manual do grupo Gerador
CGERP - equipe de engenharia	Acionamento manual do grupo Gerador
Cenário 2: Nobreak não funcionou ou não segurou o fornecimento de energia até os geradores entrarem	
Responsável	Atribuição
CGERP - equipe de engenharia	Verificar a causa e tomar as providências - manutenção corretiva pós incidentes
Alternativas para a continuidade do negócio	
Responsável	Atribuição
CGERP - equipe de engenharia	Acionamento manual do grupo Gerador
CGERP	Acionar a equipe de manutenção
Cenário 3: Furto de cabos	
Responsável	Atribuição
Equipe de manutenção - CGERP	Substituir os cabos furtados
CGSAT	<ul style="list-style-type: none"> Apurar os fatos com: Brigadas de incêndio, Equipes de segurança, Usando sistema de CFTV
CGERP	Acionar Polícia
Alternativas para a continuidade do negócio	
Responsável	Atribuição
CGERP	Acionar a equipe de manutenção

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

QUEDA DE ENERGIA (DCD)			
Gestor	Superintendência Regional de Administração de cada estado		
Responsável	Superintendência Regional de Administração de cada estado.		
Contratos Relacionados	<ul style="list-style-type: none"> • Manutenção predial; • Brigada de incêndio; • Segurança predial; • Contratos de limpeza; administrativo. 		
Contatos úteis			
Órgão	Unidade responsável pelo contato	Forma de Comunicação	Tempo limite para comunicação
MGI-SRA	Indicados de cada órgão	Telefone/ofício	Imediato
Companhia de energia de cada estado.	Central de atendimento	Telefone/ofício.	Imediato
Resposta a incidentes por cenários			
Cenário 1: Danificação na rede externa			
Responsável		Atribuição	
<ul style="list-style-type: none"> • Equipe de segurança; • Qualquer pessoa que possa detectar visualmente o problema. 		<ul style="list-style-type: none"> • Detecção visual e • Comunicação inicial. 	
Equipe de Manutenção		<ul style="list-style-type: none"> • Identificar fonte, • Drenar água, • Secar áreas afetadas 	
Alternativas para a continuidade do negócio quando a queda é breve			
Responsável		Atribuição	
Equipe de TI		Manter sistemas críticos com energia de backup, preparar para retomada rápida	
Cenário 2: rede interna geral			
Responsável		Atribuição	
<ul style="list-style-type: none"> • Equipe de segurança; 		<ul style="list-style-type: none"> • Detecção Visual E • Comunicação Inicial. 	

Plano de Continuidade de Negócios

Ministério da Gestão e Inovação em Serviços Públicos

<ul style="list-style-type: none"> Qualquer pessoa que possa detectar visualmente o problema. 	
Equipe de Manutenção e Defesa Civil	<ul style="list-style-type: none"> Comunicar Secretaria Executiva e • Chefe de Gabinete da(o)Ministra(o)
Alternativas para a continuidade do negócio (queda prolongada até 4 horas)	
Responsável	Atribuição
Superintendência Regional de Administração de cada estado	<ul style="list-style-type: none"> Ativar plano de trabalho remoto, e Redirecionar serviços essenciais para unidades com energia
Cenário 3: rede interna geral	
Responsável	Atribuição
<ul style="list-style-type: none"> Equipe de segurança; Qualquer pessoa que possa detectar visualmente o problema. 	<ul style="list-style-type: none"> Detecção visual; e Comunicação inicial.
<ul style="list-style-type: none"> Equipe de Manutenção e Defesa Civil 	<ul style="list-style-type: none"> Implementar plano de continuidade; Considerar dispensa de funcionários; e Proteger ativos críticos.
Alternativas para a continuidade do negócio queda extensa, acima de 4 horas	
Responsável	Atribuição
Superintendência Regional de Administração de cada estado	<ul style="list-style-type: none"> Implementar plano de continuidade de longo prazo; Considerar realocação temporária de operações; e Alocar pessoal trabalho remoto.

Avaliação do Incidente

AVALIANDO O INCIDENTE					
	1	2	3	4	5
O incidente afeta a entrega de serviços públicos em que escala? 1 se não afeta; 5 se afeta para todos os usuários do serviço.					
O incidente interrompe as atividades de suporte? 1 se não interrompe; 5 se interrompe para todos os servidores do órgão					
Quantos órgãos são afetados pelo incidente? 1 = 1 órgão afetado; 2 = entre 2 e até 5 órgãos afetados; 3 = entre 5 e até 8 órgãos afetados; 4 = entre 9 e até 12 órgãos afetados; 5 = acima de 12 órgãos afetados;					
O incidente afeta a imagem/reputação da organização? 1 = não afeta; 5 = afeta.					
O incidente a compromete ou coloca em riscos ativos de informações (em meios digitais ou físicos)? Se sim, acionar ETIR e POSIC.					
PONTUAÇÃO:					
Moderado: até 4 pontos (não é necessário convocar reunião)					
Sério: de 5 a 7 pontos (diretor decide a conveniência da convocação)					
Muito grave: acima de 7 pontos (nesses casos a reunião do Comitê deve ser convocada imediatamente).					

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

Pós-Incidente

QUEDA DE ENERGIA (DAL)	
Documentação do Incidente	Responsável
Relatório de incidente CGSAT/CGERP	CGSAT/CGERP
ATUALIZAÇÃO DA POLÍTICA, CONTRATOS E PROTOCOLO	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável
Revisar o mapeamento de serviços cobertos pelo Geradores	CGERP/DTI

Plano de Continuidade de Negócios
Ministério da Gestão e Inovação em Serviços Públicos

QUEDA DE ENERGIA (DCD)	
Documentação do Incidente	Responsável
Relatório detalhado do incidente	<ul style="list-style-type: none"> • Superintendência Regional de Administração de cada estado; e • Equipe de Manutenção
Registro de comunicação com a concessionária de energia	
Relatório técnico da causa da queda de energia	
Registro de ativação de sistemas de backup	
Relatório de impacto nas operações e sistemas	
Plano de ação para prevenção de incidentes futuros	
Registro de tempo de inatividade e custos associados	
Avaliação da eficácia do plano de contingência	
ATUALIZAÇÃO DA POLÍTICA, CONTRATOS E PROTOCOLO	
Documentos a atualizar, aprimorar ou criar no pós-incidente	Responsável
Plano de Contingência para Falhas de Energia	SRA
Política de Uso de Geradores de Emergência	
Contrato com a concessionária de energia	
Protocolo de Desligamento Seguro de Equipamentos	
Plano de Manutenção Preventiva de Equipamentos Elétricos	

Anexo 09 – Ocupação de prédio público

Informação Sensível

Risco à Segurança Predial

Acesso restrito a agentes
do MGI