 <b>CPFL</b> <b>ENERGIA</b> Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

## Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO.....	1
3.	DEFINIÇÕES.....	2
4.	DOCUMENTOS DE REFERÊNCIA .....	4
5.	RESPONSABILIDADES .....	4
6.	REGRAS BÁSICAS .....	5
7.	CONTROLE DE REGISTROS.....	5
8.	ANEXOS .....	15
9.	REGISTRO DE ALTERAÇÕES .....	18

### 1. OBJETIVO

Este documento tem como objetivo estabelecer um Plano de Resposta a Incidentes para os sistemas críticos de TI, estabelecendo os procedimentos que deverão ser seguidos de modo a reduzir a descontinuidade operacional derivada de indisponibilidade dos sistemas críticos responsáveis da Operação e Clientes a saber:

**Sistemas Técnicos:** ADMS | CWSI | OFS | PO Técnico | CCS

**Canais Atendimento (Digitais e CallCenter):** Call Center (URA, Telefonia e CCS) WhatsApp, Portal Web, Site, chat, SMS e CCS.

A situação de indisponibilidade de sistemas é objeto do presente documento, devido a sua relevância para garantir a continuidade do controle e operação do ambiente sistêmico de distribuição e transmissão de energia, bem como devido a importância de impacto para a Companhia.

Caso aconteça uma interrupção dos sistemas, representando ser uma preocupação relevante, principalmente à medida que cresce a dependência dos processos em relação à tecnologia e seus canais digitais.


Estabelecer critérios de disparo de ações de mitigação de uma crise diferenciando questões climáticas e funcionais a luz da interação do cliente.

### 2. ÂMBITO DE APLICAÇÃO

#### 2.1. Empresa

Todas as empresas do Grupo CPFL.

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 1 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

## 2.2. Área

Todas as áreas do Grupo CPFL.

## 3. DEFINIÇÕES

### 3.1. Contingência

Situação de crise decorrente de evento ou desastre que leve a indisponibilidade dos sistemas classificados como críticos para a continuidade dos serviços prestados aos nossos clientes, através dos sistemas: Sistemas Técnicos: ADMS | CWSI | OFS | PO Técnico | CCS e Canais Atendimento (Digitais e CallCenter): Call Center (URA, Telefonia e CCS) WhatsApp, Portal Web, Site, chat, SMS e CCS.

### 3.2. Executivo da área de crise

Gestor Sênior responsável pelo suporte do ambiente de que está ocorrendo o incidente, responsável pela área de negócio afetada pela situação de crise.

### 3.3. Governança de crise

Diretrizes de acionamento do grupo de crise para tomada de decisão e implementação de ações estratégicas e operacionais descritos neste documento.

### 3.4. Grupo de Crise

Time responsável pela análise inicial da situação de crise e classificação entre os níveis I, II ou III, e que atua como facilitador de ações estratégicas e operacionais para resolução da crise.

### 3.5. Líder da crise

Gestor da crise (sob a ótica operacional e de reputação), representado pelo Gerente de TI ou seu suplente devidamente delegado, responsável pela gestão do grupo de crise e dos times envolvidos.


### 3.6. Plano de Resposta a Incidente

Procedimento documentado que orienta a Companhia a responder, recuperar, retomar e restaurar, após a interrupção, para um nível predefinido de operação. Isto abrange recursos, serviços e atividades necessárias para assegurar a continuidade de funções críticas de negócios.

### 3.7. Sistema Mobilidade

Sistema de gerenciamento de serviços de campo, tendo como principais funções, gerenciamento da fila das atividades a serem executadas, agendamento e despacho de

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 2 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

serviços, e integrando as atividades executadas aos sistemas de inventário, cobrança e outros sistemas de origem.

### 3.8. Sala de Crise

Espaço reservado para concentração das pessoas e atividades voltadas estritamente para as contingências dos impactos causados pela crise.

**3.9 CIRT:** Computer Incident Response Team (CIRT) é o time que atua na preparação, identificação, contenção, erradicação e documentação do incidente do ambiente sendo a equipe participante de todas as fases de gestão de um incidente do ambiente.

**3.10 Controles:** Controles de Tecnologia da Informação voltados para evitar mudanças em ambientes produtivos sem as devidas autorizações.

**3.11 Notificações:** Refere-se às leis que se aplicam a uma entidade que exige quando ocorre quebras de solicitações de agências reguladoras.

**3.12 Impacto:** Consequências que podem ocorrer caso o risco se manifeste.

**3.13 Incidente de maior impacto:** É estabelecido com base na classificação de severidade na criticidade do incidente.


**3.14 Sistema ADMS:** O sistema ADMS utiliza informações em tempo real sobre a rede elétrica (SCADA), incluindo informações sobre a topologia da rede (GIS), fluxo de energia, tensão e carga, para isolar a seção da rede afetada pela falha. Em seguida, o sistema realiza uma série de manobras automáticas para restaurar a energia elétrica aos consumidores afetados, minimizando o número de clientes sem energia elétrica.

**3.15 Call Center:** Um call center é um termo em inglês que significa central de chamada. É um departamento responsável por fazer ou receber ligações de clientes. O call center é considerado uma central de atendimento que é responsável por criar uma relação entre a empresa e o cliente.

**3.16 Agências Virtuais:** Ferramenta que utiliza a Internet como meio de comunicação para demandas do setor regulado de produtos e serviços.

**3.17 OFS:** Oracle Field Service é uma solução de gerenciamento de serviços de campo baseada em nuvem que ajuda as empresas a agendar, encaminhar e equipar os trabalhadores móveis para concluir atividades de serviço.

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 3 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

**3.18 CCS:** O SAP Customer Care Services, é a solução da SAP que visa atender aos serviços públicos, tais como fornecimento de energia.

**3.19 SAP PO:** SAP PO (Process Orchestration) é uma ferramenta para automação e otimização de processos de negócios.

**3.20 Chatboot:** Programa de computador que simula e processa conversas humanas (escritas ou faladas), permitindo que as pessoas interajam com dispositivos digitais como se estivessem se comunicando com uma pessoa real.

#### 4. DOCUMENTOS DE REFERÊNCIA

- Gestão de Crise (Publicado GED 17922).
- Plano de Resposta a Incidentes de Segurança da Informação (Publicado GED 18851).
- Plano de Resposta a Incidentes de Segurança da Informação rede OT (Publicado GED 19521).
- Política de Segurança Cibernética do Grupo CPFL (Publicado GED 19368);
- ISO/IEC 27001;
- NIST Computer Security Incident Handling Guide;
- International Standard ISO/IEC27035-1;
- NIST SP-82;
- RO-CB.BR.01;
- IEC 61850;
- NIST 800-61r2.

#### 5. RESPONSABILIDADES

##### 5.1. Analistas/Especialistas/Coordenadores:

- Assim que acionados, deslocar-se imediatamente para o local de trabalho ou acessar a sala de crise imediatamente;


##### 5.2. Executivo da Área de Crise:

- Diretor de TI, deverá ser notificado das ações que estão sendo executadas;
- Responsável por notificar os executivos do Grupo CPFL sobre as ações realizadas;
- Receber e tomar decisões sustentadas pelo Líder da Crise;

##### 5.3. Líder da Crise:

- Nomear o Secretário da Crise que irá organizar os horários de ações;

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 4 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

- Facilitador na investigação e solução de incidentes críticos.
- Líder da Crise será o ponto de contato com a área de negócio.
- Responsável por reunir recursos, conforme necessário, para resolver um incidente crítico.
- Aprovar os comunicados, quando necessário, relacionados a impacto e status de incidentes críticos.
- Gerenciar salas de crise, para que os recursos sejam utilizados da melhor maneira possível para a rápida solução do incidente.
- Receber os status dos acontecimentos e ações significativas que ocorreram durante sala de crise.
- Deverá auxiliar na revisão do presente plano de resposta a incidente, após o término da situação de crise.
- Tomar decisões de possíveis alterações no ambiente sustentadas pelo time técnico.

#### 5.4. Secretário da Crise:

- Deverá auxiliar na revisão do presente plano de resposta a incidente, após o término da situação de crise.
- O Secretário deverá elaborar reporte periódico conforme item 6.3.3 deste documento sobre a situação de crise, auxiliando o executivo da área de crise na comunicação com o grupo de crise.
- Deverá realizar o acompanhamento das lições aprendidas e acompanhar as ações encontradas e que ficaram pendentes.
- Preparar e enviar comunicados, quando necessário, relacionados a impacto e status de incidentes críticos.
- Documenta os acontecimentos e ações significativas que ocorreram durante sala de crise.

## 6. REGRAS BÁSICAS


### 6.1. Equipe de Crise

A relação dos contatos que serão relevantes na implementação das ações descritas nesse documento está listada na tabela contida no anexo, item “7.1 – Equipe de Crise”.

Outros contatos pertinentes à situação de crise podem ser encontrados nos Planos de Resposta a Incidente de Tecnologia da Informação.

As funções críticas que irão atuar na situação de crise estarão inclusas no sistema de acordo com a situação de crise.

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 5 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

 CPFL ENERGIA Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

## 6.2. Premissas para Aplicação do Plano

As estratégias e planos de ação elencados nesse documento têm o objetivo de garantir a continuidade dos serviços operações de campo e relacionamento com cliente.

As ações adotadas devem ser constantemente monitoradas e terão duração até o retorno à situação normal de funcionamento.

O Líder da Crise ou suplente indicado pelo mesmo, será o executivo da área de crise, conforme governança de crise, e terá as seguintes atribuições de caráter não exaustivo durante a crise:

- Liderança sobre a situação de crise;
- Comunicação corporativas necessárias durante a crise;
- Atuar na execução do Plano de Resposta a Incidente;
- Reunir e manter contato com as fontes diretas de informação sobre a crise;
- Agregar conhecimento técnico para minimizar os impactos da situação e ajudar a estabelecer a comunicação correta sobre os fatos da crise.


No pós-crise, deverá realizar testes periódicos de efetividade dos Planos de Resposta a Incidente vigentes, bem como avaliar a necessidade de implementação de medidas de correção.

A análise de causa-raiz é a atividade do processo de tratamento pós-incidente, onde é necessário identificar os reais motivos da causa do incidente de tecnologia da informação ocorrido.

Em geral, os principais motivos de causa-raiz de um incidente de segurança são:

- Falha humana: O ser humano é inerente ao erro. Em um processo em que foram tomadas todas as medidas de segurança e adoção de controles tecnológicos, o fator humano faz parte de uma ação de risco. O erro e falha provocados por um ser humano devem ser considerados;
- Falha de software: Erros de aplicação no sistema crítico, indisponibilidade causadas por atualizações mal implementadas podem ser a causa-raiz de incidentes de tecnologia da informação;
- Falha de plataforma: Erros na plataforma que gerencia o sistema crítico ou lentidão que causaria aumento da fila de chamados e demandas.
- Problemas de capacity: falta de recurso que supra as necessidades do acionamento e chamados;
- Falha de hardware: assim como a falha de software, problemas advindos da ausência de atualizações de firmware ou mesmo falhas oriundas de superaquecimento e erros de projetos também podem ser causa-raiz de incidentes de tecnologia da informação;

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 6 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

- Falha de processo: controles apropriados devem ser aplicados em todas as partes vulneráveis de um determinado processo. Um processo mal desenhado pode ser a causa-raiz de um incidente de tecnologia da informação;

OBS: Imediatamente após a identificação e validação da causa-raiz, os riscos e controles pertinentes devem ser inseridos no Sistema de Gestão de Problemas da Tecnologia da Informação do Grupo CPFL, quando aplicável.

Estão identificadas quatro pré-condições para o funcionamento adequado do presente plano de resposta a incidente, condições essas que também são pré-requisitos para a operação do negócio dos Sistemas Técnicos: ADMS | CWSI | OFS | PO Técnico | CCS e Canais Atendimento (Digitais e CallCenter).

- Infraestrutura
- Sistemas
- Processos
- Pessoas

A **infraestrutura** e **sistemas** englobam todas as facilidades utilizadas para realização dos processos de negócio de Tecnologia da Informação: Falha de Sistemas, Indisponibilidade de Sistemas Críticos, Mudanças mal executadas, energia, networking, telecomunicações, informática e sistemas internos. Para cada um dos itens que compõem a infraestrutura e sistema existe uma ação a ser tomada.

Os **processos** são as atividades realizadas para operar os Sistemas Técnicos: ADMS | CWSI | OFS | PO Técnico | CCS.

Canais Atendimento (Digitais e Call Center). As **pessoas** são os colaboradores da TI responsáveis por executar os processos, bem como colaboradores que atuarão como facilitadores ou apoiadores na implementação de ações.

### 6.3. Procedimentos


#### 6.3.1. Caracterização da Contingência

Uma situação de crise é caracterizada pela indisponibilidade de pelo menos um dos sistemas críticos listados nesse Plano de Resposta a Incidentes, decorrente dos eventos listados abaixo, de caráter não exaustivo:

- Ataque cibernético;
- Indisponibilidade dos Sistemas Técnicos: ADMS | CWSI | OFS | PO Técnico | CCS. Canais Atendimento (Digitais e CallCenter)
- Falha dos Sistemas Técnicos: ADMS | CWSI | OFS | PO Técnico | CCS. Canais Atendimento (Digitais e CallCenter)
- Queda dos links de comunicação entre sistemas e usuários;

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 7 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

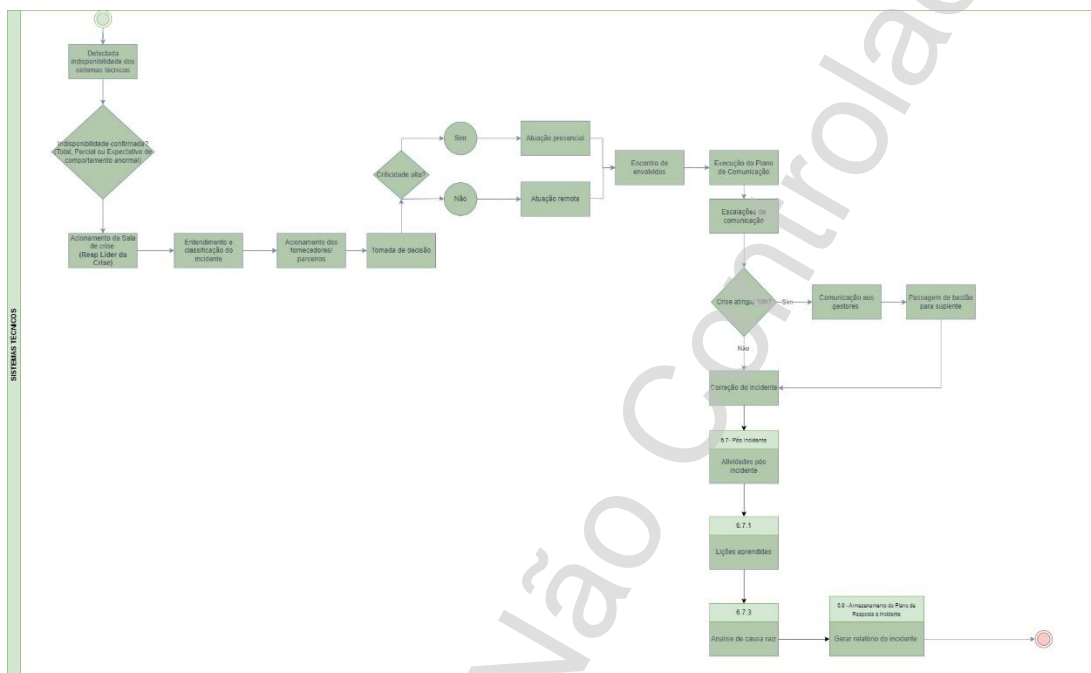


 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

- Volumetria que o capacity não suporta;

Deve-se seguir os procedimentos a seguir:

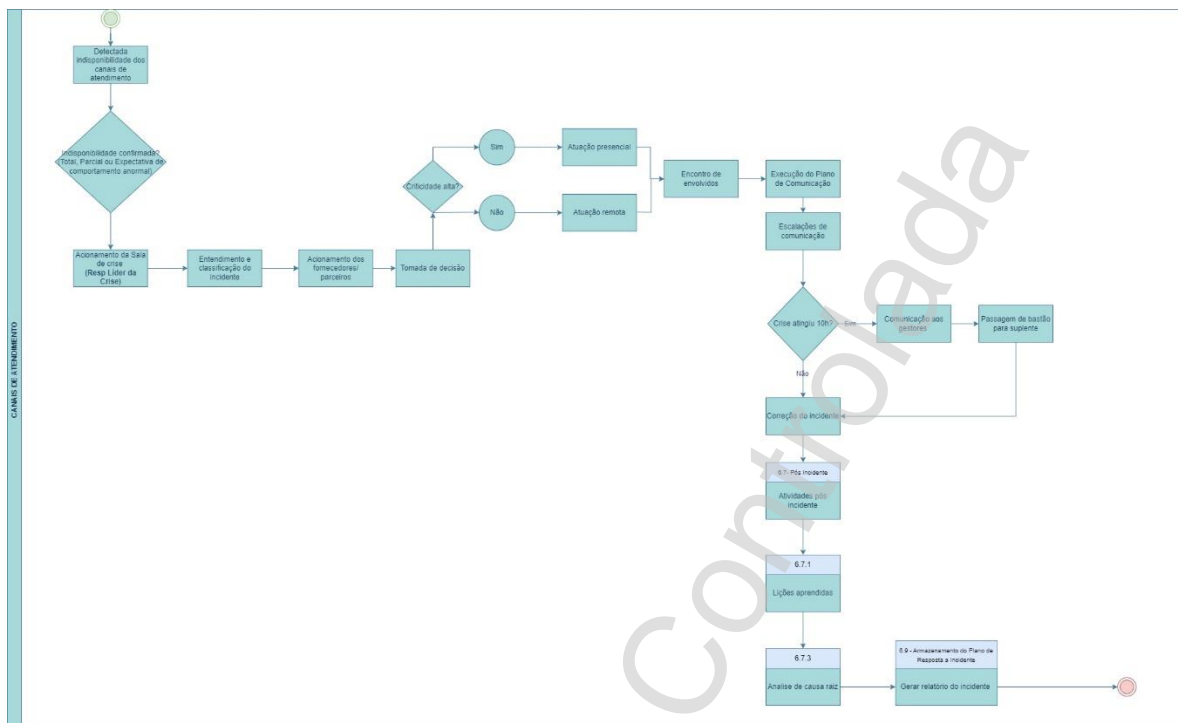
**Sistemas Técnicos: ADMS | CWSI | OFS | PO Técnico | CCS:**



**Canais Atendimento (Digitais e CallCenter):**

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 8 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------






### 6.3.2. Criticidade de um incidente

A classificação de criticidade de cada incidente é baseada na avaliação de impacto, regras de negócio, e dos ativos envolvidos, conforme importância para o negócio, a depender da criticidade do incidente deve ser acionado e disparado uma sala de crise (Warroom):

#### 6.3.2.1 Sistemas Técnicos:

Criticidade	Descrição
<b>Alta</b>	- Indisponibilidade parcial ou total do sistema; - Consumidores Interrompidos (CI) >200 mil clientes.
<b>Média</b>	- Indisponibilidade parcial do sistema; - Consumidores Interrompidos (CI) >99mil e <200 mil clientes.
<b>Baixa</b>	- Indisponibilidade parcial   lentidão do sistema; - Consumidores Interrompidos (CI) >80mil e até 99 mil clientes.

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 9 de 18
----------------------------	------------------------------	------------------------	--	---	----------------------------------

 <b>CPFL</b> <b>ENERGIA</b> Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

### 6.3.2.2 Canais de Atendimento:

Criticidade	Descrição
<b>Alta</b>	<ul style="list-style-type: none"> <li>- Número de clientes na fila de atendimento superior a 200;</li> <li>- Lentidão ou Indisponibilidade sistêmicas em qualquer uns dos canais de atendimento.</li> <li>- Consumidores Interrompidos (CI) &gt;200 mil clientes.</li> </ul>
<b>Média</b>	<ul style="list-style-type: none"> <li>- Número de clientes na fila de atendimento superior a 150;</li> <li>- Lentidão ou Indisponibilidade sistêmicas em qualquer uns dos canais de atendimento.</li> <li>- Consumidores Interrompidos (CI) &gt;99mil e &lt;200 mil clientes</li> </ul>
<b>Baixa</b>	<ul style="list-style-type: none"> <li>- Número de clientes em fila de atendimento superior a 50</li> <li>- Lentidão nos sistemas de qualquer canal de atendimento.</li> <li>- Indisponibilidade que impactem menos de 99 mil clientes.</li> </ul>

### 6.3.3 Plano de comunicação:


Criticidade	Plano de Comunicação
<b>Alta</b>	Resumo a cada 30 minutos às partes envolvidas na fase crítica e a cada hora durante a fase de resolução.
<b>Média</b>	Resumo a cada hora às partes envolvidas na fase crítica e a cada turno na fase de resolução.
<b>Baixa</b>	Resumo diário às partes envolvidas.

Se houver a indisponibilidade dos sistemas críticos de criticidade Alta (conforme métricas acima) deverá ser iniciadas o acionamento da Sala de Crise, envolver os contatos que estão no item 7.1 Equipe de Crise, deste documento e tratar a Sala de Crise como Confidencial, todos os participantes da sala de crise deverá assinar o termo de confidencialidade (Anexo II 7.2 – Termo de confidencialidade).

### 6.3.3. Implementação de Ações

As ações listadas abaixo são de caráter não exaustivo e representam um guia de possibilidades para tratamento da presente situação de crise, podendo ser combinadas com outras ações pertinentes. E as tratativas manuais pelos operadores trazidas abaixo:

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 10 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

**6.3.3.1.** Usar modelo de Excel para registrar os dados presentes no sistema como: (i) tipo de ocorrência, (ii) local, (iii) horário e (iv) demais informações necessárias para posterior regularização do indicador, devendo permanecer salvo nos desktops.

**6.3.3.2.** Notificar todas as equipes de campo que estão em serviço sobre a indisponibilidade do sistema ADMS Sistema de Mobilidade, através de contato direto entre operadores do Centro de Operação e o time de serviço de campo, via telefonia móvel ou qualquer meio de comunicação disponível no momento.

**6.3.3.3.** Formalizar todas as ações tomadas, visando demonstrar ao órgão regulador a preocupação em entregar o serviço contratado e, também, para destacar lições aprendidas.

#### **6.4. Indisponibilidade do Sistema ADMS**

##### **6.4.1. Indisponibilidade do sistema ADMS**

O sistema ADMS caracteriza-se pelo registro de operações, possibilitando o acompanhamento online das linhas secundárias, servindo de suporte para os despachos de equipes para trabalhos de campo, inclusive com monitoramento das próximas demandas, com organização automática por ordem de urgência.


Tais sistemas estão contemplados na estrutura coordenada pela Diretoria de Tecnologia da Informação – EI, onde o DR irá suportar as atividades do DC, com replicação automática dos sistemas e seus dados, sem prejuízo para a continuidade das atividades dos usuários, até que seja reestabelecida a infraestrutura do DC. Esta representa, portanto, a primeira contingência do sistema. Seu acionamento é automático e é de responsabilidade da Diretoria de Tecnologia da Informação – EI.

A ação de contorno à indisponibilidade dos sistemas DMS e ADMS é através do Sistema de Contingência - DR, que opera online, sendo necessário somente o funcionamento da rede. Após orientação do Coordenador, as seguintes ações devem ser tomadas pelos operadores:

**6.4.1.1.** Utilizar o Sistema de Contingência através do link: <http://portalti/contingencia/>, o qual passa a carregar automaticamente as entradas de ocorrência recebidas pelo Call Center.

**6.4.1.2.** Informar a equipe de Campo que está em operação sobre a indisponibilidade dos sistema ADMS, através de contato direto entre operadores do Centro de Operação e o líder de serviço de campo, via telefonia móvel.

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 11 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

**6.4.1.3.** Registrar na planilha “modelo” em Excel todas as informações fornecidas pelo serviço de campo.

**6.4.1.4.** Lançar manualmente no ADMS, os dados das ocorrências registrados na planilha “modelo” do Excel para compor o indicador.

**6.4.1.5.** Formalizar todas as ações tomadas, visando demonstrar ao órgão regulador a preocupação em entregar o serviço contratado e também para destacar lições aprendidas.

#### **6.4.2. Indisponibilidade Canais de Atendimento**

Se houver indisponibilidade da rede, Canais Atendimento (Digitais e CallCenter) todo o tratamento será manual. Após orientação do Coordenador, as seguintes ações devem ser tomadas pelos operadores:

**6.4.2.1.** Utilizar a planilha “modelo” de Excel, desenvolvida pela área previamente à ocorrência da situação de crise, contendo dados presentes no sistema, como (i) tipo de ocorrência, (ii) local, (iii) horário e (iv) demais informações necessárias para posterior regularização do indicador, devendo esta permanecer salva nos desktops dos Centro de Operações, para utilização em caso de indisponibilidade dos sistemas.

**6.4.2.2.** Entrar em contato com os pontos focais do Call Center nos celulares disponíveis da área ou celulares corporativos dos líderes.

Recomendações:


(i) Manter atualizado o contato dos pontos focais do Call Center nos celulares da área, como da gerente da CPFL Atende.

(ii) Manter os celulares corporativos presentes na área, pois representarão uma alternativa para comunicação, caso a comunicação telefônica esteja indisponível por operarem via IP (dependência de rede).

(iii) Disponibilização de dois celulares backup carregados e habilitados para comunicação entre a Operação e o Call Center, em tempo integral na área.

**6.4.2.3.** Promover interação, por telefonia móvel, entre Call Center e Centro de Operações para alimentar planilhas com os dados das chamadas recebidas.

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 12 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

**6.4.2.4.** Informar equipe de campo sobre a indisponibilidade dos sistema ADMS, deve ser via centro de operações.

**6.4.2.5.** Formalizar todas as ações tomadas, visando demonstrar ao órgão regulador a preocupação em entregar o serviço contratado e também para destacar lições aprendidas.

## 6.5. Comunicação

**6.5.1.** Elaborar, levar para aprovação do líder da crise e divulgar, comunicado sobre a situação de crise, impactos para a companhia e principais ações endereçadas com o objetivo de dar transparência e tranquilizar os colaboradores através dos canais internos oficiais.

A responsabilidade de disparo das ações de alteração do ambiente no que tange regras de negócio, deve ser solicitada pelas áreas de negócios.

## 6.6. Procedimentos Gerais

Por outras razões não previstas no presente Plano de Resposta da Incidente e que afetem a disponibilização de sistemas, como contingências no sistema elétrico, intervenções programadas/emergenciais, eventos sociais, situações com alto risco de impacto midiático poderá ser solicitado, em caráter excepcional, o acionamento desse plano e a mobilização imediata para essas situações mesmo que não claramente definidas neste documento, desde que tenha a análise a autorização do **líder da crise**.

**Caso necessário ser realizado alguma alteração no ambiente, o líder da crise tem autonomia para autorizar a alteração e controlar a abertura da RDM antes da passagem de turno para a próxima equipe.**


Caso de passagem de turno, o líder da crise deve preencher a planilha Anexo V, antes da passagem de bastão para a equipe que irá te substituir.

## 6.7. Pós Crise

Todos os danos causados pela situação de crise e as ações endereçadas para garantir a continuidade da operação deverão ser monitoradas e registradas pelo Secretário do Executivo da Área de Crise, presente na sala de crise durante todo o evento, o que irá fornecer subsídios para avaliar a evolução da situação.

Após decreto de término da situação de crise, ações deverão ser endereçadas para retorno da normalidade da operação, assim como avaliação de demandas e ordem de serviços represadas e estimativa do tempo para finalização das mesmas, impactos na diretoria comercial - RC, impactos no atendimento ao cliente e comunicação com órgãos reguladores e público em geral, visando reduzir impactos à imagem da companhia e manter um bom relacionamento com os stakeholders.

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 13 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------

 CPFL ENERGIA Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

**6.7.1.** Realizar o dimensionamento de serviços represados pela situação de crise, com o objetivo de restabelecer o padrão normal de atendimento e atividades internas e as lições aprendidas.

**6.7.2.** Revisar o presente Plano de Resposta a Incidentes de acordo com a situação vivenciada, atualizando a relação de ações estratégicas e responsáveis, se necessário.

**6.7.3.** Os incidentes devem possuir um relatório que contém a análise da causa raiz.

## 6.8. Simulações de Contingência

**6.8.1.** A cada 12 meses deverá ser realizada simulação de execução do Plano de Resposta a Incidente. Não há necessidade de ser simultânea nem envolver a totalidade dos colaboradores ao mesmo tempo, porém deve-se fazer o registro dos participantes de modo que, ao longo do tempo, todos participem para reciclar o conhecimento do plano.

**6.8.2.** Após simulação, o presente plano de resposta a incidente deverá ser revisitado e, em caso de necessidade, melhorias e aprimoramentos.


## 6.9. Armazenamento do Plano de Resposta a Incidentes

O presente plano deverá ser de conhecimento de todos os participantes da área de TI, os gestores citados neste documento, e **deve ter cópias atualizadas e armazenadas no Teams e E-mail de cada participante.**

## 7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 14 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------

 <p><b>CPFL</b> ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos


## 8. ANEXOS

### 8.1. Anexo I - Equipe de Crise

Posição na Crise	Cargo	Nome	Telefone Celular	E-mail
Executivo da área de crise	Diretor de Tecnologia da Informação - EI	Thiago Amante	(11) 99602-8319	<a href="mailto:thiago.amante@cpfl.com.br">thiago.amante@cpfl.com.br</a>
Gerente de Segurança da Informação	Gerente de Segurança da Informação	Emerson Cardoso	(11) 99593-9300	<a href="mailto:emerson.cardoso@cpfl.com.br">emerson.cardoso@cpfl.com.br</a>
Responsável ADMS	Gerente Soluções TI para Operações Sr	Carlos Alberto Belarmino Teixeira	(19) 99222-9966	<a href="mailto:belarmino@cpfl.com.br">belarmino@cpfl.com.br</a>
Responsável CWSI	Gerente Soluções TI para Operações Sr			
Responsável OFS				
Responsável Canais Digitais	Gerente Soluções Clientes Sr	Augusto Cesar Reolon	(19) 99369-1089	<a href="mailto:areolon@cpfl.com.br">areolon@cpfl.com.br</a>
AMS SAP	Gerente Soluções Clientes Sr	Augusto Cesar Reolon	(19) 99369-1089	<a href="mailto:areolon@cpfl.com.br">areolon@cpfl.com.br</a>
Responsável Demais Canais	Gerente Digital Ops Sr	Diogo Ribeiro Santana	(19) 99644-1025	<a href="mailto:diogo.santana@cpfl.com.br">diogo.santana@cpfl.com.br</a>
Responsável CCS				
Telefonia Call Center				
Gerente de Governança de TI	Gerente de Governança de TI	Luana Ribeiro Javoni	(19) 99288-0338	<a href="mailto:luanaj@cpfl.com.br">luanaj@cpfl.com.br</a>
Gerente Arquitetura	Gerente Arquitetura e Dados	Diego Perissato	19988219831	<a href="mailto:diego@cpfl.com.br">diego@cpfl.com.br</a>
SAP PO	Analista Arquitetura Soluções TI Sr	Angelo Simonato	(11) 98305-2222	<a href="mailto:augustosimonatosanches@cpfl.com.br">augustosimonatosanches@cpfl.com.br</a>
ADMS	Tech Partner Especialista	Paulo Coelho Marçal	(17) 98131-4835	<a href="mailto:pcoelho@cpfl.com.br">pcoelho@cpfl.com.br</a>
ADMS	Tech Partner Especialista	Vinicius Rodrigues	54984081064	<a href="mailto:vdias@cpfl.com.br">vdias@cpfl.com.br</a>
Canais Digitais	Analista de Sistemas Web Sr	Ricardo Hoytman	19992706833	<a href="mailto:rhoytmansoaresklesse@cpfl.com.br">rhoytmansoaresklesse@cpfl.com.br</a>
Canais Digitais	Analista de Sistemas Web Sr	Rafael Lagranha	19992387048	<a href="mailto:rafael.lagranha@cpfl.com.br">rafael.lagranha@cpfl.com.br</a>
ADMS	Tech Partner Especialista	Emilio Gabriel Gomyde	19996865684	<a href="mailto:emilio.gomyde@cpfl.com.br">emilio.gomyde@cpfl.com.br</a>
Canais Digitais	Coordenador Produtos Digitais	Danilo Rothe	11951778337	<a href="mailto:drote@cpfl.com.br">drote@cpfl.com.br</a>
ADMS	Tech Partner Especialista	Thiago Pavan	19981794580	<a href="mailto:tpavan@cpfl.com.br">tpavan@cpfl.com.br</a>
Infraestrutura	Coordenador Smart Operations e Web	Samuel Flores	51996020201	<a href="mailto:samuel.flores@cpfl.com.br">samuel.flores@cpfl.com.br</a>
ADMS	Tech Partner Especialista	Patricia Lopes	19982026609	<a href="mailto:pcavalcante@cpfl.com.br">pcavalcante@cpfl.com.br</a>
Gerente Arquitetura	Gerente Arquitetura e Dados	Diego Perissato	19988219831	<a href="mailto:diego@cpfl.com.br">diego@cpfl.com.br</a>
Gerente Soluções Empresariais	Gerente Soluções Empresariais Sr	Cristiano Alberto	19982873201	<a href="mailto:cristianoalberto@cpfl.com.br">cristianoalberto@cpfl.com.br</a>
Infraestrutura	Gerente Serviços e Cloud	Alexandre Barrias	19997157806	<a href="mailto:alexandre.barrias@cpfl.com.br">alexandre.barrias@cpfl.com.br</a>
Coordenador TI	Coordenador de Sistemas Técnicos	Thiago Henrique Souza Domingues	(19) 99165-2850	<a href="mailto:thiago.domingues@cpfl.com.br">thiago.domingues@cpfl.com.br</a>
Coordenador TI	Tech Partner Especialista	Leandro Danilo Piovezan	(17) 991581794	<a href="mailto:ldpiovezan@cpfl.com.br">ldpiovezan@cpfl.com.br</a>
Serviços comerciais	Diretor de Gestão de Energia	Rafael Lazaretti	(19) 99294-5455	<a href="mailto:rlazaretti@cpfl.com.br">rlazaretti@cpfl.com.br</a>
Serviços comerciais	Gerente de Gestao Comercial	Eduardo Crivelaro	(19) 99501-7500	<a href="mailto:crivelaro@cpfl.com.br">crivelaro@cpfl.com.br</a>
Serviços comerciais	Coordenador Solu. Integ Processo Comerc	Luciana Dalben Lima	(19) 99121-4167	<a href="mailto:ludalben@cpfl.com.br">ludalben@cpfl.com.br</a>
Tecnologia da Informação	Diretor de Tecnologia da Informação - EI	Thiago Amante	(11) 99602-8319	<a href="mailto:thiago.amante@cpfl.com.br">thiago.amante@cpfl.com.br</a>
Call Center	Gerente Sr CPFL Atende	Luiz Henrique Pinto	(19) 99778-8245	<a href="mailto:luizhenrique@cpfl.com.br">luizhenrique@cpfl.com.br</a>
Operação CallCenter				<a href="mailto:luizhenrique@cpfl.com.br">luizhenrique@cpfl.com.br</a>
Coordenador SI	Coordenador SI	Renato Amabile	(19) 99971-5763	<a href="mailto:ramabile@cpfl.com.br">ramabile@cpfl.com.br</a>
	Coordenador SI	Leandro Barbosa do Carmo	(19) 97151-7509	<a href="mailto:leandro.carmo@cpfl.com.br">leandro.carmo@cpfl.com.br</a>
	Coordenador SI	Adriana Soares Pimenta Silva	(11) 98571-4755	<a href="mailto:adriana.pimenta@cpfl.com.br">adriana.pimenta@cpfl.com.br</a>
	Coordenador SI	Everton F. Duarte dos Santos	(19) 97172-2778	<a href="mailto:everton.duarte@cpfl.com.br">everton.duarte@cpfl.com.br</a>
Operações	Gerente de Operacoes	Rolands Sarreta Menezes	(19) 99909-1477	<a href="mailto:rolands@cpfl.com.br">rolands@cpfl.com.br</a>
Operações	Diretor de Operações	Osvanil Oliveira Pereira	19997009036	<a href="mailto:osvanil@cpfl.com.br">osvanil@cpfl.com.br</a>
Operações	Gerente do Centro de Operacao Paulista	Luiz Sakaguchi Junior	1999198-8732	<a href="mailto:saka@cpfl.com.br">saka@cpfl.com.br</a>
Gestão do sistema ADMS	Fornecedor	(Schneider)	(19) 99657-4097	N/A
CloudFlare	Fornecedor	CloudFlare	1 561 4796660	<a href="mailto:jverges@cloudflare.com">jverges@cloudflare.com</a>
Acquia	Fornecedor	Acquia	NA	<a href="mailto:pablo.perez@acquia.com">pablo.perez@acquia.com</a> <a href="mailto:hector.iribarne@acquia.com">hector.iribarne@acquia.com</a> <a href="mailto:cadu.monteiro@acquia.com">cadu.monteiro@acquia.com</a>

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 15 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------



 <p><b>CPFL</b> ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

Horário para atuação os plantonistas estão disponíveis no link abaixo:  
<https://cpflenergia.sharepoint.com/:x/s/TL-Operaes/EV341NISbdxHI8YYJP216J4BOn-Z3TQuo4pDhuc0YblkyQ>

## 8.2. Anexo III – Modelo de Notificação a ser enviado: Teams e WhatsApp

Enviado de:	
Enviado para:	
Assunto:	
Prioridade:	
Ticket:	
Sistema:	
Resumo inicial:	
Impacto:	
Próxima comunicação:	
Resumo Final:	


Em um evento de criticidade ALTA, a notificação deverá ser através do grupo do WhatsApp e na sala aberta do Teams.

## 8.3. Anexo IV – Checklist de Ações

Checklist de Ações - Momento De Um Incidente				
Sistemas Técnicos: ADMS   CWSI   OFS   PO Técnico   CCS				
#	Ação	Ambiente	Responsável	Previsão

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 16 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------



 CPFL ENERGIA Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidente para Sistemas Críticos

## 9. REGISTRO DE ALTERAÇÕES

### 9.1. Colaboradores

Empresa	Área	Nome
CPFL Paulista	Tecnologia da Informação	Mateus Rocha
CPFL Renováveis	Tecnologia da Informação	Emerson Cardoso

### 9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não aplicável	Não aplicável	Documento em versão inicial

N.Docu mento: 150104	Cate goria: Tátic o	Ver são : 1.0	Apro vado por: Emer son Card oso	Data Public ação: 29/12/ 2023	Pá gin a: 18 de 18
----------------------------	------------------------------	------------------------	--	---	-----------------------------------