# PLANO DE CONTINGÊNCIA SUPMER

TECNOLOGIA DA INFORMAÇÃO

COMPANHIA DE SANEAMENTO DE ALAGOAS

## Controle de Versão

| Versão | Data | Autor(es) | Revisor(es) | Setor |
|---|---|---|---|---|
| 1.0 | 18/02/2024 | Gedival Luiz | | SUPMER/GETIN |

## Sumário

## 1. OBJETIVO

Este plano objetiva estabelecer procedimentos de comunicação e mobilização para controle e tratamento de incidentes, com foco na redução de impacto negativo causado por desastres e no restabelecimento dos serviços de Tecnologia da Informação (TI). Visando aplicar as ações necessárias para correção e/ou eliminação do problema.

## 2. APLICAÇÃO

Este documento se aplica a todos os serviços e infraestruturas de Tecnologia da Informação executados no âmbito da CASAL.

## 3. ESCLARECIMENTOS / DEFINIÇÕES

**Acionamento:** é o processo de comunicação com as equipes envolvidas o controle da emergência, de acordo com a ordem estabelecida para que as equipes desempenhem as atividades sob suas responsabilidades, a fim de controlar a emergência.

**Administrador do Plano de Contingência:** Responsável pela manutenção e atualização dos dados e procedimentos necessários à plena operacionalidade do Plano de Contingência.

**Áreas Sensíveis:** Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas encontram-se os laboratórios de informática, salas administrativas, Datacenter e demais locais que possuam equipamentos de informática.

**Área Vulnerável:** Área atingida pela extensão dos efeitos provocados por um evento de falha.

**Contingência:** Situação de risco com potencial de ocorrer, inerente as atividades, os serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

**Datacenter:** Ou centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores, e outros equipamentos computacionais.

**DHCP:** Dynamic Host Configuration Protocol.

**Incidente:** É o evento não programado de grande proporção capaz de causar danos graves aos sistemas e aos equipamentos de TI da CASAL.

**Hipótese Acidental:** Toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade, da qual possam resultar danos aos sistemas e/ou equipamentos de TI da CASAL.

**Intervenção:** É a atividade de atuar durante a emergência, seguindo ações planejadas, visando minimizar os possíveis dados aos equipamentos e sistemas de TI da CASAL.

**Sistema de Suporte:** Sistema REDMINE (www.redmine.casal.al.gov.br) instalado em um servidor web da CASAL, onde é possível receber, organizar e manter o solicitante/servidor informado sobre o andamento do chamado de suporte.

**Situação de Emergência:** Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho do trabalho de servidores da CASAL.

**TI:** Tecnologia da Informação.

**VM:** Máquina Virtual, virtualizada no servidor *VMware Workstation*.

# 4. RESPONSABILIDADES

## 4.1. Equipe do Setor de Tecnologia da Informação

Deve fornecer suporte técnico, auxiliando os docentes, discentes e colaboradores da CASAL em todo trabalho computacional ou que envolva indiretamente os sistemas corporativos e acadêmicos da organização. Sua responsabilidade também consiste em administrar o local físico e informar a um nível superior sobre os problemas identificados para solução de forma rápida e precisa.

## 4.2. Colaboradores da CASAL

Responsáveis por informar o Setor de TI, por meio de abertura de chamado na INTRANET (www.intranet.casal.al.gov.br) ou Telefone, caso detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis do Campus Sertão.

# 5. NÍVEIS DE INCIDENTES

**Nível I** – Hipótese acidental que pode ser controlada pela equipe de TI e que não afeta o andamento do trabalho do servidor.
Ex: Problemas com equipamentos periféricos de computadores.

**Nível II** – Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo colaborador.
Ex: Problema com o funcionamento do Computador (não liga, travado, etc) ou ainda sistemas offline impedindo o uso do mesmo.

**Nível III** – Hipótese acidental que impede o uso de sistemas ou equipamentos de toda a Unidade, impedindo assim o desenvolvimento do trabalho de todos os colaboradores daquela Unidade ou de toda a CASAL.
Ex: Falha na conexão com a internet ou queda de energia elétrica na Unidade ou ainda problema técnico em algum servidor de rede que controla a conexão interna da CASAL.

## 6. PRIORIDADES

A definição da prioridade no atendimento precisa ser técnica e pragmática, sendo assim a opção é seguir as boas práticas. O framework ITIL é uma delas. Portanto, a PRIORIDADE é definida pela relação URGÊNCIA versus IMPACTO.

| URGÊNCIA \ IMPACTO | ALTO | MÉDIO | BAIXO |
|---|---|---|---|
| ALTA | 1 | 2 | 3 |
| MÉDIA | 2 | 3 | 4 |
| BAIXA | 3 | 4 | 5 |

*Figura 1 – Tabela Impacto / Urgência*

O número de usuários afetados define o impacto do incidente. Já a urgência pode levar em conta a característica da atividade e o quanto ela impacta, por exemplo, nas atividades que não podem ser interrompidas: aulas, palestras, pregões eletrônicos, webconferências.

| PRIORIDADE | | | |
|---|---|---|---|
| 1 | CRÍTICA | 1 hora | |
| 2 | ALTA | 4 horas | |
| 3 | MÉDIA | 24 horas | |
| 4 | BAIXA | 48 horas | |
| 5 | PLANEJADA | - | |

*Figura 2 – Tabela de prazo para atendimento da Priorização*

## 7. PRINCIPAIS RISCOS

O Plano de Contingência foi desenvolvido para ser acionado quando da ocorrência de cenários que apresentam risco à continuidade dos serviços essenciais.

O quadro abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

| Evento | Possíveis |
|---|---|
| 01 – Interrupção de energia elétrica | Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 30 minutos.<br><br>Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuito, incêndio e infiltrações. |

| | |
|---|---|
| 02 – Falha na climatização do DataCenter. | Superaquecimento dos ativos devido a falha no sistema de climatização. |
| 03 – Indisponibilidade de rede-circuitos | Rompimento de cabeamento decorrente de execuções de obras internas, desastres ou incidentes. |
| 04 – Falha humana | Acidente ao manusear equipamento. |
| 05 – Falha de hardware | Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório. |
| 06 – Ataque cibernético | Ataque virtual que comprometa o desempenho, os dados ou a configuração dos serviços essenciais. |

# 8. PRINCIPAIS PROBLEMAS, INCIDENTES E DEVIDAS AÇÕES DE CONTINGÊNCIA

## 8.1. Problemas com computadores

a) O Colaborador que está utilizando o equipamento, informa ao Setor de TI através de chamado na INTRANET (www.intranet.casal.al.gov.br), caso não seja possível acessar a INTRANET, o chamado pode ser aberto entrando em contato com o Setor de TI através do telefone do Setor;
b) O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c) Caso o problema impeça o andamento do trabalho do servidor, o Setor de TI vai até o local fazer uma primeira verificação do problema e tentar solucioná-lo *in-loco*. Caso não seja possível a resolução do problema, o computador será recolhido para reparo no laboratório.

## 8.2. Problema de conexão com a rede interna

a) Identificar o local onde está ocorrendo o problema;
b) Analisar a conexão do Servidor até o local afetado;
c) Identificar a causa do problema;
d) Caso o problema de conexão seja em toda a Unidade, verificar se os servidores de endereços DHCP e de autenticação estão funcionando adequadamente.

### 8.3. Problemas de conexão com a internet

a) Identificar o local onde está ocorrendo o problema;
b) Analisar a conexão do Servidor até o local afetado;
c) Identificar a causa do problema;
d) Caso o problema de conexão seja em toda a Unidade, verificar se há conexão até o FIREWALL e até o Modem da Operadora. Caso haja conexão interna até os referidos equipamentos, deverá ser aberto um chamado para a operadora Veloo.

### 8.4. Problemas com acesso aos sistemas internos da CASAL

A) Identificar qual o sistema está apresentando o problema de acesso;
B) Verificar se o Sistema está em execução;
C) Por fim, identificar e resolver o problema informando a solução aos demais colaboradores.

### 8.5. Problemas com acesso a algum site específico

a) O Colaborador que está utilizando o equipamento, informa ao Setor de TI através de chamado na INTRANET (www.intranet.casal.al.gov.br), e informando o site que está com problemas ao abrir;
b) O chamado de suporte chega até o Setor de TI e o atendimento é agendado;
c) O Setor verifica o site e o motivo do problema de acesso procedendo com a liberação no firewall caso não entre em conflito com outras regras ou normativas;
d) Após a resolução o solicitante é informado da conclusão/resolução do problema informado.

### 8.6. Problemas físicos com cabeamento de rede interna e externa

a) Identificar qual o problema e onde está ocorrendo;
b) Verificar as ligações (Switches) do cabeamento que está com defeito e testa-lo, bem como os conectores RJ45;
c) Se necessário refazer a crimpagem dos conectores RJ45 imediatamente;
d) Caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas.

### 8.7. Problemas com equipamentos de rede

a) Identificar qual equipamento está apresentando o problema;
b) Caso possível realizar a manutenção do mesmo;

c) Caso não tenha como consertar, realizar a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades dos demais Colaboradores da Unidade;
d) Verificar o estoque do ativo substituído e providenciar aquisição de equipamentos de reposição.

### 8.8. Problemas com falta de energia elétrica

a) Caso seja identificada queda ou falta total de energia elétrica na Unidade entramos em contato com a empresa de energia elétrica para informar o problema;
b) Se a falta de energia for de curta duração os servidores de rede e sistemas continuam em funcionamento, pois estão ligados em um nobreak;
c) Caso a falta de energia dure mais de 1 hora aproximadamente, os sistemas são desligados, bem como os equipamentos e serão religados assim que a energia for restabelecida.

### 8.9. Incidentes de Segurança e Ataques Cibernéticos

a) Caso sejam detectadas anomalias de tráfego de rede pelo firewall o tráfego deve ser monitorado, se necessário, origem e destino podem ser colocados em quarentena ou banidos da rede.
b) Salvar relatórios e logs de acesso para investigação futura.

### 8.10. Incidentes de Segurança e Ataques Cibernéticos

Para qualquer outro tipo de problema que envolva a TI, como configurações de e-mail, impressoras, problemas de acesso que envolvam login e senha e etc. Os passos a serem seguidos são os seguintes:

a) Informar o problema ao Setor de TI, através de Chamado na INTRANET (www.intranet.casal.al.gov.br);
b) O chamado de suporte chegará até o setor de TI e o atendimento é agendado;
c) Após o atendimento o solicitante é informado da conclusão/resolução do problema reclamado;

## 9. CONTROLES PREVENTIVOS E ESTRATÉGIA DE RECUPERAÇÃO

a) O Setor de TI deverá manter cópias backup de VMs com serviços importantes para uma possível restauração mesmo com alguma perda de informação para situações onde a VM em execução entre em um estado crítico de não inicialização ou bug geral;
b) Sempre que possível um computador e/ou notebook estarão à disposição para substituir outro equipamento em uso que apresentou problema;
c) Os colaboradores poderão ter mais de uma impressora cadastrada para realizar impressões institucionais;
d) Servidor de arquivos efetua backup regulares possibilitando a recuperação de arquivos quando da detecção de algum problema.

## 10. MANUTENÇÕES PREVENTIVAS

a) Anualmente o nobreak e seu banco de baterias deverá receber manutenção preventiva realizada por empresa técnica especializada;
b) Semestralmente o sistema de climatização do Data Center deverá receber manutenção preventiva;
c) Anualmente os Servidores deverão receber manutenção preventiva especializada;

## 11. COMUNICAÇÃO

### 11.1. Quem deve comunicar

Qualquer Colaborador que detecte qualquer tipo de problema que diga respeito a sistemas, equipamentos e/ou infraestrutura.

### 11.2. A quem comunicar

A comunicação deve ser feita para o Setor de TI da CASAL.

### 11.3. Como comunicar

Os problemas detectados devem ser informados através de abertura de chamado na Intranet (www.intranet.casal.al.gov.br) ou, entrar em contato através do telefone da SUPMER/GETIN.

## 12. CONSIDERAÇÃO FINAL

Este documento será revisado e atualizado sempre que houver mudanças significativas na infraestrutura.