PLANO DE CONTINGÊNCIA

TECNOLOGIA DA INFORMAÇÃO DO INSTITUTO DE QUÍMICA

Sumário

1. OBJETIVO 3
2. APLICAÇÃO 3
3. ESCLARECIMENTOS / DEFINIÇÕES 3
4. RESPONSABILIDADE 4
   4.1 Equipe do Setor de Tecnologia da Informação 5
   4.2 Coordenador de ti 5
5. NÍVEIS DE INCIDENTES 5
6. PRIORIDADES 6
   8.1 Problemas com computadores nos laboratórios de informática 8
   8.2 Problemas com computadores administrativos 8
   8.3 Problemas de conexão com a rede interna do Instituto 8
   8.4 Problemas de conexão com a rede externa ao Instituto, incluindo Internet. 8
   8.5 Problemas com acesso aos sistemas internos do IQ 8
   8.6 Problemas com acesso à internet pelos servidores em equipamentos particulares 9
   8.7 Problemas com acesso a algum site específico 9
   8.8 Problemas com UPS/no-break 9
   8.9 Problemas com equipamentos de rede 10
   8.10 Problemas físicos com cabeamento da rede interna e externa 10
   8.11 Problemas com falta de energia elétrica 10
   8.12 Incidentes de Segurança e Ataques Cibernéticos 11
   8.13 Outros Problemas 11
9. CONTROLES PREVENTIVOS E ESTRATÉGIA DE RECUPERAÇÃO 11
10. MANUTENÇÕES PREVENTIVAS 12
11. COMUNICAÇÃO 12
   11.1 Quem deve comunicar 12
   11.2 A quem comunicar 12
   11.3 Como comunicar 12
   11.4 Fluxograma 13
12. PUBLICAÇÃO 13
13. VIGÊNCIA/VALIDADE DO PLANO 13

1. OBJETIVO

Este plano descreve os procedimentos de comunicação e mobilização para o controle e tratamentos de incidentes, desastres ou interrupções, com foco na redução de impacto negativo nos os processos críticos de TI relacionados aos sistemas essenciais que impactam os setores administrativos e de ensino do Instituto de Química, ou seja, o documento estabelece as medidas de proteções rápidas e eficazes a serem tomadas para o restabelecimento dos serviços de Tecnologia da Informação (TI) e contém, ainda, os procedimentos de correção e/ou eliminação dos problemas. Para tanto, esse plano possibilita assegurar que os processos críticos têm seus riscos identificados, avaliados, monitorados e controlados.

2. APLICAÇÃO

Este documento se aplica à todos os serviços e infraestruturas de Tecnologia da Informação executados no âmbito do IQ/UFRJ.

Este documento deverá ser empregado no preenchimento nos planos de ações cabíveis à cada ocorrência.

3. ESCLARECIMENTOS / DEFINIÇÕES

Acionamento: é o processo de comunicação com as equipes envolvidas no controle da emergência, de acordo com a ordem estabelecida para que as equipes desempenhem as atividades sob sua responsabilidade, 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, armários de distribuição de redes, 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.

TC: Centro de Processamentos de Dados do IQ.

DHCP: Dynamic Host Configuration Protocol.

DNS: Domain Name Server.

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

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.

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

Sistema de Suporte: OTicket instalado em um servidor, 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 que resulte ou possa resultar em danos próprios sistemas ou equipamentos ou ao desempenho do trabalho dos docentes, discentes e corpo técnico-administrativo do IQ.

TI: Tecnologia da Informação.

UPS: Uninterruptible Power Supply.

VM: Máquina Virtual, virtualizada em um dado *Hypervisor*.

4. RESPONSABILIDADE

Cabe a equipe de TI identificar e analisar os impactos nos processos e perdas potenciais para garantir a continuidade dos serviços priorizando processos críticos por meio do estabelecimento de procedimentos, divisão de responsabilidades e alocação de recursos.

4.1 Equipe do Setor de Tecnologia da Informação

Deve fornecer suporte técnico, auxiliando os docentes, discentes e colaboradores do IQ da UFRJ em todo trabalho computacional ou que envolva indiretamente os sistemas corporativos e academicos da organização. Isso é devem mitigar os impactos que por ventura venham a ocorrer decorrentes de emergências ou situações de emergência que afetem os sistemas, equipamentos ou infraestrutura de TI.

Sua responsabilidade também consiste em administrar o local físico e informar a um nivel superior sobre os problemas identificados para solução de forma rápida e precisa.

A equipe também deve elaborar uma documentação (*pos-morten*) descrevendo os desafios superados, as soluções e os aprendizados obtidos na resolução dos problemas.

4.2 Coordenador de ti

Responsável por informar os envolvidos, caso detecte algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis do IQ.

A depender do impacto e urgência dos incidentes a gestão, representada por setores como: Direção, LIG, Secretárias, entre outros tem papel estratégico de tomada de decisão, principalmente em casos que envolva aquisições/compras de emergência.

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 servidor. Ex: Problema com o funcionamento do Computador (não liga, travado, etc) ou ainda sistemas *offline* impedindo o uso do mesmo.

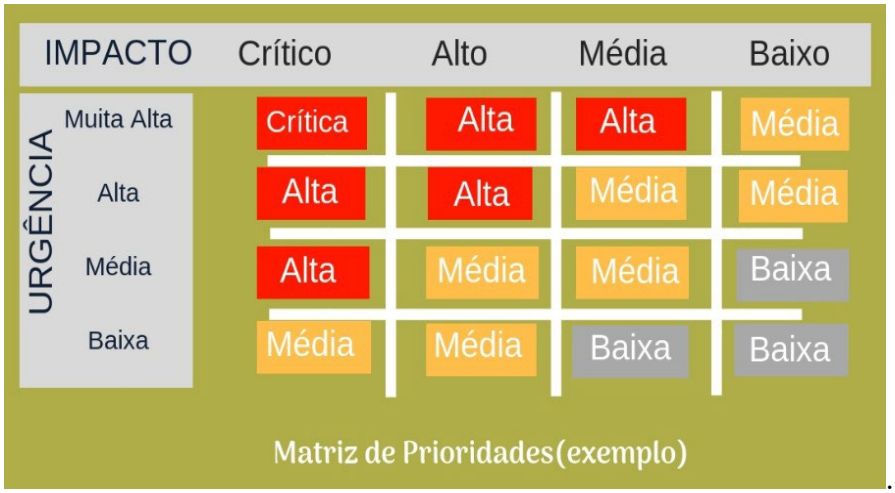
Nível III – Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o IQ, impedindo assim o desenvolvimento do trabalho de todos os servidores. Ex: Falha na conexão com a internet ou queda de energia elétrica no IQ ou ainda problema técnico em algum servidor de rede que controla a conexão interna.

Nível IV – Hipótese acidental que impede o uso de sistemas para o docente ou discente, afetando não só a equipe interna como seus respectivos clientes. Ex. Software acadêmico ou portal do aluno indisponível.

Nível V - Hipótese acidental que impede o uso de sistemas para o docente, discente ou colaborador. Todo o trabalho da organização é suspenso ou impedido pela falha. Ex. Servidores e dados foram comprometidos através de um vírus ou ataque.

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.



O número de usuários afetados (Alunos, Professores, TAEs, etc) 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, licitaçoes, webconferências.

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 1 abaixo define estes riscos e

aponta quais parâmetros para reportar as possíveis causas da ocorrência.

Quadro 1. Eventos e suas possíveis causas

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 10 minutos. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações.
02 - Falha na refrigeração do Datacenter	Superaquecimento dos ativos devido a falha no sistema de refrigeração.
03 - Indisponibilidade de rede/circuitos	Rompimento de cabeamento decorrente de execuções obras internas, desastres ou acidentes.
04 - Falha humana	Acidente ao manusear equipamento.
05 - Ataques internos (usuários insatisfeitos)	Ataque aos ativos do DataCenter e equipamentos de TI com origem nos laboratórios, salas de aula e de uso administrativo/ensino.
06 - Falha de hardware	Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo de aquisição de novos equipamentos.
07- Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.

8. PRINCIPAIS PROBLEMAS, INCIDENTES E DEVIDAS AÇÕES DE CONTIGÊNCIA

8.1 Problemas com computadores nos laboratórios de informática

a. Professores que estão utilizando ou que irão utilizar o referido laboratório, informam ao Setor de TI enviando um e-mail para o endereço suporte@iq.ufrj.br;

b. O chamado de suporte chega até o setor de TI e o atendimento é agendado;

c. Após o atendimento o solicitante é informado da conclusão/resolução do problema informado; e

d. Caso o problema impeça o andamento da aula, o Setor de TI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo *in-loco*.

8.2 Problemas com computadores administrativos

a. O servidor que está utilizando o equipamento, informa ao Setor de TI enviando um e-mail para o endereço suporte@iq.ufrj.br;

b. O chamado de suporte chega até o setor de TI e o atendimento é agendado;

c. Após o atendimento o solicitante é informado da conclusão/resolução do problema informado;

8.3 Problemas de conexão com a rede interna do Instituto

a. O Setor de TI identificará qual serviço está sendo afetado está ocorrendo o problema;

b. Analisar a conexão do servidor central até o setor afetado

c. Identificar a causa do problema;

8.4 Problemas de conexão com a rede externa ao Instituto, incluindo Internet.

a. Identificar em qual setor está ocorrendo o problema;

b. Analisar a conexão do usuário;

c. Identificar a causa do problema se é de responsabilidade da TI ou do próprio usuário;

d. Implementar a solução ou sugestão de solução caso o problema seja de responsabilidade de terceiro.

8.5 Problemas com acesso aos sistemas internos do IQ

a. Identificar qual o sistema está apresentando problema de acesso;

b. Identificar se o problema é para toda a organização ou apenas para algum ou alguns usuários;

c. Verificar se o problema de fato é no sistema em questão ou se é do lado do usuário.

d. Caso seja do lado do usuário:

- ✓ Verificar se o ponto de acesso, cabo, ou outra conexão ao qual o usuário está se conectando está funcional e compatível com a rede do Instituto.
- ✓ Se o problema for no equipamento do usuário orientá-lo a procurar uma assistência técnica ou, em melhor esforço, sugerir uma solução para resolução.

e. Caso seja do lado do serviço prestado:

- ✓ Implementar os reparos necessários de forma mais efetiva possível a fim de reduzir o impacto nas atividades do Instituto.

8.6 Problemas com acesso à internet pelos servidores em equipamentos particulares

a. Verificar configurações definidas de forma manual no equipamento;

b. Verificar se a rede administrativa está funcionando corretamente;

c. Verificar se o ponto de acesso, cabo, ou outra conexão ao qual o usuário está se conectando está funcional e compatível com a rede do Instituto.

d. Se o problema for no equipamento do servidor orientá-lo a procurar uma assistência técnica.

8.7 Problemas com acesso a algum site específico

a. O servidor que está utilizando o equipamento, informa ao Setor de TI através do e-mail suporte@iq.ufrj.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.

8.8 Problemas com UPS/no-break

a. Verificado problema ou anormalidade informado pelo próprio no-break, com o multímetro testa-se a entrada de energia no equipamento pela porta trifásica (entrada da fornecedora) bem como pela porta do banco de baterias;

b. Intervenção imediata para problemas adicionais deve-se contatar de imediato o Departamento de Administração e planejar medidas corretivas junto a empresa técnica especializada externa;

c. Verificar a possibilidade de desligar equipamentos e/ou serviços não essenciais enquanto o funcionamento do no-break não é normalizado;

d. Em caso de desligamento total proceder com o passo "B" e, em paralelo deixar conectado apenas servidor que possui o serviço de Firewall e Roteamento em fonte de energia alternativa para que pelo menos o acesso externo à rede continuem disponíveis no IQ;

8.9 Problemas com equipamentos de rede

a. Identificar qual equipamento está apresentando 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 servidores do IQ.

d. Verificar o estoque do ativo substituído e providenciar aquisição de equipamento de reposição.

8.10 Problemas físicos com cabeamento da 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 testá-lo, bem como os cabos, conectores e outros dispositivos;

c. Se necessário fazer o reparo do equipamento ou cabeamento imediatamente;

d. Caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas.

8.11 Problemas com falta de energia elétrica

a. Caso seja identificada queda ou falta total de energia elétrica no IQ informar aos responsáveis para as devidas providências;

b. Se a falta de energia for de curta duração (menos de 10 minutos), os sistemas e servidores de rede continuam em funcionamento, pois estão ligados em um sistema UPS;

c. Caso a falta de energia dure mais de 10 minutos aproximadamente, os sistemas são desligados, bem como os equipamentos e serão religados assim que a energia for restabelecida.

8.12 Incidentes de Segurança e Ataques Cibernéticos

a. Caso sejam identificadas anomalias de tráfego de rede de forma automática ou pelo TI do Instituto, o tráfego deve ser monitorado, se necessário, origem e destino podem ser colocados em quarentena ou banidos da rede.

b. Qualquer comprometimento de sistemas internos do Instituto são avisados diretamente a Direção do Instituto para análise do incidente delimitado um plano de ação a ser definido dada a criticidade.

8.13 Outros Problemas

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 do IQ através do e-mail suporte@iq.ufrj.br.

b. O chamado de suporte chega até o setor de TI e o atendimento é agendado;

c. Caso seja necessário, o chamado será escalonado para outros setores ou responsáveis

d. 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 dos serviços importantes para uma restauração total dos serviços em execução. Para os serviços não críticos é tolerada perda de informações não relevantes: como logs de acesso, atividade e outros.

b. Sempre que possível um computador de mesa ou portátil estarão a disposição para substituir outro equipamento em uso que apresentou problema nas salas de aula;

c. A Direção possui projetores reservas que poderão ser usados em sala de aula no caso de problemas com os projetores fixos;

d. Atualização dos equipamentos de TI para funcionamento continuado e atualização tecnológica idealmente de 3 em 3 anos. No melhor esforço de 5 em 5 anos.

10. MANUTENÇÕES PREVENTIVAS

a. Anualmente o sistema de UPS deverá receber manutenção preventiva realizada por empresa técnica especializada;

b. Se possível, anualmente os projetores deverão receber manutenção preventiva especializada;

c. Semestralmente o sistema de refrigeração do CPD (Datacenter) deverá receber manutenção preventiva.

11. COMUNICAÇÃO

11.1 Quem deve comunicar

Qualquer servidor que identifique qualquer tipo de problema que diga respeito a sistemas, equipamentos e/ou infraestrutura de TI.

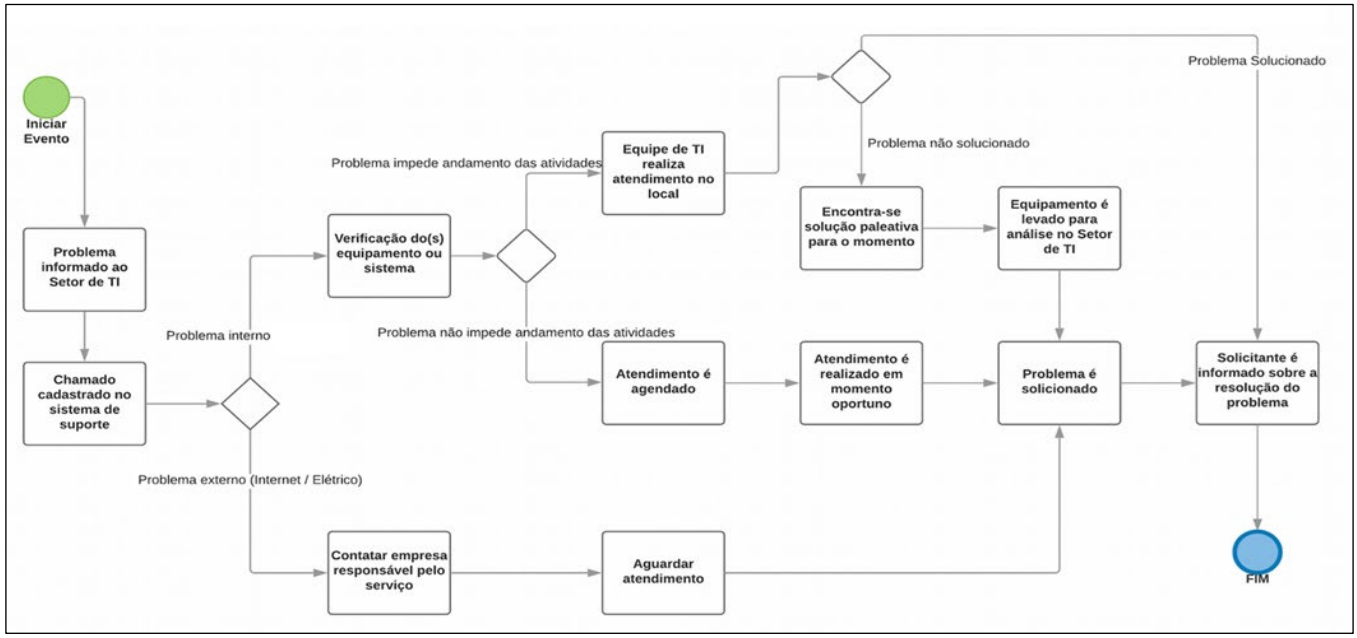
11.2 A quem comunicar

A comunicação deve ser feita para o Setor de TI do IQ.

11.3 Como comunicar

Os problemas identificados devem ser informados através do Sistema de Suporte ou, enviando um e-mail para o endereço suporte@iq.ufrj.br.

11.4 Fluxograma



12. PUBLICAÇÃO

Este documento deve ser publicado no site institucional.

13. VIGÊNCIA/VALIDADE DO PLANO

Este plano tem validade de 5 anos, entrando em vigor a partir da data de sua aprovação pelas instâncias superiores, com revisões anuais obrigatórias ou em caso de mudanças significativas na infraestrutura.

14. REFERÊNCIAS

ABNT NBR ISO/IEC 27001

ABNT NBR ISO/IEC 27002

Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018)

Decreto nº 9.637, de 26 de dezembro de 2018

AXELOS Global Best Practice. ITIL® 4: The framework for the management of IT-enabled services. Disponível em: https://www.axelos.com/certifications/itil-service-management.