PLANO DE CONTINGÊNCIA

UNIVERSIDADE DE BRASÍLIA

CENTRO DE INFORMÁTICA

1. INTRODUÇÃO

Este documento apresenta um plano de contingência que deve ser utilizado imediatamente após a identificação de falhas ou inconsistências nos serviços de TI disponibilizados pelo Centro de Informática – CPD para os usuários da Universidade de Brasília - UnB. Este documento define ações e métodos de comunicação a serem executados em caso de falha nos serviços considerados como críticos que são oferecidos pelo CPD.

2. APLICAÇÃO

Este documento se aplica a todos os serviços críticos, detalhados na tabela Serviços Críticos, suportados pelo Centro de Informática – CPD da Universidade de Brasília – UnB fornecidos para sua comunidade.

3. DEFINIÇÕES DOS TERMOS

a) **Analista de monitoração:** equipe responsável pelo monitoramento e gestão dos eventos de TI (NOC).

b) **Equipe de Especialistas:** equipe de suporte de 3º nível.

c) **Evento:** para fins deste plano, são os itens apresentados no *dashboard* de incidente do *Zabbix* ou sistemas de eventos dos próprios serviços.

d) **Grupo executor:** direção, chefe de área, coordenadores ou integrantes do setor da UnB responsável pelo *host*.

e) **Horário de expediente:** O NOC da UnB funciona 24x7x365, porém a equipe de especialistas compostas por servidores tem o horário de trabalho entre 07h e 19h.

f) ***Host*:** ativo de TI, de equipamentos a sistemas, monitorado pelo *Zabbix*.

g) ***Service* de *host*:** um serviço (POP, SMTP, HTTP, etc.) ou métrica (resposta a um *ping*, número de usuário *logados*, espaço livre em disco, etc.) associada a um host no *Zabbix*.

h) **Incidente:** Qualquer evento que traga incertezas a um serviço do negócio.

i) **Serviço de negócio:** serviço na visão de negócios, produto final oferecido pela UnB, exemplo: e-mail, Sistema SEI, conectividade, DNS etc.

j) **Zabbix:** ferramenta utilizada para monitoração dos ativos da UnB nele cadastrados.

k) **Contingência:** Situação de risco com potencial de ocorrer, inerente às atividades, serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência.

l) **Equipe de Tratamento de análise de risco e tratamento de incidente - ETIR:** Equipe responsável por obter informações quantitativas acerca dos incidentes ocorridos descrevendo sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes.

m) **Sala Cofre**: Ambiente estanque que visa garantir a máxima segurança ao Data Center envolvendo a proteção, seja de mídias físicas ou eletrônicas, armazenamento de dados, equipamentos ou documentos de alta importância operacional ou estratégica contra incêndios, alagamentos, calor, umidade, pó, poeira, fumaça ou qualquer outra variação ambiental brusca ou extrema que coloque em risco a continuidade dos serviços.

4. CENÁRIO

4.1. Serviços de Tecnologia da Informação

O Centro de Informática é responsável pela coordenação, padronização, supervisão e acompanhamento dos recursos de tecnologia de informação e comunicação coorporativas, especialmente pelos bens comuns de informação e comunicação da UnB. Destaca-se que os processos de gerenciamento de serviços de TIC abrangem a gestão e a entrega de serviços de tecnologia da informação e comunicação com as finalidades de fornecer o suporte necessário aos objetivos de negócio e de atender às necessidades dos usuários, compreendendo a integração entre pessoas, processos e tecnologias que compõem a Universidade. Dessa forma, considerando as melhores práticas do campo de gerenciamento de TIC nas organizações, o CPD utiliza as recomendações da *Information Technology Infrastructure*

Library (ITIL V3) e do modelo de governança de TI denominado *Control Objectives for Information and Related Technology* (COBIT 5), adaptando alguns processos à maturidade da UnB para melhor a qualidade e propiciar uma melhor gestão.

A UnB tem um contrato de prestação de serviços de suporte tecnológico ao ambiente de TIC, operado pela empresa CENTRAL IT TECNOLOGIA DA INFORMAÇÃO LTDA (contrato nº 507/2019), no qual se tem observado o aprimoramento de alguns processos de gerenciamento de TIC. Por meio de pesquisas de satisfação aplicadas aos usuários de TIC da Universidade, constatou-se que 97,52% dos usuários qualificaram os serviços como "bom" ou "ótimo". O percentual de chamados atendidos dentro do prazo foi de 98,66% e estava dentro da meta definida em contrato.

A UnB conta também com um contrato de serviço de *outsourcing* de impressão operado pela empresa SIMPRESS Com. Locação e Serviços S/A (contrato nº 26/2016).

A Sala Cofre, localizada neste centro, está submetida a um contrato operado pela empresa ORION TELECOMUNICAÇÕES ENGENHARIA S/A (contrato nº504/2019). O contrato abrange monitoramento, inspeção dos elementos, manutenção corretiva com o fornecimento de materiais, substituição de componentes, treinamentos para as equipes envolvidas na operação e segurança do ambiente. Todo o processo é certificado conforme a norma ABNT NBR 15247 e ABNT NBR IEC 60529.

Para a infraestrutura de telefonia e redes de dados, a empresa STELMAT TELEINFORMÁTICA LTDA cuida dos serviços continuados, instalação e manutenção de infraestrutura de telefonia e redes de dados com caráter preventivo e corretivo.

A execução de serviços de infraestrutura da rede via fibra óptica está sob a responsabilidade da empresa R&L Santos Construtora LTDA EPP (contrato nº617/2010.

Este Centro também possui solução de *virtualização* que atende ao ambiente de produção do CPD nas áreas de suporte, assistência técnica, manutenção e garantia on-site. Os servidores virtuais estão hospedados no próprio CPD.

Com relação à proteção quanto a perda de arquivos e documentos essenciais, a UnB utiliza uma solução integrada de antivírus, contratada da empresa ESYWORLD SISTEMAS E INFORMATICA LTDA (contrato nº179/2017), bem como conta com licenças

de serviços de suporte para *antispam canit* contratado da empresa UNO DATACENTER ANTISPAM INTERNET SOLUTIONS – LTDA ME (contrato nº097/2017).

4.2. Infraestrutura

No ambiente gerenciado pelo Centro de Informática, responsável pela infraestrutura de TI de toda a instituição, há uma variedade de aspectos que definem as atividades e o funcionamento do ambiente de TI.

Em relação à estabilidade da energia elétrica, há uma subestação de energia no subsolo do prédio do Centro de Informática, no qual se encontra a interface com o sistema de redundância de energia elétrica constituído de 01 (um) gerador de 450 KVA, e 02 (dois) *nobreaks* de 120 KVA.

No que diz respeito a rede lógica, contamos com um ambiente computacional de alta disponibilidade, composto de *blades*, *storages*, roteadores, *switches* de agregação e *core*, *firewalls* enterprises de ponta, controladoras de rede sem fio, sistema de CFTV (Circuito Fechado de Televisão), sistema de backup, os quais suportam os sistemas administrativos, acadêmicos e serviços em rede. Estes equipamentos, bem como o sistema de energia redundante sustentam a Sala Cofre.

Para manter o ambiente dentro de níveis aceitáveis de recuperação de incidentes e problemas relacionados ao funcionamento do ambiente de TI, são definidos acordos de nível de serviço – ANS. O ambiente de monitoramento de serviços e sistemas (NOC) opera 24 horas nos 07 dias da semana e nos 365 dias do ano. Também há o ANS referente à recuperação, englobando manutenção preventiva e corretiva do sistema de alta disponibilidade (Sala Cofre).

No tocante à segurança da informação, há 01 (um) cluster de equipamentos de segurança do ambiente de TI (firewall enterprise) enquadrado no "quadrante mágico" do Gartner como solução de ponta, rotinas de backups pré-definidas executadas por conjunto de *tape libraries* e sistema especializado de armazenamento em disco.

Por fim, com relação a este Plano de Contingência, são realizadas pelo Centro de Informática as atividades de rotinas de backup para armazenamento em ambiente externo. A rede de dados da UnB conta com um cluster de firewall (composto por dois equipamentos que operam em regime de redundância); um cluster de roteamento

para a saída de rede de dados do CPD (composto por dois equipamentos que operam em regime de redundância); monitoramento (NOC – 24x7x365) de ambiente de alta disponibilidade com rotinas básicas preestabelecidas; sistema de redundância (gerador e nobreaks) conectados à rede elétrica da concessionária com contrato de manutenção no regime de 24x7x365; ambiente de virtualização implementado sobre o conjunto de *blades* e dupla abordagem de infraestrutura de fibra óptica na interligação com o link da Rede Metropolitana (GigaCadanga).

5. ATRIBUIÇÕES E RESPONSABILIDADES

PAPEL	RESPONSABILIDADE
Analista de monitoração	• Monitorar de forma ininterrupta o ambiente computacional de alta disponibilidade a ele aplicado. • Acionar a direção, os chefes de área, os coordenadores, o grupo executor ou a equipe Bimodal de acordo com meio de comunicação adequado. • Repassar, com precisão, as informações sobre os eventos sempre que requerido. • Verificar se há falta de energia. • Registrar, tratar e/ou escalonar os chamados relacionados aos eventos do *Zabbix* quando necessários. • Tratar devidamente os eventos no *Zabbix*. • Registrar no diário de turno e no controle do *CITSmart* os eventos ocorridos no *Zabbix* quando necessário. • Desabilitar/Habilitar os *checks* no *Zabbix* em casos de manutenção de *hosts* ou *services* quando requerido.
Diretoria do CPD	• Garantir a execução deste plano de contingência.
Grupo executor	• Tratar e solucionar os incidentes relacionados aos ativos. • Encerrar os chamados após a resolução do incidente no Nagios apondo a devida descrição da solução. • Informar ao NOC da manutenção dos ativos. • Identificar oportunidades de melhorias mantendo o plano sempre atualizado, divulgado e acessível. • Elaborar relatório mensal correlacionado à execução deste plano de contingência, conforme critérios de medição.

Tabela 1: Atribuições e Responsabilidades

6. TABELA DE RESPONSABILIDADES

6.1. Direção do Centro de Informática

A Direção será comunicada sempre que um serviço crítico possuir um Risco que cause interrupção no seu funcionamento.

NOME	FUNÇÃO	E-MAIL (@unb.br)
Domingos	Vice-diretor	domingos
Prof. Jacir Bordim	Diretor CPD	bordim

Tabela 2: Direção

6.2. Chefes das áreas

Os chefes das áreas serão comunicados quando houver indisponibilidade de qualquer serviço crítico de negócio que envolva seus grupos executores.

NOME	FUNÇÃO	E-MAIL (@unb.br)
Consuelo Galo	Chefe – SSI	consuelogalo
Juvenal dos Santos	Chefe – SRS	jbarreto

Tabela 3: Chefes das áreas

6.3. Coordenadores

Os coordenadores serão comunicados somente quando os serviços críticos estiverem com algum evento de alerta no *Zabbix* ou caso ocorra um incidente.

NOME	FUNÇÃO	E-MAIL (@unb.br)
Alex Fidelis	Coordenador Redes / SRS	alekez
Marcos Castro	Coordenador SOP / SRS	mvlcastro
Marcus Vinícius	Coordenador SA / SRS	marcusv
Rodrigo Guidotti	Coordenador CDC / SRS	guidotti

Tabela 4: Coordenadores

6.4. Grupos executores

Listagem dos setores/unidades/empresas responsáveis pela execução das atividades correlatas.

GRUPO EXECUTOR	RAMAIS
ADMINISTRAÇÃO E SUPORTE DE REDES - ASR	70042
CENTRAL IT	70159
DATA CENTER – CDC	70048
GRUPO ORION (SALA COFRE)	Contato NOC
PREFEITURA UNB	Contato NOC
SERVIÇO DE ESTRATÉGIA DE DADOS – SED	70101
SERVIÇO DE SERGURANÇA E OPERAÇÃO – SOP	70019
SERVIÇO DE SISTEMA DE INFORMAÇÃO – SSI	70151
SUPORTE AVANÇADO – SA	70004

Tabela 5: Grupos executores

6.5. Plantonistas

Caso o serviço fique indisponível fora do horário de trabalho dos servidores dos grupos executores, essa lista abaixo será comunicada.

Nome	Função	Ramal
Fabiana Figueredo	Supervisora	(61) 3107-0159
Fábio Melo da Silva	Preposto	(61) 3107-0049
Prof. Jacir Bordim	Diretor CPD	(61) 3107-0100

Tabela 6: Plantonistas

7. RELAÇÃO DE SERVIÇOS CRÍTICOS

Relação dos serviços essenciais ao atendimento das necessidades institucionais e funcionamento do negócio.

SERVIÇO DE NEGÓCIO	DESCRIÇÃO	GRUPO EXECUTOR
Active Directory	Serviços de diretórios para computadores tombados pela Fundação Universidade de Brasília	SA
Banco de dados	Serviços que visam proporcionar a disponibilidade, confiabilidade, integridade e guarda dos Bancos de Dados sob custódia	SED

	do Centro de Informática (CPD)	
CitSmart	Sistema de aberturas de chamados utilizado no suporte aos docentes, técnicos administrativos, discentes e prestadores de serviços.	CENTRAL IT
DNS	Sistema de nomes de domínio hierárquico e distribuído de gestão de nomes para computadores, serviços ou máquinas conectadas à rede.	CDC
Internet	Gestão do acesso à rede mundial de computadores.	SOP e ASR
Portal UnB	Site público da UnB com informações relacionadas ao Ensino, Pesquisa e Extensão e Gestão universitária.	SSI
SALA COFRE	Ambiente seguro de alta disponibilidade que hospeda todos os serviços e servidores da UnB	CDC
Serviço de Firewall	Gerencia as comunicações internas e externas da UnB de acordo com a política de segurança determinada.	SOP
Sistema de Catraca	Sistema de acesso ao Restaurante Universitário	SA
Sistema e-mail – Webmail	Sistema de Email para Servidores e Alunos	SA
Sistema Matricula WEB	Sistema de matriculas disponibilizado para os alunos	SSI e SA
Sistema SEI	Sistema de gestão dos processos e documentos eletrônicos da UnB.	SA e SSI
Sistema SIG	Sistema de administração, acadêmico e de Pessoal da UnB	SA
UnB Wireless e Eduroam	Serviço de fornecimento de conexão sem fio à internet para alunos, professores e servidores.	ASR
Virtualização	Hospedagem dos sistemas virtuais nos servidores do CPD.	CDC

Tabela 7: Relação de serviços críticos

8. PRINCIPAIS RISCOS E CONTINGENCIAMENTO

Esse plano tem como objetivo ser acionado quando algum risco afetar diretamente no funcionamento dos serviços críticos, impactando na continuidade das atividades do negócio.

Com isso, a tabela abaixo mostra os principais riscos que possam impactar na continuidade dos serviços críticos listados anteriormente.

RISCO	DESCRIÇÃO	CONTIGENCIAMENTO
Acesso à Sala Cofre	Acesso de pessoas não autorizadas ao ambiente interno da sala cofre.	A Sala cofre possui monitoramento 24x7x365 e controle de acesso.
Ataques Externos	Ataque cibernético que causa danos ou roubo de informação dos serviços disponíveis externamente, grande parte dos ataques são de negação do serviço, que tem como foco deixar o serviço indisponível.	Gerenciamento de eventos e redundância de equipamentos de Firewall. Equipe de tratamento de análise de risco e tratamento de incidente - ETIR.
Ataques Internos	Causados por usuários legítimos da rede, porém, tentando acessar algum serviço ou equipamento para deixa-lo indisponível.	Gerenciamento de eventos e redundância de equipamentos de Firewall. Equipe de ETIR.
Falha Humana Acidental	Causada pela falta de atenção dos usuários	Capacitação, e controle de acesso as serviços e sistemas.
Falha Humana por imperícia	Causada por falta de capacidade técnica ou conhecimento suficiente para dá suporte em algum serviço ou sistema.	Capacitação, treinamento e controle de acesso aos serviços e sistemas.
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 3 horas.	Gerador com tanque interno com capacidade/autonomia de 25 horas, mais um tanque externo com capacidade de dois mil litros possibilitando manter o gerador em pleno funcionamento por pelos menos 100 horas.
Migração e Mudanças em Aplicações Virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades do Negócio.	Uso de *kubernets* e VM para migração das aplicações em caso de falha de hardware, minimizando ou mesmo eliminando a indisponibilidade do serviço.
Problema com Equipamentos (Hardwares que	Causado por equipamentos antigos ou equipamentos que por algum motivo necessite reparar alguma peça.	Contrato com os Fabricantes dos equipamentos, garantia de 5 anos e peças para substituição e reparo

dão suporte aos serviços críticos)		imediato.
Problemas de conexão (rede interna à UnB e externa)	Causados principalmente por rompimentos de cabos de rede e fibra óptica ou por problemas em equipamentos de redes, como Roteadores, Switches e Firewalls.	Gerenciamento de eventos, cabeamento e equipamentos para troca imediata. Redundância dos enlaces da Universidade de Brasília.
Risco na Identificação de Eventos	Causado por falta de pessoal para monitoramento dos eventos no serviço *Zabbix*.	Contrato com empresa para trabalho com NOC – Núcleo de operação e controle 24x7x365.
Risco Pessoal	Causado pela perda de capital humano.	Plano de capacitação e apoio à educação continuada. Programa de Pós-Graduação em Computação Aplicada – PPCA.
Sala Cofre	Risco que pode comprometer a vida útil dos hardwares da sala cofre, causando superaquecimento, inundação, incêndios.	Sala Certificada com manutenção em dia e redundância de climatização.

Tabela 8: Principais Riscos e Contingenciamento

9. PLANO DE COMUNICAÇÃO

Quem deve comunicar: Analista de monitoramento ou qualquer servidor que detecte algum incidente que possa gerar risco aos serviços.

A quem comunicar: Seguir a tabela de responsabilidades do grupo executor disposta na Tabela 5: Grupos executores.

Como comunicar: Na tabela de responsabilidades possui o ramal e e-mail de todos os responsáveis e também deverá ser feito o registro do incidente no sistema CITSmart e encaminhar para o grupo executor.