

UnB | STI

# Plano de Contingência da Secretaria de Tecnologia da Informação da Universidade de Brasília



**Secretário de TI**

Jacir Luiz Bordim

**Coordenadoria de Gestão e Planejamento – CGESP**

Francisco Jackson Alves de Freitas

**Divisão de Contratações e Aquisições de TIC**

Wellington Ferreira

**Divisão de Apoio à Governança de TIC**

André de Lanna Sette Fiuza Lima

**Núcleo de Capacitação**

Henrique de Almeida Ramos

**Diretoria de Operações e Serviços - DOS**

Domingos Pereira Costa

**Coordenadoria de Redes e Infraestrutura**

Alex Anderson Dantas Fidelis

**Coordenadoria de Serviços Especializados**

Marcus Vinicius da Silva Jorge

**Coordenadoria de Segurança da Informação**

Juvenal dos Santos Barreto

**Divisão de Atendimento ao Usuário**

Rister Abadio Barbosa

**Divisão de Data Center**

Rodrigo Coelho Guidotti

**Diretoria de Sistemas da Informação**

Consuelo Martins Galo

**Coordenadoria de Sistemas Administrativos**

Eduardo Chagas Lustoza

**Coordenadoria de Sistemas Acadêmicos**

Felipe Evangelista dos Santos

**Coordenadoria de Sistemas de Pessoal**

Andrei Lima Queiroz

**Coordenadoria de Estratégia de Dados**

Tiago Medina Chagas

**Coordenadoria de Sites Corporativos**

Elaine Teixeira dos Santos

**Equipe Técnica**

Domingos Pereira Costa

Fernando de Britto e Silva

Fernando Alecsandro dos Santos Teixeira

Juvenal dos Santos Barreto

Rodrigo Coelho Guidotti

**Equipe de Apoio**

André de Lanna Sette Fiuza Lima

Antônio Carlos Baptista de Oliveira

John Lennon da Silva Rodrigues



## Histórico de Revisões

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>	<b>Autor</b>
01/08/2022	1.0	Modelo Inicial	Equipe Técnica
02/08/2022	1.1	Revisão	Antônio Carlos, André de Lanna, Jacir Bordim, Francisco Jackson, Rodrigo Guidotti, Fernando Alecsandro, Fernando de Britto, Domingos Pereira.
04/08/2022	1.2	Revisão	Jacir Bordim, Antônio Carlos, André de Lanna, Francisco Jackson, Rodrigo Guidotti, Fernando Alecsandro, Fernando de Britto, Domingos Pereira, Juvenal dos Santos Brito, Jonh Lenon da Silva Rodrigues.

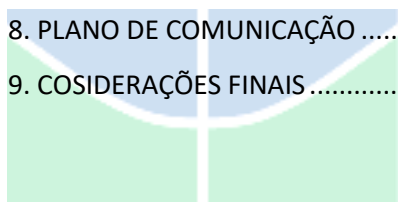


UnB | STI



## Sumário

DEFINIÇÃO E TERMOS UTILIZADOS NESTE DOCUMENTO .....	6
1. INTRODUÇÃO .....	7
2. APLICAÇÃO .....	7
3. CENÁRIO .....	7
3.1. Serviços de Tecnologia da Informação .....	7
3.2. Infraestrutura .....	8
4. ATRIBUIÇÕES E RESPONSABILIDADES .....	8
5. HIERARQUIZAÇÃO DE RESPONSABILIDADES PARA ATENDER OS SERVIÇOS CRÍTICOS .....	8
5.1. Equipe de Monitoração .....	8
5.2. Grupo Responsável .....	8
5.3. Diretorias .....	9
5.4. Direção da Secretaria de Tecnologia da Informação .....	9
6. RELAÇÃO DE SERVIÇOS CRÍTICOS .....	9
7. PRINCIPAIS RISCOS E CONTINGENCIAMENTO .....	10
8. PLANO DE COMUNICAÇÃO .....	11
9. CONSIDERAÇÕES FINAIS .....	11



UnB | STI



## **Tabelas**

Tabela 1: Atribuições e Responsabilidades.....	8
Tabela 2: Grupos responsáveis .....	9
Tabela 3: Diretorias das áreas.....	9
Tabela 4: Direção .....	9
Tabela 5: Relação de serviços críticos.....	10
Tabela 6: Principais Riscos e Contingenciamento.....	11



UnB | STI

## DEFINIÇÃO E TERMOS UTILIZADOS NESTE DOCUMENTO

- a) **Analistas de monitoração:** equipe responsável pelo monitoramento e gestão dos incidentes de Tecnologia da Informação (TI) do Núcleo de Operação e Controle (NOC da UnB);
- b) **Ativos de TI:** todos os componentes da Tecnologia da Informação que a UnB utiliza para proteger seus hardwares (switches, sistemas de software ou informações e insumos que agregam valor para o cumprimento de sua missão.
- c) **Contingência:** situação de risco com potencial de ocorrer, inerente às atividades, serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência;
- d) **Equipe de Tratamento e Reposta a Incidente Cibernético (ETIR):** equipe responsável por receber, analisar e responder às notificações e atividades relacionadas aos incidentes cibernéticos ocorridos descrevendo sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes;
- e) **Garantia:** Período em que o produto ou serviço contará com o suporte do fornecedor para garantir a sua disponibilidade e/ou correto funcionamento.
- f) **Grupo Responsável:** equipe de especialistas de 3º nível, composta por coordenadores da STI/UnB;
- g) **Grupo responsável:** setores da STI responsáveis por um ou mais serviços críticos;
- h) **Incidente:** qualquer evento que traga indisponibilidade ou falha nos ativos de TIC;
- i) **Nobreak:** dispositivo alimentado a bateria, capaz de fornecer energia elétrica ao sistema por um certo tempo em caso de interrupção de energia elétrica;
- j) **NOC (Network Operation Center):** Centro de Operações de Rede em português, estrutura de profissionais especializados que realiza o monitoramento e a gestão dos eventos de TI, que na Secretaria de Tecnologia da Informação da UnB é denominado Núcleo de Operação e Controle (NOC da UnB).
- k) **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 nela hospedados;
- l) **Serviços críticos:** são sistemas e ativos fundamentais ao pleno funcionamento da UnB e que estão hospedados dentro do ambiente da STI.

## 1. INTRODUÇÃO

Este documento apresenta um plano de contingência que deve ser utilizado imediatamente após a identificação de falhas ou inconsistências nos serviços (críticos) de Tecnologia da Informação (TI) disponibilizados pela Secretaria de Tecnologia da Informação - STI 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 disponibilizados pela STI.

## 2. APLICAÇÃO

Este documento se aplica a todos os serviços críticos, detalhados na “Tabela 5 - Relação de serviços críticos”, suportados pela Secretaria de Tecnologia da Informação (STI) da Universidade de Brasília (UnB) fornecidos para sua comunidade.

## 3. CENÁRIO

### 3.1. Serviços de Tecnologia da Informação

A Secretaria de Tecnologia da Informação (STI) é responsável pela coordenação, padronização, supervisão, custódia das informações e acompanhamento dos recursos de tecnologia de informação e comunicação corporativas, responsável por assegurar a confidencialidade, integridade e disponibilidade da informação por meio de adoção e aplicação de mecanismos e controles de segurança alinhados às políticas e normativos internos e externos, visando obter maior eficiência institucional nas atividades de ensino, pesquisa, extensão e gestão universitária.

Os processos de gerenciamento e gestão de serviços de Tecnologia da Informação e Comunicação (TIC) abrangem a entrega dos serviços de TIC com as finalidades de fornecer o suporte necessário aos objetivos da instituição e de atender às necessidades dos usuários, compreendendo a integração entre pessoas, processos e tecnologias que compõem a Universidade, considerando as melhores práticas de gerenciamento de TIC nas organizações adaptando alguns processos à maturidade da UnB para melhorar a qualidade e propiciar uma melhor gestão.

### 3.2. Infraestrutura

No ambiente gerenciado pela Secretaria de Tecnologia da Informação, responsável pela infraestrutura de TI dos serviços críticos, há uma variedade de aspectos que definem as atividades e o funcionamento do ambiente de TI.

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), documento que descreve o que será acordado entre as partes interessadas e descreverá o que uma pode oferecer e o que a outra pode exigir. O ambiente de monitoramento de serviços e sistemas do NOC da UnB opera de maneira ininterrupta. Também há o ANS referente à recuperação, englobando manutenção preventiva e corretiva do sistema de alta disponibilidade (Sala Cofre).

## 4. ATRIBUIÇÕES E RESPONSABILIDADES

PAPEL	RESPONSABILIDADE
Secretário de TI	<ul style="list-style-type: none"><li>• Aprovar o plano de contingência e solicitar atualizações.</li></ul>
Analista de monitoração	<ul style="list-style-type: none"><li>• Monitorar de forma ininterrupta o ambiente computacional de alta disponibilidade.</li><li>• Acionar a direção, os chefes de área, os coordenadores e/ou grupo responsável pelo acordo com o meio de comunicação adequado.</li><li>• Registrar, tratar e/ou escalonar os chamados relacionados aos eventos do sistema de monitoramento.</li></ul>
Grupo responsável	<ul style="list-style-type: none"><li>• Tratar e solucionar os incidentes relacionados aos serviços críticos.</li><li>• Identificar oportunidades de melhorias sugerindo atualizações do plano sempre que necessário.</li></ul>

**Tabela 1: Atribuições e Responsabilidades**

## 5. HIERARQUIZAÇÃO DE RESPONSABILIDADES PARA ATENDER OS SERVIÇOS CRÍTICOS

### 5.1. Equipe de Monitoração

A equipe de monitoração é composta pelo NOC da UnB, atua de forma preventiva e proativa com objetivo de manter o ambiente de TI o mais estável possível e quando identificam algum alerta que não consigam resolver acionam o Grupo Responsável.

### 5.2. Grupo Responsável

Os coordenadores serão comunicados sempre que um serviço crítico estiver com algum evento do sistema de monitoramento.



Listagem dos setores responsáveis pela execução das atividades.

GRUPO RESPONSÁVEL	E-MAIL
Coordenação de Redes e Infraestrutura (DOS/CRI)	sti.cri@unb.br
Coordenação de Estratégia de Dados (DSI/CED)	sti.ced.unb.br
Coordenação de Segurança da informação (DOS/CSI)	sti.csi@unb.br
Coordenação de Serviços Especializados (DOS/CSE)	sti.cse@unb.br
Divisão de Data Center (DOS/DDC)	sti.ddc@unb.br
Coordenadoria de Sites Corporativos (DSI/Sites)	sti.sites@unb.br
Coordenadoria de Sistemas Administrativos (DSI/ADM)	sti.admin@unb.br
Coordenadoria de Sistemas Acadêmicos (DSI/ACAD)	sti.acad@unb.br

**Tabela 2: Grupos responsáveis**

### 5.3. Diretorias

Os Diretores das áreas serão comunicados quando houver indisponibilidade de qualquer serviço crítico da instituição que envolva seus grupos responsáveis.

DIRETORIA	E-MAIL
Diretoria de Sistemas da Informação (DSI)	sti.dsi@unb.br
Diretoria de Operações e Serviços (DOS)	sti.dos@unb.br

**Tabela 3: Diretorias das áreas**

### 5.4. Direção da Secretaria de Tecnologia da Informação

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

FUNÇÃO	E-MAIL
Secretário de Tecnologia da Informação	sti.dir@unb.br

**Tabela 4: Direção**

## 6. RELAÇÃO DE SERVIÇOS CRÍTICOS

Relação dos serviços essenciais ao atendimento das necessidades institucionais e funcionamento dos serviços de TIC.

SERVIÇO DE TIC	DESCRIÇÃO	GRUPO RESPONSÁVEL
<b>Active Directory</b>	Serviços de diretórios para computadores tomados pela Fundação Universidade de Brasília	CSE
<b>Banco de dados</b>	Serviços que visam proporcionar a disponibilidade, confiabilidade, integridade e guarda dos Bancos de Dados sob custódia da Secretaria de Tecnologia da Informação (STI)	CED
<b>ServiçosTIC</b>	Sistema de aberturas de chamados utilizado no suporte aos docentes, técnicos administrativos, discentes e prestadores de serviços.	CSE
<b>DNS</b>	Sistema de nomes de domínio hierárquico e distribuído de gestão de nomes para computadores, serviços ou máquinas conectadas à internet.	CSE e DDC
<b>Internet</b>	Gestão do acesso à rede mundial de computadores.	DDC e CRI
<b>Portais UnB</b>	Sites públicos da UnB com informações relacionadas ao Ensino, Pesquisa e Extensão e Gestão universitária.	Sites
<b>Controle de acesso ao Restaurante Universitário (RU)</b>	Sistema de acesso ao Restaurante Universitário (Catraca).	ADM
<b>E-mail e listas de discussão</b>	Sistema de e-mail e listas de discussão para comunidade.	CSE
<b>SEI</b>	Sistema de gestão dos processos e documentos eletrônicos da UnB.	DSI e CSE
<b>SIG UnB</b>	Sistema de administração, acadêmico e de Pessoal da UnB	ADMIN, ACAD e CSE
<b>Rede sem fio</b>	Serviço de fornecimento de conexão sem fio à internet para alunos, professores e servidores (UnB Wireless e Eduroam).	CRI

**Tabela 5: Relação de serviços críticos**

## 7. 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 da instituição.

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

RISCO	DESCRIÇÃO	CONTINGENCIAMENTO
Acesso indevido à Sala Cofre	Acesso de pessoas não autorizadas ao ambiente interno da sala cofre.	A Sala cofre possui monitoramento ininterrupto 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 segurança de TI, ações dos grupos responsáveis e equipe de ETIR.
Ataques Internos	Causados por usuários legítimos da rede, porém, tentando acessar algum serviço ou equipamento para deixá-lo indisponível.	Gerenciamento de eventos e redundância de equipamentos de segurança de TI, ações dos grupos responsáveis e equipe de ETIR.

Falha Humana Acidental/Imperícia	Causada por falta de atenção, capacidade técnica ou conhecimento suficiente para dar suporte em alguns equipamentos ou sistemas.	Uso de privilégio mínimo para as permissões de usuários, senhas fortes, capacitação e etc.
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade.	Grupo Gerador composto de um Gerador e nobreak.
Migração e Mudanças em Aplicações Virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades dos serviços de TIC.	Processo de gerenciamento de mudança.
Problema com Equipamentos (Hardwares que dão suporte aos serviços críticos)	Causado por equipamentos que por algum motivo necessitem de reparos.	Manter contratos de garantia/suporte e/ou mecanismos de redundância.
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 e segurança da informação.	Manter contratos de garantia/suporte e/ou mecanismos de redundância.
Falha na Identificação de Eventos	Causado por falta de pessoal para monitoramento dos eventos no serviço de monitoramento.	Firmar contrato com empresa para trabalho no Núcleo de Operação e Controle (NOC).
Indisponibilidade da Sala Cofre	Incidentes que podem comprometer a disponibilidade e/ou a integridade dos equipamentos.	Manter contrato de manutenção e a certificação da sala cofre.

**Tabela 6: Principais Riscos e Contingenciamento**

## 8. PLANO DE COMUNICAÇÃO

Existe um plano de comunicação interno firmado entre STI e empresas terceirizadas que é colocado em prática em conjunto com este plano de contingência.

### Quem deve comunicar:

Equipe de Monitoração ou qualquer servidor que detecte algum incidente que possa gerar risco aos serviços.

### A quem comunicar:

Aos grupos responsáveis constantes na Tabela 2.

### Como comunicar:

Por e-mail e está especificado no plano de comunicação interno.

## 9. CONSIDERAÇÕES FINAIS

Este documento será publicado no site institucional da STI/UnB (<https://sti.unb.br/>), entrando em vigor a partir da data de sua aprovação. Será revisado e atualizado sempre que houver mudanças significativas na infraestrutura.