SeTI
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

UFJ
UNIVERSIDADE FEDERAL DE JATAÍ

PLANO DE CONTINGÊNCIA DA SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Versão: 1.0

Abril 2025

Câmpus Jatobá - Cidade Universitária - BR 364, km 195, nº 3800
Jataí - GO CEP 75801-615

1. Contextualização

A Universidade Federal de Jataí (UFJ), como instituição pública federal, está inserida em um contexto cada vez mais dependente das tecnologias da informação e comunicação para a execução de suas atividades finalísticas e de apoio. Essa realidade impõe não apenas a necessidade de infraestrutura tecnológica confiável, mas sobretudo a adoção de mecanismos sistemáticos que assegurem a continuidade dos serviços críticos diante de incidentes que comprometam a disponibilidade, integridade e confidencialidade das informações.

A conformidade com normativos vigentes exige atenção especial à gestão de riscos e à segurança da informação. A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) estabelece diretrizes rigorosas para o tratamento de dados pessoais, inclusive no setor público, determinando que os órgãos implementem medidas eficazes de proteção contra acessos não autorizados e perda de dados. O Decreto nº o Decreto nº 12.198/2024, reforça esse compromisso ao exigir ações concretas voltadas à mitigação de riscos e à garantia da continuidade das operações.

No mesmo sentido, o Decreto nº 10.748/2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos, trata a continuidade de serviços como elemento essencial da resiliência institucional. Já a Instrução Normativa nº 2/2020 do Gabinete de Segurança Institucional/Presidência da República (GSI/PR) orienta a elaboração de documento de constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, que devem estar alinhados aos processos críticos e sustentados por análise de impacto e avaliação de riscos.

Adicionalmente, a Estratégia de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados (Decreto nº 12.198/2024) destaca a importância de infraestruturas resilientes, escaláveis e seguras para sustentar os serviços digitais da administração pública, o que inclui a adoção de soluções redundantes, ambientes alternativos e capacidade de recuperação em tempo hábil. Tais exigências são igualmente reforçadas pela Instrução Normativa da Secretaria de Governo Digital do então Ministério da Economia (SGD/ME) nº 1/2019, que regulamenta Plano Diretor de Tecnologia da

Informação e Comunicação (PDTIC) e impõe a previsão de ações voltadas à expansão, contingência e continuidade das soluções de TIC.

Diante desse cenário normativo e da complexidade crescente dos ambientes computacionais, este Plano de Contingência foi concebido com o propósito de estabelecer diretrizes, responsabilidades e procedimentos operacionais que permitam à UFJ manter a continuidade de seus serviços essenciais em situações adversas. A proposta fundamenta-se em boas práticas reconhecidas pelo Tribunal de Contas da União (TCU), pela Controladoria Geral da União (CGU) e por normativos técnicos nacionais, observando os princípios da segurança da informação, da gestão de riscos e da governança de TIC. Assim, o objetivo principal é assegurar a manutenção de serviços críticos, minimizar os prejuízos e permitir a recuperação rápida das operações em caso de incidentes.

2. Diretrizes propostas para o plano de contingência da SeTI/UFJ

- Priorizar os serviços críticos e definir parâmetros de recuperação;
- Adotar padrões técnicos e normativos nacionais;
- Manter monitoramento contínuo e resposta imediata a incidentes;
- Fortalecer a governança de TI, a gestão de riscos e a capacitação institucional;
- Realizar testes e revisões periódicas para melhoria contínua.

3. Apresentação Institucional

A Universidade Federal de Jataí (UFJ) é uma Instituição pública de ensino superior, organizada como Autarquia Federal e vinculada ao Ministério da Educação (MEC). Foi criada em 2018, pela Lei nº 13.635, de 20 de março, a partir do desmembramento da Universidade Federal de Goiás (UFG) e encontra-se inscrita no CNPJ/MF sob o nº 35.840.659/0001-30. Sua sede está situada no município de Jataí, na região sudoeste do estado de Goiás.

Dentro da sua estrutura organizacional da UFJ consta a existência da Secretaria de Tecnologia e Informação (SeTI).

A estrutura organizacional da SeTI é constituída da seguinte forma:

I. Conselho Consultivo Interno;

II. Direção;
III. Coordenação Administrativa;
IV. Coordenação de Suporte;
V. Coordenação de Telefonia e Cabeamento;
VI. Coordenação de Desenvolvimento;
VII. Coordenação de Infraestrutura de Redes;
VIII. Coordenação de TI de Dados Educacionais e Censo;
IX. Coordenação de Informação, Documentação e Arquivo; e
X. Coordenação do Setor de Protocolo e Arquivo.

São objetivos da SeTI:

I. Implementar a Política de Tecnologia da Informação (TI) da UFJ, aprovada pelo Conselho Universitário;
II. Administrar a infra-estrutura de TI da UFJ e, em particular, a rede de dados da UFJ, tanto no seu âmbito interno como externo;
III. Informatizar processos organizacionais da UFJ, de forma a promover uma execução eficaz e eficiente do trabalho da comunidade acadêmica;
IV. Projetar, desenvolver e manter sistemas computacionais corporativos de acordo com as necessidades da UFJ;
V. Elaborar e executar o seu planejamento estratégico de TI de forma a atender a política de TI da UFJ;
VI. Coordenar o processo de aquisição de produtos e serviços de TI na UFJ;
VII. Estudar, promover, implementar e divulgar novos recursos de Tecnologia da Informação que contribuam para a melhoria geral das atividades da UFJ; e
VIII. Assessorar e capacitar os colaboradores dos órgãos administrativos, das unidades acadêmicas e dos campi da UFJ no uso adequado de seus recursos de TI.

4. Aplicação

Este documento deve ser utilizado para tratar incidentes envolvendo todos serviços de TIC suportado pela SeTI, oferecidos para a comunidade acadêmica nos campi da Universidade Federal de Jataí (UFJ).

5. Definições e Termos

Data center: Ambiente que concentra os servidores institucionais, equipamentos de processamento e armazenamento de dados, ativos de TI, switches roteadores, sistemas de segurança como firewalls entre outros equipamentos.

Firewall: Solução de Segurança que monitora e controla o tráfego de rede a partir de um conjunto de regras estabelecidas. Um firewall pode ser baseado em hardware ou em software.

GLPI - (Gestão livre de parque de informação): É um sistema utilizado para chamados técnicos, esse sistema permite o acompanhamento de solicitações destinadas ao setor de tecnologia da informação.

TI: Tecnologia da Informação.

TIC: Tecnologia da informação e comunicação.

VM: (Virtual machine) máquina Virtual.

Incidente: Evento inesperado ou situação anormal que ocorre, causando danos leves ou graves aos equipamentos ou ao sistema de TI, ou qualquer evento que cause indisponibilidade ou falha nos ativos de TIC da instituição.

Ativos de TI: São todos componentes que instituem a infraestrutura de tecnologia da informação que são utilizados na UFJ.

RNP: Rede Nacional de Ensino e Pesquisa.

NOC: *Network Operation Center*, central de monitoramento de rede.

MTTR - (Mean Time To Recovery): Tempo médio para recuperação após uma falha.

MTTF - (Mean Time To Failure): Tempo médio entre falhas.

6. Relação dos serviços críticos oferecidos pela SeTI.

Dentre os diversos serviços oferecidos, destacam-se os considerados críticos, como a gestão do datacenter da UFJ, incluindo a manutenção de máquinas virtuais e gestão de servidores. A parada parcial ou total de determinados serviços, podem gerar perdas significativas de informações e prejuízos financeiros.

São considerados os serviços prioritários:

Serviços	Descrição
Data center	Condições para que os servidores sejam ativados para disponibilização de recursos hospedagem de serviços.
Conexão RNP	Disponibilidade de conexão a internet para o campus. Link de dados oferecido pela RNP.
Wifi	Acesso a rede wifi institucional (Eduroam).
SEI	Sistema Eletrônico de Informação.
Sistemas SIG	Gestão acadêmica e administrativa.
VM's Docker	4 VM's disponibilizadas para a equipe de desenvolvimento. Hospedagem de alguns serviços desenvolvidos na SeTI.
LDAP	Serviço que utiliza o protocolo LDAP que fornece base para autenticação do login único.
DNS	Sistema de resolução de nomes para internet. Permite que seja acessado os sistemas que estão no domínio ufj.edu.br.
Google Workspace	Serviços oferecidos pelo google. A exemplo o email institucional.

7. Principais Riscos

A gestão de riscos é fundamental para assegurar a continuidade dos serviços de TIC. Existem vários riscos a serem levados em consideração, porém existem aqueles que são críticos por possuírem sua probabilidade alta e um impacto significativo. A seguir é apresentado riscos de alta criticidade a que a infraestrutura de TI da UFJ está exposta.

Risco	Descrição	Contingenciamento
Interrupção de Energia Elétrica	Causado por fatores externos ou internos, falhas na rede elétrica do data center ou no prédio de distribuição.	Todos os equipamentos do datacenter deverão ser desligados imediatamente, a fim de evitar a queima de equipamentos e/ou a perda da integridade dos dados. Abertura de chamado para SeInfra.
Falha na climatização interna do data center	Problemas no equipamento, ou defeito acidental.	Manutenção preventiva e contenção de acesso às unidades que compõem o sistema de refrigeração do data center. Abertura de chamado para empresa Gemelo.
Incêndio na sala do data center	Incêndio interno e/ou externo à sala do data center.	Manutenção preventiva realizada por terceiros na verificação de central de incêndio.
Falha no link de dados da RNP.	Causado por rompimento de enlace de comunicação ou falha de equipamento.	Em caso de perda de comunicação, deve-se notificar imediatamente a RNP através de abertura de chamado.
Falha de conexão interna.	Problemas, relacionados a equipamento (switches), ou conexão física.	Monitoramento proativo dos switches pela equipe de infraestrutura - SeTI. Em caso de falhas não percebidas pelo monitoramento, deve-se informar à SeTI, através de chamado para ser verificada a situação.
Falha física de equipamentos (Servidores e ativos de rede) que dão suporte aos serviços críticos.	Causado por equipamentos antigos e/ou sem garantia/suporte.	Manter contratos de garantia e suporte quando possível. Realizar troca de equipamentos obsoletos sem garantia por novos que oferecem maior segurança de funcionamento.
Falhas humanas acidentais/imperícia	Erros operacionais ou imperícia técnica.	Disponibilizar privilégios mínimos, oferecer cursos de capacitação na área de atuação e não fornecer senhas de altos privilégios, como senhas root.
Ataques internos ou externos	Ameaças cibernéticas que exploram vulnerabilidades da rede institucional, gerando indisponibilidade de alguns serviços ou obtendo acesso não autorizado.	Atualizar sistemas críticos para aplicar correções de software. Monitorar observando eventos de logs de switches, servidores e até estações de trabalho, se assim for necessário.
Possíveis incidentes não identificados	Causado por não possuir pessoal suficiente e capacitado para monitorar e manter a estrutura física em conformidade às boas práticas e legislação vigente.	Procurar atualização profissional como capacitações na área de redes e contratação para suprir a deficiência do setor de tecnologia da informação.

Segue a matrix para o levantamento da criticidade dos riscos levando em consideração os seguintes critérios:

Probabilidade (P):

Baixa (1): Raro ou improvável de ocorrer.

Média (2): Pode ocorrer ocasionalmente.

Alta (3): Alta chance de ocorrência.

Impacto (I):

Baixo (1): Afeta levemente a operação, sem danos ou interrupções críticas.

Médio (2): Gera indisponibilidade parcial ou danos reversíveis.

Alto (3): Causa paralisação crítica, perda de dados ou danos irreversíveis.

Classificação:

1 – 2: Baixo; 3 – 4: Moderado; 6 – 9: Alto

Risco	Probabilidade (P)	Impacto (I)	Nível de Risco (PxI)	Classificação	Justificativa
Interrupção de Energia Elétrica	2	3	6	Alto	Pode ocorrer por fatores externos, e afeta diretamente a integridade dos dados e operação dos serviços críticos.
Falha na climatização interna do data center	2	3	6	Alto	O superaquecimento compromete a integridade de servidores e pode causar falhas em cascata.
Incêndio na sala do data center	1	3	3	Moderado	Pouco provável, mas com impacto catastrófico - exige sistema de detecção e supressão eficaz.
Falha no link de dados da RNP	2	2	4	Moderado	Pode causar indisponibilidade temporária de sistemas, mas geralmente há redundância ou mitigação rápida.
Falha de conexão interna	2	2	4	Moderado	Impacto localizado, recuperação geralmente rápida pela equipe técnica.

Falha física de equipamentos críticos	3	3	9	Alto	Alta probabilidade em equipamentos obsoletos, com impacto direto sobre serviços essenciais.
Falhas humanas acidentais/imperícia	3	2	6	Alto	Bastante comum, especialmente em ambientes sem controle de acesso e capacitação contínua.
Ataques internos ou externos	3	3	9	Alto	Muito prováveis e de alto impacto, exigem vigilância contínua e plano de resposta a incidentes.
Possíveis incidentes não identificados	2	3	6	Alto	Falta de pessoal e monitoramento eficaz aumenta o risco de falhas passarem despercebidas.

8. Objetivos de RTO e RPO por serviços críticos

Serviço/Sistema	RTO	RPO	Justificativa
Data center	3h	4h	Tempo necessário do processo de religar os equipamentos e inicialização dos serviços hospedados no Data Center afetando todos os serviços hospedados. Este tempo é considerado pensando em que os equipamentos estejam operacionais.
Conexão RNP	2h	2h	Quedas de link de dados da RNP.
Wifi	24h	24h	Tempo necessário para acionamento da equipe e reconfiguração dos equipamentos. O tempo pode aumentar dependendo da quantidade de Access Point e controladoras afetadas.
SEI	2h	2h	Tempo necessário para restabelecimento dos serviços, testes e correções acrescido a 1 hora de restabelecimento do data center afetando todo o peticionamento de processos.
Sistemas SIG	2h	2h	Recuperação dos sistemas SIGs, afetando a comunidade acadêmica e administrativa.
VM's Docker	4h	4h	Infraestrutura para equipe de desenvolvimento. Utilizada para sistemas da UFJ.
LDAP	2h	24h	Base utilizada em diversos sistemas para autenticação.
DNS	2h	24h	Tempo necessário para reconfiguração do serviço de DNS afetando a comunicação internas e externas.
Google Workspace	2h	2h	As contas institucionais de email funcionam pelo google workspace. Sendo esse um serviço que demanda tratativas com o próprio Google. Um RPO baixo se dá por conta da

9. Comunicação

Toda comunicação relacionada a riscos e/ou incidentes observados deve ser encaminhada às respectivas equipes responsáveis. A Matriz RACI de Riscos (item 9.4) define a divisão de responsabilidades e orienta sobre os fluxos de comunicação entre as equipes envolvidas.

9.1. A quem comunicar:

9.1.1. Coordenação de Infraestrutura - SeTI

No âmbito institucional, o setor de infraestrutura é responsável pela gestão dos equipamentos de conectividade de internet, tanto rede Wi-Fi e rede física, em ambos os campos, além de garantir a disponibilidade, atualização e o funcionamento contínuo de todas as máquinas virtuais hospedadas no data center da Instituição.

9.1.2. Coordenação de Desenvolvimento - SeTI

A equipe de desenvolvimento é responsável por gerenciar todos os sistemas institucionais desenvolvidos pela Secretaria de Tecnologia da Informação (SeTI). A coordenação de desenvolvimento também é incumbida de acionar os responsáveis pelo suporte a sistemas externos.

9.1.3. Coordenação de Manutenção e Suporte - SeTI

O suporte desempenha um papel essencial na instituição, sendo responsável pelo atendimento aos usuários e pela resolução de problemas técnicos relacionados a softwares, além de realizar a manutenção dos equipamentos ligados à TI institucional, garantindo seu perfeito funcionamento.

9.1.4. Coordenação de Telefonia e Cabeamento Estruturado - SeTI

A equipe de telefonia e cabeamento estruturado é responsável pela ampliação, manutenção e gestão do cabeamento estruturado e telefonia que torna possível a disponibilidade de conexão inter *campi*. Também faz a gestão de racks das salas técnicas dos blocos da instituição.

9.1.5. Equipe de Prevenção, Tratamento e Resposta a Incidentes de Cibernéticos - Etir.

A equipe Etir foi instituída na UFJ pela portaria 1392/2024 - UFJ de 19 de Dezembro de 2024. Trata-se de uma equipe para tratamento e respostas a incidentes cibernéticos.

9.1.6. Secretaria de Infraestrutura (SeInfra).

A SEINFRA é um órgão que mantém no âmbito da Universidade Federal de Jataí a coordenação das ações relativas à implantação, manutenção e ampliação da infraestrutura, a exemplo a energia elétrica.

9.1.7. Rede Nacional de Ensino e Pesquisa (RNP).

A RNP é responsável por fornecer conexão de alta velocidade para ensino e pesquisa em todo território nacional. A UFJ utiliza esse link para poder disponibilizar acesso a internet e serviços que são disponibilizados através deste convênio.

9.1.8. Gemelo do Brasil data centers.

A atual empresa que possui contrato com a UFJ para manutenções preventivas realizadas na parte física do data center mensalmente, como sistema de refrigeração e combate a incêndio e mantém monitoramento de funcionamento com um NOC 24/7.

9.2. Como comunicar:

A comunicação deve ser realizada por meio de e-mails para cada equipe responsável. É fundamental que a comunicação esteja de forma clara e com a maior riqueza possível de detalhes, indicando os seguintes itens como consta no seguinte modelo:

Data e hora do incidente: *Quando ocorreu o incidente.*

Local/sistema afetado: *Qual ambiente, aplicação, serviço ou infraestrutura que foi impactada.*

Descrição do incidente: *Relato com a maior riqueza de detalhes possível.*

Equipe responsável: *Para qual equipe deve ser direcionada comunicação*

Remetente: *Nome da pessoa ou equipe que está fazendo o relato.*

Equipe		E-MAIL
SeTI	Coordenação de Infraestrutura	redes.seti@ufj.edu.br
	Coordenação de Desenvolvimento	desenvolvimento.seti@ufj.edu.br
	Coordenação de Manutenção e Suporte	suporte.seti@ufj.edu.br
	Coordenação de Telefonia e Cabeamento Estruturado	telecomunicacoes.seti@ufj.edu.br
Etir		etir@ufj.edu.br
SeInfra		seinfra@ufj.edu.br
RNP		atendimento@rnp.br
GEMELO		https://new.infraspeak.com/login

9.3. Matriz RACI de riscos:

Risco	Atividade Principal	Infraestrutura	Suporte	Desenvolvimento	Telefonia	Etir	SeInfra	RNP	Gemelo	Gestão SeTI
Interrupção de Energia Elétrica	Abertura de chamado para SeInfra	R				I	A	I	I	I
	Manutenção preventiva em sistemas de distribuição, Ex.: Gerador	I					R			I
Falha na Climatização do Data Center	Abertura de chamado para Gemelo	R				I			A	I
Incêndio na Sala do Data Center	Ação inicial e notificação	R					I		A	I
	Manutenção preventiva contratada	A							R	A
Falha no Link de Dados da RNP	Diagnóstico e abertura de chamado e comunicação com a Secom	R				I		A		I
	Comunicação com operadora para reparo	I						R		I
Falha de Conexão Interna (Switches)	Diagnóstico e correção	R	C		C	I				I
Falha Física de Equipamentos (Servidores)	Monitoramento e correção de vulnerabilidades	R	C	C	C	I				A
	Atualização de inventário e análise de causas	R								A
Falha Humana/Imperícia	Adoção de boas práticas e controle de acesso	R	R	R	R					A
	Capacitação contínua	C	C	C	C					R
Ataques Internos ou Externos	Monitoramento e correção de vulnerabilidades	R	C	C		C				A
	Atualizações de segurança	R	C	R		C				A
Possíveis Incidentes Não Identificados	Contratação e capacitação de equipe	C	C	C	C	C				R
	Reforço de monitoramento e auditorias	R	R	R						I

9.4. Quem deve comunicar:

A comunicação deve ser acessível a qualquer servidor ou partícipe que detectou o problema ou a falha que possa levar ao incidente.

9.5. Capacitação e Atualização Técnica.

Para um contingenciamento eficaz de riscos, com o objetivo de alcançar maiores níveis de maturidade e previsibilidade nos resultados, é essencial manter a constante atualização técnica e o treinamento contínuo do pessoal. Além disso, a modernização dos equipamentos é igualmente necessária, devendo ocorrer em conjunto com treinamentos oferecidos pelas empresas fornecedoras.

O plano de capacitação deve ser executado sempre que houver disponibilidade orçamentária do órgão ou instituição, aproveitando oportunidades oferecidas por plataformas parceiras, como a Escola Superior de Redes (ESR), a Escola Nacional de Administração Pública (ENAP) ou por meio de treinamentos especializados promovidos por entidades certificadoras e instituições de formação profissional.

10. Mecanismo de Gestão e Governança do Plano

Na estrutura definida para a UFJ é criado o Comitê Estratégico de Governança, Riscos e Controles (CGRC), tendo suas atribuições regidas pela portaria Nº 134/2025, de 20 de fevereiro de 2025. Cabe o destaque para a "absorção" das competências relativas ao Comitê de Governança Digital que desempenha o papel crucial para a gestão do plano. Conforme segue no **Art. 2 da portaria 134/2025.**

> XVIII - Incentivar e apoiar a concretização dos princípios estabelecidos pela *Estratégia Federal de Governo Digital, absorvendo as competências do Comitê de Governança Digital, no que se refere à aprovação dos seguintes instrumentos de planejamento:*
>
> *a) Plano de Transformação Digital;*

b) Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC); e

c) Plano de Dados Abertos (PDA).

Como esse plano faz parte de documentos suplementares ao PDTI, é englobado na gestão e apreciação do CGRC.

11. Indicadores de Desempenho e monitoramento

Para garantir a eficiência e avanço na maturidade de um plano consolidado, será considerado o uso de métricas como disponibilidade dos serviços considerados críticos para a UFJ. É apresentado o relatório sobre a indisponibilidade de conexão para os campus Riachuelo e Jatobá. Esse levantamento está registrado desde dezembro de 2024 para fins de indicadores e desempenho.

Foi escolhido o link de conexão, pois através dele que se dá a disponibilidade para ambientes externos ao campus Jatobá, bem como acesso a internet e wifi, sendo todos os sistemas dependentes do link. Nesse período não foram registrados incidentes para os demais sistemas críticos.

Diante dos dados brutos apresentados abaixo, chegamos nos seguintes números de MTTR para queda de link no serviço “Conexão RNP”:

Campus	MTTR
Riachuelo	11:09:00
Jatobá	42:46:00

Tabela de incidentes de disponibilidade de Conexão RNP:

Data	Campus	Horário			
		Inicial	Final	Data Final	Duração
03/12/2024	Jatobá	17:30	16:00	04/12/2024	22:30:00
15/12/2024	Jatobá	21:00	14:11	16/12/2024	17:11:00
03/01/2025	Jatobá	18:00	19:10	06/01/2025	73:10:00
10/01/2025	Riachuelo	08:00	19:00	10/01/2025	11:00:00
25/01/2025	Riachuelo	11:00	14:30	25/01/2025	3:30:00

21/02/2025	Jatobá	16:30	21:00	24/02/2025	76:30:00
05/03/2025	Jatobá	20:31	21:00	06/03/2025	24:29:00
24/04/2025	Riachuelo	15:25	10:50	25/04/2025	19:25:00
20/05/2025	Riachuelo	19:40	12:30	21/05/2025	16:50:00
27/05/2025	Riachuelo	12:40	17:40	27/05/2025	5:00:00

11.1. Revisão e testes

A revisão deste documento deverá ser realizada periodicamente, no prazo máximo de um ano. No período de revisão, será levado em consideração os novos valores de incidentes registrados.

A atualização em momentos ordinários, como exemplo após um incidente ou mudanças relevantes de acordo com legislação aplicável.

Também será mantido um histórico de versão para acompanhar a evolução do plano, sendo essa inicial para futuros riscos e novos procedimentos a serem adotados.

11.2. Simulação e testes de Disaster Recovery (DR)

Para a devida manutenção do plano, é fundamental que ocorram simulações periódicas e registros de possíveis melhorias no plano. Essas simulações se dão pelo restabelecimento de serviços críticos, ainda que estejam em funcionamento. Por meio desses testes, torna-se possível identificar necessidades específicas, validar a integridade dos fluxos e verificar a consistência das informações necessárias para a reconstrução dos serviços em um ambiente alternativo.

Recomenda-se que essa simulação tenha periodicidade semestral, sem prejuízo de execuções em intervalos menores, conforme a criticidade dos serviços ou necessidades identificadas.

12. Considerações finais

O plano de contingência da UFJ foi elaborado com o objetivo de orientar, reunir informações, procedimentos a serem tomados no caso de incidentes de TIC que possam comprometer serviços considerados críticos.

Também tem como objetivo a mitigação de impactos gerados por possíveis incidentes. Todavia sua implementação e sucesso depende do engajamento das equipes envolvidas e responsáveis na adoção do plano como padrão.

13. Referências

INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021 -

Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
Disponível em:
https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172

PORTARIA Nº 134/2025 UFJ, DE 20 DE fevereiro DE 2025

…normatiza as atribuições e funcionamento do Comitê Estratégico de Governança, Riscos e Controles da Universidade Federal de Jataí e dá outras providências.

RESOLUÇÃO CONSUNI/UFJ Nº 015/2025, DE 07 DE MAIO DE 2025.

Dispõe sobre a Política de Governança, Riscos e Controles Internos da Universidade Federal de Jataí.

Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD)

Disponível em:
https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

DECRETO Nº 12.198, DE 24 DE SETEMBRO DE 2024

Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.
Disponível em:
https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2024/Decreto/D12198.ht

m#art9:~:text=DECRETO%20N%C2%BA%2012.198%2C%20DE%2024%20DE%20SETEMBRO%20DE%202024

DECRETO Nº 10.748, DE 16 DE JULHO DE 2021

Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm

INSTRUÇÃO NORMATIVA Nº 2, DE 24 de JULHO DE 2020

Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

Disponível em:

https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700

INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019

Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

Disponível em:

https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/instrucao-normativa-sgd-me-no-1-de-4-de-abril-de-2019#:~:text=INSTRU%C3%87%C3%83O%20NORMATIVA%20N%C2%BA%201%2C%20DE%204%20DE%20ABRIL%20DE%202019&text=Disp%C3%B5e%20sobre%20o%20processo%20de,SISP%20do%20Poder%20Executivo%20Federal.