**Ministério da Educação**
**Secretaria de Educação Profissional e Tecnológica**
**Instituto Federal de Educação, Ciência e Tecnologia Baiano**
**Órgão de Assessoramento - Comitê de Governança Digital**

# PORTARIA 3/2025 - OA-CGD/IFBAIANO, de 26 de novembro de 2025

**O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL,** no uso de suas atribuições legais previstas no artigo 6º do Regimento Interno do Comitê de Governança Digital, e, considerando:

- o teor do Processo nº 23327.251891.2025-40; e

- a deliberação dos membros do CGD, em sua 3ª Reunião Extraordin ária, realizada em 19.11.2025.

**RESOLVE:**

Art. 1º Aprovar o Plano de Continuidade de Negócio de Tecnologia da Informação do IF Baiano, conforme documento anexo.

Art. 2º Esta Portaria entra em vigor nesta data.

Marcelito Trindade Almeida

Presidente

Documento assinado eletronicamente por:

- **Marcelito Trindade Almeida**, **DIRETOR(A) EXECUTIVO(A) - CD3 - RET-DIREX**, em 26/11/2025 08:35:12.

Este documento foi emitido pelo SUAP em 19/11/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

**Código Verificador:** 775456
**Código de Autenticação:** d521b4019d

Rua do Rouxinol, 115, Imbuí, Salvador / BA, CEP 41720-052
Fone: None

# Plano de Continuidade de Negócio de Tecnologia da Informação

# Termos e Abreviações

| | |
|---|---|
| ASCOM | Assessoria de Comunicação |
| CGD | Comitê de Governança Digital |
| CSIC | Comissão de Segurança da Informação e Comunicação |
| CONSUP | Conselho Superior do IF Baiano |
| DGTI | Diretor da Gestão da Tecnologia da Informação |
| DICOM | Diretoria de Comunicação |
| IF Baiano | Instituto Federal de Educação, Ciência e Tecnologia Baiano |
| NGTI | Núcleo de Gestão de Tecnologia da Informação (Campi) |
| PCA | Plano de Administração de Crises |
| PCN de TI | Plano de Continuidade de Negócio de TI |
| PCO | Plano de Continuidade Operacional |
| PDR | Plano de Recuperação de Desastres |
| PoSIN | Política de Segurança da Informação |
| RPO | Objetivo de Ponto de Recuperação |
| RTO | Objetivo de Tempo de Recuperação |
| TI | Tecnologia da Informação |

# Sumário

# 1. Apresentação

A TI desempenha um papel fundamental na prestação de serviços educacionais e administrativos, e a interrupção desses serviços pode impactar significativamente a capacidade do IF Baiano de cumprir sua missão institucional.

Com isso em mente, o PCN de TI foi desenvolvido com o objetivo de estabelecer medidas eficientes para garantir a continuidade dos processos críticos de TI, especialmente aqueles relacionados aos sistemas essenciais, em casos de incidentes graves ou desastres.

A implementação deste plano busca minimizar o tempo de inatividade e assegurar que as operações possam ser retomadas com a máxima eficiência e o menor impacto possível para a comunidade acadêmica e administrativa. Tendo o compromisso com a educação de qualidade e a excelência nos serviços prestados.

# 2. Abrangência

O PCN de TI do IF Baiano, abrange os seguintes aspectos:

1. **Sistemas críticos de TI**:
    - O plano abrange todos os sistemas essenciais que suportam as operações acadêmicas e administrativas, como sistemas de gestão acadêmica, plataformas de ensino a distância, sistemas financeiros e de recursos humanos.
2. **Infraestrutura de TI**:
    - Inclui a infraestrutura física e virtual necessária para a operação dos sistemas de TI, como servidores, redes, data centers e sistemas de armazenamento.
3. **Processos de negócio**:
    - Engloba processos críticos que dependem de sistemas de TI para garantir a continuidade das operações institucionais, como matrículas, registros acadêmicos, processamento de pagamentos e comunicação interna.

4. **Gestão de incidentes e desastres**:
    - O plano estabelece procedimentos para responder a incidentes que possam causar interrupções nos serviços de TI, incluindo desastres naturais, falhas técnicas e ataques cibernéticos.
5. **Recuperação de desastres**:
    - Define estratégias para a recuperação rápida e eficaz das operações de TI, com foco na minimização do tempo de inatividade e na proteção dos dados institucionais.
6. **Segurança da informação**:
    - Abrange medidas para proteger a confidencialidade, integridade e disponibilidade das informações, incluindo controles de acesso, criptografia e políticas de segurança.
7. **Comunicação e coordenação**:
    - Estabelece canais de comunicação e coordenação entre as equipes de TI, administração do IF Baiano e outras partes interessadas para garantir uma resposta coesa e eficiente a incidentes.
8. **Treinamento e capacitação**:
    - Inclui programas de treinamento para preparar as equipes de TI e outros funcionários para atuar conforme o plano, garantindo que todos saibam seus papéis e responsabilidades em situações de emergência.
9. **Revisão e atualização**:
    - O plano deve ser revisado e atualizado regularmente para refletir mudanças nos sistemas, infraestrutura e riscos identificados, garantindo que permaneça relevante e eficaz.

## 3. Objetivos

1. **Garantir a disponibilidade dos sistemas críticos**:
    - Assegurar que os sistemas e serviços de TI essenciais estejam sempre disponíveis ou sejam rapidamente restaurados em caso de interrupção, minimizando o impacto nas operações acadêmicas e administrativas.

2. **Proteger a integridade e segurança da informação**:
    - Implementar medidas eficazes para proteger os dados institucionais contra perda, corrupção ou acesso não autorizado, garantindo a confidencialidade, integridade e disponibilidade das informações.
3. **Assegurar uma resposta eficaz a incidentes e desastres**:
    - Estabelecer procedimentos claros e treinamentos regulares para preparar as equipes de TI e outras partes interessadas a responder rapidamente a incidentes e desastres, facilitando uma recuperação eficiente e reduzindo o tempo de inatividade.

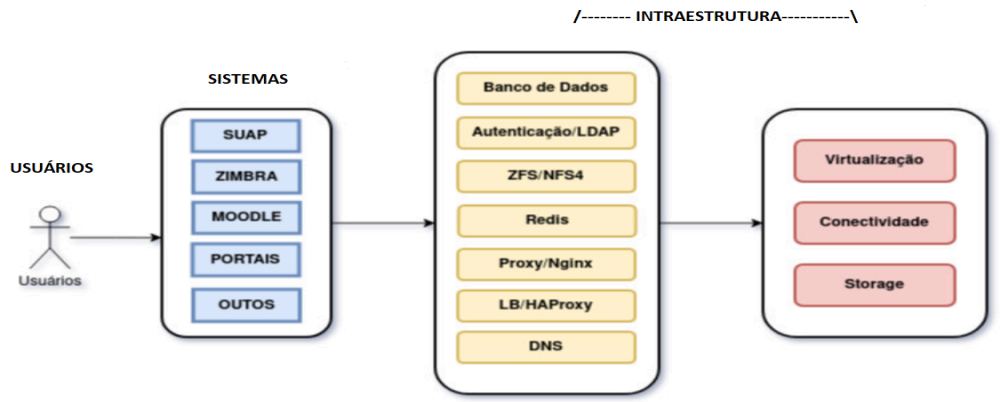
## 4. Serviços Essenciais

Os seguintes serviços são considerados essenciais para a ativação e execução deste plano.

| Serviço | Criticidade | RPO[1] | RTO[2] | Impacto | | | |
|---|---|---|---|---|---|---|---|
| | | | | Financeiro | Legal | Imagem | Operacional |
| CAU | Alta | 24 | 24 | Médio | Médio | Alto | Alto |
| SUAP | Alta | 24 | 24 | Alto | Alto | Alto | Alto |
| E-mail institucional / Webmail | Alta | 6 Meses | 24 | Baixo | Médio | Alto | Alto |
| Links de Internet | Alta | – | | Alto | Médio | Alto | Alto |
| Moodle | Média | 24 | 24 | Médio | Médio | Alto | Médio |
| Biblioteca Digital | Baixa | – | 72 | Baixo | Baixo | Médio | Baixo |
| Pergamum | Baixa | 24 | 72 | Baixo | Baixo | Médio | Baixo |
| Wiki | Baixa | 24 | 72 | Baixo | Baixo | Baixo | Baixo |
| TelefoneIP | Baixa | – | | Médio | Baixo | Médio | Médio |
| SIGA ADM | Média | 24 | 24 | Médio | Médio | Médio | Médio |
| SIGA Protocolo | Baixa | 24 | 72 | Baixo | Médio | Médio | Baixo |
| SGC | Alta | 24 | 24 | Médio | Alto | Alto | Alto |
| Website/Portais | Alta | 24 | 24 | Médio | Médio | Alto | Alto |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Helios | Baixa | 24 | 72 | Baixo | Baixo | Médio | Baixo |
| SIPPAG | Alta | 24 | 24 | Alto | Alto | Alto | Alto |
| Diploma Digital | Alta | 24 | 24 | Médio | Alto | Alto | Alto |
| Dspace | Média | 24 | 24 | Médio | Médio | Médio | Médio |
| OJS | Média | 24 | 24 | Baixo | Médio | Médio | Médio |

1 RPO - tolerância a perdas de sua empresa em relação aos dados.
2 RTO - tempo máximo em que um sistema ou informação pode ficar indisponível depois de um desastre.
Atenção 1: As rotinas de backup são executade 24h durante a semana (Segunda à Sexta) e 72h nos finais de semana
Atenção 2: A infraestrutura que sustenta os sistemas é responsável por garantir seu pleno funcionamento. Assim, quaisquer incidentes nessa infraestrutura podem comprometer a continuidade e a operação adequada dos sistemas, conforme ilustrado no esquema a seguir.




## 5. Principais Ameaças

Este plano deve ser ativado em situações de desastres que ameaçam a continuidade dos serviços essenciais.

| **Evento de Desastre** | **Possíveis Causas** |
|---|---|
| Interrupção de energia elétrica | Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas |
| | Causada por fator interno que compromete a rede elétrica do prédio com curto-circuito, incêndios e infiltrações. |
| Falha na climatização do Data Center | Superaquecimento dos ativos devido a sobrecargas, curtos-circuitos ou outros problemas na infraestrutura elétrica |
| | Quebra ou mau funcionamento dos sistemas de ar condicionado. |
| | Mau funcionamento nos sistemas de controle |

| | |
|---|---|
| | automatizado que regulam a temperatura e umidade, levando a falhas na operação. |
| Interrupção nos circuitos de rede | Danos aos cabos de fibra óptica ou infraestrutura devido a obras de construção, roedores, acidentes ou desastres naturais. |
| | Defeitos em roteadores, switches, cabos de rede ou outros equipamentos de infraestrutura. |
| | Interferência eletromagnética ou física nos cabos de rede pode causar degradação ou perda de sinal. |
| Ataques internos | Ataque aos ativos do Data Center ou aos servidores internos. |
| Falha de hardware | Falha que necessite de reposição de peça ou cujo reparo ou aquisição dependa de processo de aquisição e orçamento. |
| Ataques Cibernéticos | Acesso não autorizado ou ataques direcionados podem comprometer os circuitos de rede, causando interrupções. |
| Falhas em Provedores de Serviço | Problemas nos serviços dos provedores de internet ou telecomunicações podem afetar os circuitos de rede externos. |
| Falhas na Atualização de Sistemas | Falha devido a erros de instalação, corrupção de arquivos ou interrupções durante a atualização. |
| Incompatibilidades de Software | Atualizações que podem introduzir incompatibilidades com o hardware existente ou com outros softwares em uso. |
| Falha humana | Qualquer ato causado por negligência, imprudência e/ou imperícia. |
| Problemas Ambientais | Temperaturas extremas ou umidade podem afetar o funcionamento dos equipamentos de rede, levando a falhas. |

# 6. Papéis e Responsabilidades

O objetivo é minimizar os impactos e garantir que os serviços de TI mais críticos permaneçam disponíveis ou sejam restabelecidos o mais rápido possível.

## 6.1. CGD

- Aprovar o plano de continuidade de negócio de TI.
- Avaliar e aprovar as políticas, procedimentos e práticas de continuidade.

- Aprovar as revisões periódicas do plano para garantir que ele esteja atualizado e eficaz.
- Liderar a resposta em caso de uma interrupção significativa dos serviços de TI.

6.2. DGTI / NGTIs (Campi)

- Supervisionar a manutenção do plano de continuidade.
- Garantir que todos os ativos de TI críticos sejam identificados e incluídos no plano.
- Coordenar testes regulares do plano de continuidade.
- Manter a comunicação com outras áreas da instituição/campus durante um evento de continuidade.
- Assegurar a recuperação dos sistemas de TI conforme planejado.
- Gerir a comunicação durante crises e desastres, mantendo informados todos os públicos relevantes.
- Atualizar regularmente o status da continuidade dos serviços para os usuários e outras partes interessadas.
- Assegurar que a informação divulgada seja precisa e consistente com o plano de continuidade.

6.3. Equipe de TI

- Implementar as ações previstas no plano de continuidade.
- Realizar backups regulares dos dados críticos e garantir que esses backups sejam armazenados de maneira segura.
- Monitorar os sistemas de TI para detecção precoce de falhas que possam desencadear a ativação do plano.
- Participar de treinamentos e exercícios para garantir a prontidão em caso de incidentes.
- Executar procedimentos de recuperação e restabelecimento de serviços conforme necessário.

6.4. Reitor / Diretor Geral

- Apoiar a implementação do plano de continuidade de TI.

- Garantir recursos financeiros e logísticos para a continuidade dos serviços de TI.
- Tomar decisões estratégicas durante incidentes críticos.

6.5. Usuários Finais (Servidores, Docentes, Estudantes)

- Seguir as diretrizes de continuidade definidas pelo plano.
- Relatar quaisquer problemas ou incidentes à equipe de TI prontamente.
- Participar de treinamentos e atividades de conscientização sobre continuidade de serviços.
- Colaborar com as equipes de TI durante os eventos de recuperação.

6.6. Fornecedores de Serviços e Parceiros Externos e Visitantes.

- Assegurar que os serviços fornecidos estejam de acordo com os requisitos de continuidade do IF Baiano.
- Colaborar no processo de recuperação em caso de falhas ou interrupções.
- Manter contratos e SLAs (Service Level Agreements) que incluam cláusulas de continuidade de negócios.

## 7 - Invocação do Plano

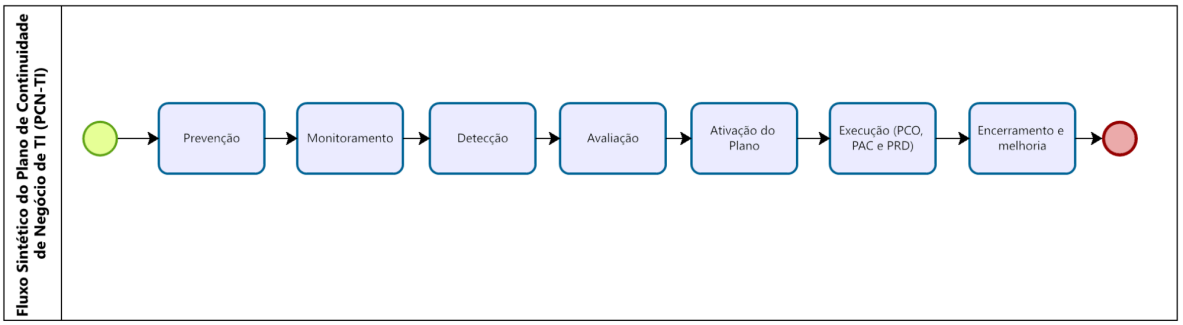
Este plano será acionado em caso de ocorrência de desastres, surgimento ou detecção de um risco, ou na hipótese de uma vulnerabilidade com alta probabilidade de exploração. Além disso, o plano poderá ser ativado em situações de testes ou por decisão conjunta do CGD e da alta administração do IF Baiano.

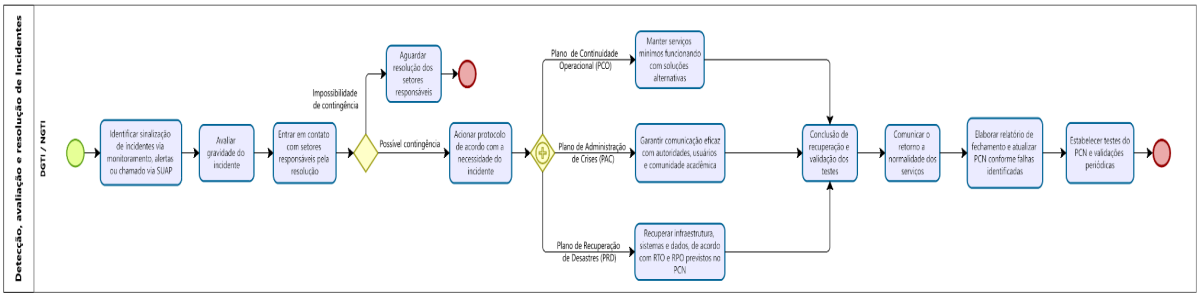
Os servidores do IF Baiano terão a responsabilidade de acionar os contatos e partes interessadas, preferencialmente por telefone ou pessoalmente, sempre que for necessário, diante das ameaças previstas neste plano.

## 8 - Macroprocessos

A seguir, apresentam-se o fluxo do PCN de TI e o metaprocesso de detecção, avaliação e resolução de incidentes. Nos anexos, encontram-se descritos os detalhes desses processos, bem como o metaprocesso de prevenção e mitigação

de erros, com o objetivo de demonstrar a estrutura metodológica adotada para assegurar a continuidade operacional dos sistemas de TI.




# 9 - Estratégias de Prevenção

A Estratégia de Prevenção visa minimizar a probabilidade de ocorrências que possam causar interrupções nos serviços de TI e, em caso de incidentes inevitáveis, reduzir os impactos negativos sobre as operações essenciais da instituição.

## 9.1. Identificação e Análise de Riscos

Realizar levantamentos periódicos, conforme Anexo I, para identificar potenciais ameaças aos sistemas de TI, incluindo riscos físicos (incêndios, inundações), cibernéticos (ataques de malware, hacking), e operacionais (falhas de hardware, erro humano).

Classificar os riscos com base na sua probabilidade de ocorrência e impacto, conforme a Política de Gestão de Riscos* do Instituto, priorizando aqueles que representam maior ameaça às operações críticas do IF Baiano.

* Política de Gestão de Riscos (https://ifbaiano.edu.br/portal/wp-content/uploads/2019/03/Resolu%C3%A7ao-n.-62.pdf)

9.2. Medidas de Proteção e Segurança

Segurança Física: Implementar controles de acesso físico aos data centers e áreas de TI, como uso de câmeras de vigilância, crachás de identificação e monitoramento, se necessário.

Segurança da Informação: Adotar práticas robustas de segurança cibernética, incluindo firewalls, sistemas de detecção de intrusão, criptografia de dados, políticas de senha forte e acesso com duplo fator de segurança, conforme Política de Segurança de TI do Instituto.

Manutenção Preventiva: Realizar manutenção regular em equipamentos e infraestrutura de TI para prevenir falhas inesperadas, garantindo que todos os sistemas estejam atualizados e operando corretamente.

9.3. Backup e Recuperação de Dados

Backups Regulares: Estabelecer uma política de backup frequente, com cópias de segurança armazenadas em locais diferentes, incluindo opções fora do local físico (off-site) para proteção contra desastres locais.

Testes de Recuperação: Realizar testes periódicos de recuperação de backups para assegurar que os dados possam ser restaurados de forma rápida e eficiente em caso de falha ou perda de dados.

9.4. Redundância e Alta Disponibilidade

Implementar soluções de redundância para sistemas e componentes críticos, como servidores, discos de armazenamento e conexões de rede, de modo que falhas individuais não interrompam as operações.

Adotar práticas de alta disponibilidade, incluindo balanceamento de carga e clusters de servidores, para garantir que os serviços permaneçam acessíveis mesmo sob condições adversas.

9.5. Capacitação e Conscientização

Treinamento Regular: Promover treinamentos periódicos para os servidores sobre procedimentos de segurança, melhores práticas em TI e respostas a incidentes.

Simulações de Incidentes: Realizar exercícios e simulações de incidentes de continuidade de negócios para testar a prontidão da equipe e identificar possíveis melhorias nos planos e processos.

9.6. Monitoramento Contínuo

Monitoramento Proativo: Utilizar ferramentas de monitoramento contínuo para detectar anomalias, atividades suspeitas ou falhas em tempo real, permitindo ações rápidas antes que ocorram interrupções.

Relatórios e revisões: manter um plano regular para rever a conformidade com as políticas de segurança e continuidade, gerando relatórios que apoiem a melhoria contínua dos processos.

9.7. Planos de Contingência

A estratégia de continuidade para o cenário atual da TI e serviços essenciais do Instituto, está estabelecida da seguinte forma:

TIPO : Warm Computing Site ou parcialmente Hot Computing Site com espelhamento, porém no mesmo local.

DESCRIÇÃO:
As cópias de backup dos sistemas essenciais do IF Baiano são armazenadas em um cofre localizado no prédio distinto da Reitoria. A criação de um site de backup remoto é crucial para garantir a continuidade dos serviços em caso de desastres, que está em desenvolvimento pela equipe de TI.

A reitoria do IF Baiano possui um  redundante, mas que no momento não funciona como contingência. Essa estrutura alternativa atua como uma possível via de contingência, permitindo que os serviços permaneçam operacionais mesmo diante de interrupções, aumentando a disponibilidade e a resiliência da rede.

● Nuvem
○ A computação em nuvem possibilita o armazenamento externo de dados em locais com infraestrutura de datacenter. A DGTI vem analisando a viabilidade desse serviço com cautela e responsabilidade, considerando os aspectos técnicos e administrativos envolvidos.

○ Pode-se evoluir para um Hotsite como estratégia de contratação.

Situação dos campi:

○ Cada campus possui uma realidade específica e uma configuração local distinta, que variam conforme a gestão local, adaptando-se às necessidades e particularidades de seu contexto.

AÇÕES DE CONTINGÊNCIA/RECUPERAÇÃO:
Mapear perda de dados e ativos, restabelecer toda a estrutura afetada e, após o ambiente principal estar operacional, prover a recuperação dos dados em backups.

OBSERVAÇÕES:

As ações de contingência e recuperação são detalhadas nos subplanos a seguir.

## 10 - Plano de Continuidade Operacional (PCO)

Este plano detalha cenários de inoperância e os procedimentos alternativos planejados para cada incidente, estabelecendo atividades prioritárias que garantam a continuidade dos serviços essenciais.

OBJETIVO E ESCOPO

O objetivo deste plano é assegurar medidas de continuidade durante e após uma crise ou desastre, focando exclusivamente nas ações de contingência delineadas na estratégia.

Objetivos do PCO:

- Garantir a manutenção e o funcionamento dos principais serviços de TI, assegurando a continuidade das operações e dos sistemas essenciais da instituição.
- Definir procedimentos, controles e regras alternativas que permitam a continuidade das operações de TI em situações de crise ou desastre.
- Estabelecer equipes dedicadas à execução dos planos PCO, PRD e PAC.
- Definir os formulários, check lists e relatórios necessários para que as equipes realizem as ações de contingência de maneira eficaz e organizada.

GESTÃO

A DGTI/NGTI é a diretoria/coordenadoria responsável por implementar, manter e melhorar o PCO e documentação inerente.

EXECUÇÃO DO PLANO

**Avaliação de Impacto de Desastre**

Ao identificar a ocorrência de um incidente ou crise, a equipe de operação de TI deve avaliar cuidadosamente a extensão do impacto, a abrangência da situação e os possíveis desdobramentos e divulgar a informação a todas as equipes envolvidas e ao Reitor/Diretor-Geral do Campus.

**Acionamento do Plano**

O plano deve ser acionado pela equipe de TI que também deverá dedicar atenção ao PRD e PAC com o objetivo de:

- Coordenar prazos e organizar as ações de contingência.
- Informar as equipes sobre as ações de contingência, com foco na priorização dos serviços essenciais.

**Ações de Contingência**

Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial.

| Id | Instrução | Duração | Observação | Resultado |
|---|---|---|---|---|
| 1 | Verificar status da aplicação de backup e estimar impacto de perda dados (janela) | | | |
| 2 | Identificar jobs de backup cujos dados em questão foram afetados | | | |
| 3 | Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais | | | |
| 4 | Atestar retorno do funcionamento do ambiente principal com a equipe de TI | | | |
| 5 | Teste de aplicação de backup após desastre | | | |
| 6 | Validar políticas de backup implementadas | | | |

ENCERRAMENTO DO PCO

Uma vez validados o funcionamento do retorno dos sistemas essenciais e a estabilidade do datacenter, deverá ser emitido um parecer relatando as atividades realizadas neste PCO. O Diretor/Coordenador na Reitoria/Campi informará à gestão o retorno das atividades.

# 11 - Plano de Administração de Crises (PCA)

Este plano define as ações a serem tomadas diante de cenários de desastre, abrangendo a gestão, administração, mitigação ou neutralização dos impactos. Ele se concentra na coordenação das atividades e na manutenção de uma comunicação eficaz entre todos os agentes envolvidos e/ou afetados, até a completa superação da crise.

OBJETIVO

O objetivo deste plano é assegurar uma comunicação eficaz, gerenciar as crises e proporcionar uma compreensão clara e consistente para todos os envolvidos sobre as ações a serem tomadas antes, durante e após uma catástrofe.

- Reduzir ao máximo os efeitos negativos causados pelo desastre, preservando a integridade das pessoas, das operações e dos recursos.
- Implementar ações imediatas para enfrentar a crise, garantindo que todas as partes envolvidas saibam seus papéis e responsabilidades.
- Estabelecer canais de comunicação claros e constantes entre todos os agentes, garantindo o fluxo de informações corretas e em tempo real.
- Conduzir ações para restabelecer as operações ao seu estado normal no menor tempo possível.
- Registrar todas as ações e decisões tomadas, para que possam ser analisadas e melhoradas em futuras situações.

EXECUÇÃO DO PLANO

Comunicação na ocorrência de um Desastre

Na ocorrência de um desastre será necessário entrar em contato com a gestão máxima e com a gestão administrativa e principalmente com as áreas afetadas para informá-las de seu efeito na continuidade dos serviços e no tempo de recuperação. A equipe responsável pela área afetada terá a incumbência de contatar estas unidades e passar as informações pertinentes em relação ao ocorrido.

A interação com cada parte será conduzida da seguinte forma:

● Comunicar às autoridades

A equipe responsável pela unidade afetada, ou aquela indicada pela autoridade máxima, terá como prioridade notificar as autoridades competentes sobre o ocorrido (desastre ou catástrofe), especialmente se houver risco às pessoas, fornecendo informações sobre a localização, natureza, magnitude e impacto do evento.

- ☐ Samu: 192
- ☐ Corpo de Bombeiros: 193
- ☐ Coelba: 0800-71-0800
- ☐ Polícia Militar: 190
- ☐ Defesa Civil: 199
- ☐ Polícia Civil: 197
- ☐ Polícia Federal: (77) 3420-8224
- ☐ Polícia Rodoviária Federal: (77) 3424-3529 / 3422-7885
- ☐ Ibama: 0800-61-8080

● Comunicação após um Desastre

Após análise do PRD e do PCO, a equipe da unidade afetada irá elaborar um breve plano de ação para manter as partes envolvidas e afetadas devidamente informadas. O objetivo é garantir que todos compreendam a perspectiva dos esforços necessários para o restabelecimento dos serviços atualmente inativos.

● Comunicação com os servidores e prestadores de serviços

A unidade afetada deverá prover um meio de contato específico para este fim, com intuito de que as unidades do IF Baiano se mantenham informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI.

Números de contatos a serem disponibilizados:
Telefone: (71) :
Contatos de E-mail:
Central de Serviços (service desk):
*Caso não haja conectividade ou linha telefônica disponível,

ceder essas informações por meio de publicações, ou outra estratégia definida no momento.

● Comunicar com estudantes e colaboradores externos

A DICOM ou ASCOM (campi), em alinhamento com o Reitor/Diretor-Geral e o Diretor de TI, deverá fornecer informações relevantes aos estudantes e colaboradores externos. O objetivo é informar o ocorrido e o restabelecimento das operações.

● Comunicar retorno das operações

Comunicar às unidades afetadas sobre o retorno das operações à normalidade.

ENCERRAMENTO DO PAC

Uma vez validados o funcionamento do retorno dos sistemas essenciais e a estabilidade do data center, a equipe da unidade afetada com o ocorrido entrará em contato com as partes descritas neste plano, provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação às atividades necessárias após a ocorrência de desastres como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

## 12 - Plano de Recuperação de Desastres (PRD)

Este plano apresenta os possíveis cenários de inatividade e os procedimentos correspondentes, detalhando as atividades prioritárias para recuperar o nível de operação dos serviços no ambiente impactado dentro de um prazo aceitável.

OBJETIVO E ESCOPO

O objetivo deste plano é assegurar a retomada das operações do ambiente principal após a ocorrência de uma crise ou desastre, focando exclusivamente nos ativos, conexões e configurações desse ambiente.

São objetivos PRD:

● Avaliar danos aos ativos importantes, conexões e configurações que sustentam a operação do ambiente afetado e prover meios para sua recuperação.

● Assegurar que o ambiente principal retome suas funções normais após uma crise ou desastre e evitar desdobramentos de outros incidentes.

● Minimizar o período em que os serviços ficam inativos, buscando restabelecer o funcionamento dentro de um prazo aceitável.

EXECUÇÃO DO PLANO

● Identificar ativos danificados

A equipe de TI responsável pela INSTALAÇÃO/BACKUP/SERVIDORES/REDE deverá identificar e listar todos os ativos danificados pela ocorrência do desastre.

● Identificar acessos interrompidos

A equipe de TI responsável pela REDE deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, na rede WAN ou com o provedor de serviços.

● Listar serviços descontinuados

A equipe de TI deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do Reitor/Diretor do campus. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, DNS, rotas, VLans, etc.

● Elaborar cronograma de recuperação

O DGTI/NGTI após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração:

1. A priorização dos serviços essenciais ou determinação de nível institucional.
2. O RTO definido para cada serviço essencial.
3. A força de trabalho disponível.

● Substituição de ativos e equipamentos

Em caso de perda de ativos, deverá ser imediatamente informada ao Reitor/Diretor a necessidade de aquisição de ativos perdidos que não serão recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço, comunicando ao Reitor/Diretor se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de TI deve verificar quais ativos danificados estão cobertos por garantia e se poderá ser acionada neste caso através dos fornecedores.

As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas ao Reitor e ao Diretor de TI para que sejam comunicadas às outras unidades.

● Reconfiguração de ativos e equipamento

A equipe de TI deverá verificar se as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, prover cronograma estimado para configurar estes ativos informando ao Reitor/Diretor o tempo estimado.

● Teste de ambiente

O ambiente principal do data center antes do recovery dos dados do backup deverá ser testado a fim de garantir que o processo de recuperação ocorra conforme o planejado.

Os testes incluem:

1. Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre.

● Recuperar dados do backup

Proceder a recuperação dos dados para as aplicações, seja do storage ou fitas de

backup.

1. Validar as configurações e funcionalidades dos sistemas:

▪ A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços

▪ Por equipe designada pela DGTI/NGTI.

ENCERRAMENTO DO PRD

Após a conclusão do processo de recuperação, as informações serão reunidas em um relatório detalhado, informando o horário de retomada de cada serviço, os equipamentos adquiridos, os procedimentos de recuperação aplicados e os fornecedores que foi necessário acionar.

## 13 - Documento de Validação e Teste

O Plano de Continuidade de Negócio de Tecnologia da Informação será testado e validado em reunião entre os líderes de cada unidade de TI do Instituto a cada semestre ou com a insurgência de novos fatores de risco, mudança na análise de impacto ou com a inclusão de um novo serviço no plano de continuidade.

| Data | Tipo[1] | Motivo | Status[2] |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[1]Teste de mesa, Caminho percorrido ou Simulação
[2]Programado, Executado, Planejado ou Agendado

ANEXO I - RELATÓRIO DE ACOMPANHAMENTO DAS ESTRATÉGIAS DE PREVENÇÃO

1. Identificação

| Semestre | Unidade | Responsável |
|---|---|---|
| | | |

2. Infraestrutura predial

| Estratégia | Atividades | Frequência | Responsável | Está adequado? (S/N/NA) | Providências necessárias |
|---|---|---|---|---|---|
| Combate a incêndio | Verificação dos extintores | | | | |
| | Monitoramento da temperatura | | | | |
| | Monitoramento do sistema de detecção de incêndio/alarme/detecção de fumaça | | | | |
| Alagamento | Verificação de calhas, telhas, ralos e canos entupidos | | | | |
| Segurança física | Controle do acesso físico ao datacenter. | | | | |
| | Gerenciamento do acesso físico ao | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | ambiente do datacenter (entrega e devolução de chaves, troca de senhas de acesso, etc) | | | | |
| | Vigilância predial contra roubo, invasão ou depredação. | | | | |
| | Controle de acesso de visitantes e prestadores de serviço. | | | | |
| Instalações elétricas internas | Verificação preventiva da instalação elétrica contra curto-circuito e outros. | | | | |
| Climatização | Manutenção dos equipamentos | | | | |
| | Tempo de vida dos equipamentos | | | | |
| Proteção contra raios | Manutenção periódica | | | | |

3. Sistema de energia elétrica

| Estratégia | Atividades | Frequência | Responsável | Está adequado? (S/N/NA) | Providências necessárias |
|---|---|---|---|---|---|
| Instalações elétricas externas | Manutenção da instalação elétrica externa do Campus | | | | |
| | Proteção do quadro de energia externo | | | | |
| Manutenção grupo gerador | Manter contrato de manutenção ativo | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Fiscalização e getão do contrato | | | | |
| | Manutenção Corretiva | | | | |
| | Abastecimento combustível | | | | |
| | Teste de funcionamento | | | | |
| Nobreaks | Manter contrato de manutenção ativo | | | | |
| | Fiscalização e gestão do contrato | | | | |
| | Manutenção preventiva mensal | | | | |
| | Manutenção corretiva | | | | |
| | Abastecimento combustível | | | | |
| | Teste de funcionamento | | | | |

4. Ativos de rede Estratégia Atividades Periodicidade Responsável. Está adequado? (S/N/NA) Providências necessárias

| Estratégia | Atividades | Frequência | Responsável | Está adequado? (S/N/NA) | Providências necessárias |
|---|---|---|---|---|---|
| Manter ativos de rede em condições adequadas | Acompanhamento do tempo de vida dos equipamentos | | | | |
| | Processo de especificação técnica | | | | |
| | Planejamento orçamentário | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Processo licitatório (compra) | | | | |
| | Processo de instalação/configuração | | | | |
| | Manter contrato de licença e suporte ativos | | | | |
| | Manter inventário dos equipamentos centrais para planejamento de substituição | | | | |
| | Manter inventário dos equipamentos de distribuição para planejamento de substituição | | | | |
| Atualização do firmware | Instalar, configurar e verificar | | | | |
| Configurações específicas | Configurar e validar | | | | |
| Backup | Manter cópia de segurança | | | | |
| | Simulação de recuperação do backup | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Sistemas de Redundância | Garantir redundância em todos os dispositivos | | | | |

5. Conectividade

| Estratégia | Atividades | Frequência | Responsável | Está adequado? (S/N/NA) | Providências necessárias |
|---|---|---|---|---|---|
| Gestão dos serviços de conectividade Internet | Manter contratos ativos com as operadoras | | | | |
| | Fiscalizar os serviços de conectividade | | | | |
| | Revisar e gerir a necessidade de ampliação da largura de banda | | | | |
| Monitoramento e correções automáticas | Manter sistemas de monitoramento | | | | |
| | Identificar proativamente falhas nos serviços | | | | |
| | Identificar comportamento de usuários que possam degradar os serviços | | | | |
| | Manter mecanismos para isolar e corrigir automaticamente ameaças aos serviços | | | | |
| Acesso à Internet em contingência | Manter alternativas disponíveis para substituição dos links principais em caso de falha | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Manter mecanismo automatizado de acionamento de link alternativo | | | | |
| Anel de fibra óptica | Monitorar | | | | |
| | Manter contratos de manutenção ativos | | | | |

6. Sistemas Básicos

| Estratégia | Atividades | Frequência | Responsável | Está adequado? (S/N/NA) | Providências necessárias |
|---|---|---|---|---|---|
| Instalação | Instalação utilizando arquivos originais recomendados pelo fabricante ou de origem confiável | | | | |
| Atualização | Acompanhar a disponibilidade das novas versões | | | | |
| | Aplicar as atualizações do fabricante | | | | |
| | Manter um inventário dos dispositivos para controle das atualizações | | | | |
| Licenciamento | Proceder a especificação para orientar processo de compra | | | | |
| | Gerenciar as licenças e renovações | | | | |
| Cópia de segurança | Manter cópia de segurança para os dispositivos críticos (servidores, | | | | |

| | | | | | |
|---|---|---|---|---|---|
| (backup) | dispositivos de rede centrais etc) | | | | |
| | Manter cópia de segurança dos bancos de dados | | | | |
| | Testar a restauração do backup | | | | |
| | Manter estratégia de backup segura (offsite) | | | | |
| | Verificar a qualidade e o tempo de vida dos dispositivos e mídias utilizados para backup | | | | |
| Certificados SSL | Instalação | | | | |
| | Renovação automática | | | | |

7. Sistemas de desenvolvimento próprio

| Estratégia | Atividades | Frequência | Responsável | Está adequado? (S/N/NA) | Providências necessárias |
|---|---|---|---|---|---|
| Gestão de mudanças | Planejamento das mudanças mais significativas | | | | |
| | Controle das solicitações por meio do sistema Atendimento SUAP | | | | |
| Controle de versões | Acompanhamento do uso do sistema de controle de versões, especialmente considerando novos integrantes na | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | equipe | | | | |
| | Gestão das atividades dos desenvolvedores | | | | |
| Desenvolvimento seguro | Gestão do código fonte visando segurança cibernética | | | | |
| | Testar as mudanças em ambiente de homologação | | | | |
| | Homologar as mudanças mais significativas junto ao solicitante | | | | |
| Servidor de aplicação e banco de dados | Manter servidor de aplicações, banco de dados e sistema operacional atualizados | | | | |
| | Criar mecanismos de redundância para garantir máxima disponibilidade | | | | |
| | Realizar procedimentos de backup | | | | |
| | Realizar procedimentos de teste do backup com recuperação dos dados | | | | |
| | Verificar se o pool de conexões está adequado à demanda de acesso ao banco de dados | | | | |
| | Disponibilizar e gerir controles de acesso que garantam a autenticidade, confidencialidade, disponibilidade e | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | integridade das informações | | | | |
| | Disponibilizar e gerir controles de acesso ao código fonte das aplicações | | | | |

8. Sistemas de terceiros

| Estratégia | Atividades | Frequência | Responsável | Está adequado? (S/N/NA) | Providências necessárias |
|---|---|---|---|---|---|
| Contratos | Avaliar a adequação do serviço a ser contratado conforme padrões técnicos definidos pela (CODES e COTEC) | | | | |
| | Manter contrato vigente e gerenciar renovações | | | | |
| | Acompanhar a aderência do serviço em relação aos padrões da (CODES e COTEC) quando houver alguma alteração | | | | |
| | Fiscalizar o pleno cumprimento do contrato | | | | |

9. Providências necessárias

| Providência | Encaminhamento |
|---|---|
| | |

10. Observações gerais

| |
|---|
| |

Nome da Cidade, ____ de _____ de _____.

RESPONSÁVEL PELA UNIDADE

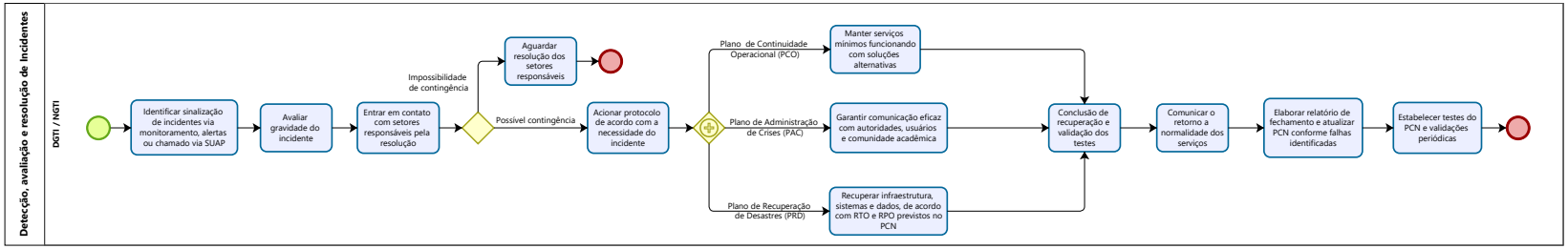
Cargo

# Detecção, avaliação e resolução de Incidentes

Bizagi Modeler

Índice

# 1 DETECÇÃO, AVALIAÇÃO E RESOLUÇÃO DE INCIDENTES



**Versão:**

1.0

**Autor:**

avspe

# 1.1 DETECÇÃO, AVALIAÇÃO E RESOLUÇÃO DE INCIDENTES

## 1.1.1 ELEMENTOS DO PROCESSO

### 1.1.1.1 ☐ Identificar sinalização de incidentes via monitoramento, alertas ou chamado via SUAP

**Entradas**

Sinalização de incidentes

**Saídas**

Incidentes identificados

### 1.1.1.2 ☐ Avaliar gravidade do incidente

**Entradas**

Incidentes identificados

**Saídas**

Gravidade do incidente avaliada

### 1.1.1.3 ☐ Entrar em contato com setores responsáveis pela resolução

**Entradas**

Gravidade do incidente avaliada

**Saídas**

Registro do incidente

### 1.1.1.4 ☐ Acionar protocolo de acordo com a necessidade do incidente

**Entradas**

Registro do incidente

**Saídas**

Protocolo acionado

#### 1.1.1.5 ☐Manter serviços mínimos funcionando com soluções alternativas

**Entradas**

Protocolo acionado

**Saídas**

Serviços mínimos funcionando e soluções alternativas acionadas

**Observações**

Necessidade de detalhar o tipo de procedimento a ser tomado de acordo com o incidente e com a infraestrutura disponível.

#### 1.1.1.6 ☐Garantir comunicação eficaz com autoridades, usuários e comunidade acadêmica

**Entradas**

Protocolo acionado

**Saídas**

Protocolo de comunicação ativado

**LGPD**

Possível

**Observações**

- Verificar melhor forma de estabelecer comunicação com os setores impactados pelo incidente;

- Verificar existência de dados sensíveis e como abordar a comunicação diante dessas situações.

#### 1.1.1.7 ☐Recuperar infraestrutura, sistemas e dados, de acordo com RTO e RPO previstos no PCN

**Entradas**

Protocolo acionado

**Saídas**

Testes realizados

#### 1.1.1.8 ☐Conclusão de recuperação e validação dos testes

**Entradas**

Testes realizados; Serviços mínimos funcionando e soluções alternativas acionadas; Protocolo de comunicação ativado

**Saídas**

Testes validados e serviços estabilizados

1.1.1.9 ☐ Comunicar o retorno a normalidade dos serviços

**Entradas**

Testes validados e serviços estabilizados

**Saídas**

Retorno das atividades comunicado; relatório de retorno; relatório de incidente; lições aprendidas

1.1.1.10 ☐ Elaborar relatório de fechamento e atualizar PCN conforme falhas identificadas

**Entradas**

Retorno das atividades comunicado; relatório de retorno; relatório de incidente; lições aprendidas

**Saídas**

PCN revisado e fortalecido.

1.1.1.11 ☐ Estabelecer testes do PCN e validações periódicas

**Entradas**

PCN revisado e fortalecido.

**Saídas**

Testes periódicos e validações estabelecidas

**Observações**

Testes e validações devem ocorrer no mínimo uma vez a cada 6 meses.

1.1.1.12 ☐ Aguardar resolução dos setores responsáveis

**Entradas**

Registro do incidente

**Saídas**

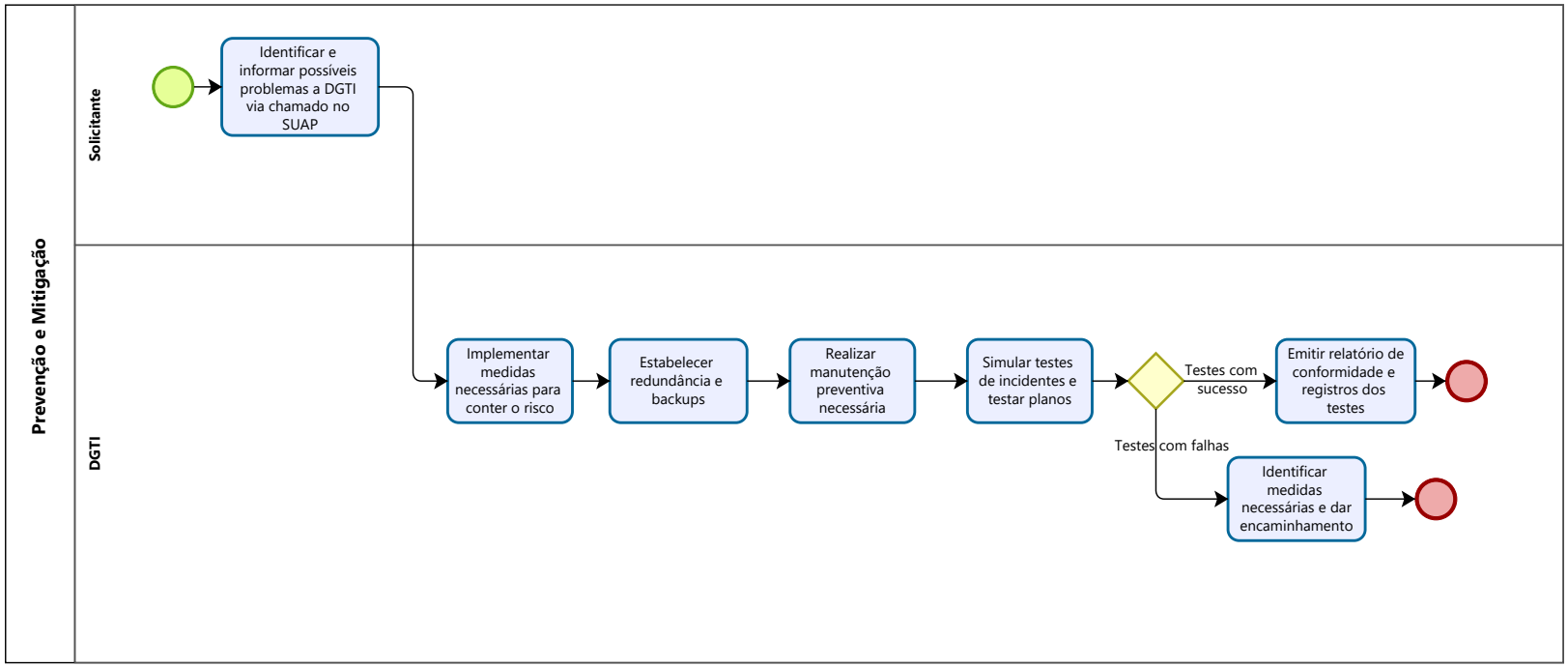
Espera de resolução dos setores reponsáveis

# Prevenção e mitigação de erros

Bizagi Modeler

Índice

# 1 PREVENÇÃO E MITIGAÇÃO



**Versão:**

1.0

**Autor:**

avspe

# 1.1 PREVENÇÃO E MITIGAÇÃO

## 1.1.1 ELEMENTOS DO PROCESSO

### 1.1.1.1 ☐ Identificar e informar possíveis problemas a DGTI via chamado no SUAP

**Entradas**

Abertura de chamado no SUAP

**Saídas**

Chamado aberto

**LGPD**

Não

### 1.1.1.2 ☐ Implementar medidas necessárias para conter o risco

**Entradas**

Chamado aberto

**Saídas**

Medidas de prevenção implementadas

### 1.1.1.3 ☐ Estabelecer redundância e backups

**Entradas**

Medidas de prevenção implementadas

**Saídas**

Alta disponibilidade de serviços de TI mantida

### 1.1.1.4 ☐ Realizar manutenção preventiva necessária

**Entradas**

Alta disponibilidade de serviços de TI mantida

**Saídas**

Serviço de manutenção realizado

#### 1.1.1.5 ☐ Simular testes de incidentes e testar planos

**Entradas**

Serviço de manutenção realizado

**Saídas**

Simulação de testes de incidentes e planos testados

#### 1.1.1.6 ☐ Emitir relatório de conformidade e registros dos testes

**Entradas**

Simulação de testes de incidentes e planos testados

**Saídas**

Relatório de conformidade e registro dos testes emitidos

**Observações**

Avaliar o resultado do teste e caso necessário solicitar treinamento técnico para equipe.

#### 1.1.1.7 ☐ Identificar medidas necessárias e dar encaminhamento

**Entradas**

Simulação de testes de incidentes e planos testados

**Saídas**

Medidas identificadas e processo encaminhado

**Observações**

Exemplos de medidas:

- Reiniciar o processo de manutenção preventiva;

- Encaminhar para manutenção corretiva;

- Acionar empresas parceiras e contratos de manutenção

- Acionar ou contatar outro setor para auxílio.

# Documento Digitalizado Público

## Plano de Continuidade de Negócio de TI

**Assunto:** Plano de Continuidade de Negócio de TI
**Assinado por:** Osmar Cunha
**Tipo do Documento:** Plano
**Situação:** Finalizado
**Nível de Acesso:** Público
**Tipo do Conferência:** Documento Original

Documento assinado eletronicamente por:

- **Osmar Ferreira da Cunha**, **TEC DE TECNOLOGIA DA INFORMACAO**, em 12/11/2025 10:23:24.

Este documento foi armazenado no SUAP em 12/11/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

**Código Verificador:** 1196994
**Código de Autenticação:** d0a427e712