Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul
Pró-Reitoria de Desenvolvimento Institucional
Diretoria de Tecnologia da Informação

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

IFRS

Rua General Osório, 348 – Centro – Bento Gonçalves/RS
CEP: 95700-000 – Telefone: (54) 3449-3321
Sítio eletrônico: http://www.ifrs.edu.br – E-mail: dti@ifrs.edu.br

1. Objetivos

- Estabelecer procedimentos de comunicação e mobilização para o controle de incidentes. O objetivo principal é garantir que haja um fluxo claro de informações e ações coordenadas quando ocorrem emergências ou situações de risco.
- Assegurar a aplicação de ações necessárias para a correção e/ou eliminação de problemas.
- Garantir que os processos críticos de TI tenham seus riscos identificados, avaliados, monitorados e controlados.
- Prover medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais.
- Reduzir o impacto negativo causado por desastres e promover o restabelecimento dos serviços de TI.
- Criar um ambiente onde se tenha como aplicar as ações necessárias para correção e/ou eliminação do problema.

2. Aplicação/escopo

- O plano se aplica a todos os serviços de Tecnologia da Informação (TI) hospedados e mantidos no IFRS.

3. Definições

- **Acionamento**: Processo de comunicação com as equipes envolvidas no controle da emergência, seguindo uma ordem estabelecida para garantir a execução adequada das ações.
- **Administrador do Plano de Contingência**: Responsável pela manutenção e atualização dos dados e procedimentos necessários para o pleno funcionamento do plano.
- **Áreas Sensíveis**: Locais que sofrem impactos negativos significativos em emergências, salas administrativas e Data Center (CPD).
- **Área Vulnerável**: Área afetada pelos efeitos de uma falha.
- **Backup**: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.
- ***Zabbix :*** Ferramenta para monitoramento da infraestrutura de rede, sistemas e aplicações.

- **Contingência**: Situação de risco com potencial de se transformar em emergência, inerente a atividades, serviços e equipamentos.
- **Data Center (CPD)**: Ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, além de ativos de rede como switches e roteadores.
- **Incidente**: qualquer evento que não seja parte da operação padrão de um serviço de TI e que cause, ou possa causar, uma interrupção ou degradação do serviço. Isso inclui falhas de hardware, erros de software, interrupções na rede, solicitações de serviço não planejadas, entre outros eventos que impactam negativamente a disponibilidade, desempenho ou qualidade de um serviço de TI.
- **Hipótese Acidental**: Ocorrência anormal, fora do controle de processos, sistemas ou atividades, com potencial para causar danos aos sistemas e/ou equipamentos de TI.
- **Intervenção**: Ação durante a emergência, seguindo procedimentos planejados, para minimizar danos aos equipamentos e sistemas de TI.
- **Sistema de Suporte**: Sistema GLPI (Gestionnaire Libre de Parc Informatique ou Gestor de Equipamentos de TI de Código Aberto", em português) instalado em um servidor web localizado na Reitoria, que recebe, organiza e mantém o solicitante informado sobre o andamento do chamado de suporte.
- **Situação de Emergência**: Evento em um sistema ou equipamento que resulta ou pode resultar em danos aos próprios sistemas, equipamentos ou ao desempenho do trabalho.
- **TI**: Tecnologia da Informação.
- **VM**: Máquina Virtual, máquina virtualizada em um servidor.
- **RNP**: Rede Nacional de Ensino e Pesquisa.
- **UPS**: Uninterruptible Power Supply (Nobreak).
- **Processos Críticos**: Processos essenciais para a operação do IFRS, cuja interrupção causaria impacto significativo.
- **Prioridade**: Relação entre urgência e impacto de um incidente, considerando o número de usuários afetados e as necessidades da atividade.

4. Responsabilidades

- **Equipe do Setor de TI:** Mitigar impactos de emergências ou situações de emergência que afetem sistemas, equipamentos ou infraestrutura de TI. Elaborar documentação pós-

incidente com desafios, soluções e aprendizados. Realizar testes regulares de backup e recuperação de dados para garantir a disponibilidade dos dados em caso de emergência. Verificar e atualizar regularmente o inventário de hardware e software da instituição, incluindo licenças e datas de expiração de garantia do fabricante com o objetivo de manter renovados os ativos de hardware e os softwares.

- **Servidores:** Informar o Setor de TI sobre emergências ou situações acidentais nas áreas relacionadas a TI.
- **Departamentos de Gestão:** Tomar decisões estratégicas, principalmente em casos que envolvam aquisições/compras de emergência.
- **Prestadores de Serviços Terceirizados e Fornecedores**: Acionar quando houver contrato de suporte e garantia vigentes.

5. Níveis de Incidentes

Nível I: Este nível é caracterizado por uma hipótese acidental que pode ser controlada pela equipe de TI e que não afeta o andamento do trabalho dos servidores.

Exemplos típicos incluem problemas com equipamentos periféricos de computadores, como um mouse ou teclado que não funciona corretamente.

Esses incidentes são geralmente de menor impacto e podem ser resolvidos rapidamente pela equipe de TI, sem causar interrupções significativas nas atividades dos usuários.

Nível II: Este nível envolve uma hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo servidor.

Exemplos incluem problemas com o funcionamento do computador (como um computador que não liga ou está travado) ou sistemas offline que impedem o uso deles.

Esses incidentes têm um impacto maior do que os do Nível I, pois afetam diretamente a capacidade do servidor de realizar suas tarefas, mas ainda são geralmente restritos a um único usuário ou sistema.

A equipe de TI deve agir prontamente para resolver esses problemas e pode precisar fornecer soluções alternativas, como um computador provisório, para garantir que o trabalho possa continuar.

Nível III: Este nível representa uma hipótese acidental que impede o uso de sistemas ou equipamentos de toda a instituição, impedindo assim o desenvolvimento do trabalho de todos os servidores.

Exemplos incluem falha na conexão com a internet, queda de energia elétrica ou indisponibilidade de um servidor de rede que hospeda os sistemas da instituição.

Esses incidentes são os mais graves e têm o maior impacto, afetando todos os usuários e serviços do IFRS. A resposta a esses incidentes exige uma ação imediata e coordenada da equipe de TI, com foco na restauração dos serviços essenciais e na minimização das interrupções.

É importante destacar que a definição da prioridade no atendimento desses incidentes é determinada pela relação entre a urgência e o impacto. O impacto é definido pelo número de usuários afetados, enquanto a urgência leva em conta a natureza da atividade e o quanto ela impacta os processos da instituição.

6. Prioridades

- Definir a prioridade de atendimento com base na relação **Urgência x Impacto**, seguindo boas práticas como o framework ITIL.
- O **impacto** é definido pelo número de usuários afetados.
- A **urgência** considera o tipo de atividade e seu impacto em atividades que não podem ser interrompidas.

7. Principais Riscos

- **Interrupção de energia elétrica:** Causada por fatores externos ou internos, com duração superior a 30 minutos.
- **Falha na climatização do Data Center:** Superaquecimento da sala devido a falha no sistema de climatização.
- **Indisponibilidade de rede/circuitos:** Rompimento de cabeamento ou falha de ativos de rede.
- **Falha humana:** Acidente ao manusear equipamentos ou erros ao aplicar configurações em equipamentos.
- **Ataques internos:** Ataque aos ativos do Data Center e equipamentos de TI.
- **Falha de hardware:** Falha que necessite reposição de peça ou reparo.
- **Ataque cibernético:** Ataque virtual que comprometa o desempenho, os dados ou a disponibilidade dos serviços de TI.
- **Desastres naturais:** Alagamentos, vendavais etc., com destruição de infraestrutura.

- **Incêndio:** Incêndio no prédio ou prédios vizinhos.

8. Estratégias de Controle, Monitoramento e Tratamento de Incidentes

- **Problemas com computadores desktops ou notebook institucionais:**
    - O usuário identifica um problema ou necessidade e abre um chamado no GLPI/Suporte (https://suporte.ifrs.edu.br), informando detalhes como a descrição do problema, categoria e nível de urgência. Caso não seja possível acessar o sistema, o chamado pode ser aberto através do telefone do Setor de suporte de TI (3449.3345) ou via e-mail (dti@ifrs.edu.br);
    - O chamado é recebido pela equipe de suporte e classificado quanto à prioridade, impacto e tipo de solicitação (incidente, requisição de serviço, etc.);
    - O chamado é atribuído a um técnico ou equipe responsável para o atendimento;
    - O técnico analisa o problema, investiga as possíveis causas e propõe uma solução. Caso não seja possível a resolução imediata do problema e o computador está inoperante, é disponibilizado um computador provisório para o servidor poder continuar desenvolvendo suas atividades e o computador com problemas é removido para reparo na sala de suporte da TI;
    - A solução é implementada e testada. Se necessário, o técnico pode entrar em contato com o solicitante para esclarecimentos adicionais;
    - O usuário valida se o problema foi realmente resolvido. Caso contrário, o chamado pode ser reaberto ou encaminhado para outra fase de análise;
    - Com o problema resolvido e validado, o chamado é encerrado e documentado no sistema, incluindo a descrição da solução aplicada; e
    - Os registros dos chamados podem ser usados para geração de relatórios e análises de performance da equipe de suporte.
- **Problemas de conexão com a rede interna e internet:**
    - Identificar a abrangência do problema (computador, sala, andar, prédio);
    - Analisar a conexão do computador até o gateway de borda;
    - Se o problema de conexão afetar todo o prédio, verificar se os servidores de endereços DHCP, DNS e de autenticação estão operando corretamente; e

- Caso haja conexão interna até os mencionados servidores, mas não até o gateway, deve-se abrir um chamado de suporte com a RNP enviando um e-mail para atendimento@rnp.br ou ligando para 0800 722 0216.

- **Problemas com acesso aos sistemas internos:**
    - O usuário que identificou o problema deve informar a DTI através dos meios de contato disponíveis (sistema de suporte ou telefone);
    - Se já não foi informado, a DTI deve identificar qual o sistema está inacessível (ou os sistemas) através de testes ou monitoramento do *Zabbix* ou do *Uptime Kuma*;
    - Verificar se a VM onde o sistema está instalado está em execução;
    - Caso esteja em execução, verificar o estado da VM, se apresenta erros, etc.;
    - Caso o estado da VM esteja normal, verificar se os serviços (Docker, mapeamentos de rede, configurações, interfaces de rede) estão funcionando;
    - Caso não esteja em execução, iniciá-la no cluster de VMs e testar seu acesso novamente; e
    - Por fim, identificar e resolver o problema informando a solução aos demais usuários se necessário.
- **Problemas com equipamentos de rede:**
    - Identificar qual equipamento está com problema;
    - Caso possível, realizar a manutenção do mesmo; e
    - Caso não seja possível consertar, realizar a substituição do equipamento;
- **Problemas físicos com cabeamento:**
    - Identificar o segmento de rede que está com problema;
    - Testar as extremidades do cabo com problema;
    - Se necessário, refazer os conectores RJ45 e testar novamente; e
    - Caso o problema persista, substituir o cabo;
- **Problemas no fornecimento de energia elétrica:**
    - Se o tempo de falta de energia elétrica for menor de 30 minutos os sistemas e servidores de rede continuam em funcionamento, pois estão ligados em nobreaks;

- Caso a falta de energia dure mais de 30 minutos, os servidores perdem o fornecimento e energia e são desligados;
- O responsável técnico pelo contrato de fornecimento de energia elétrica é informado para que sejam tomadas as medidas necessárias com a concessionária de energia elétrica; e
- Após o restabelecimento da energia elétrica, seguir o procedimento de inicialização dos servidores descrito no repositório de informações da Wiki restrita.

- **Problemas com UPS/nobreak:**
  - Em caso de problema ou anormalidade reportado pelo próprio nobreak é informado a PROAD que irá planejar e executar a contratação de manutenção corretiva com uma empresa especializada; e
  - A DTI irá transferir as conexões de energia dos servidores para o nobreak que está funcionando.
- **Problemas com o sistema de climatização do CPD:**
  - Desligar o aparelho com problema e monitorar a temperatura da sala com apenas um aparelho em funcionamento;
  - Informar a PROAD que irá planejar e executar a contratação de manutenção corretiva com uma empresa especializada; e
  - Em caso de problema na rede elétrica informar a PROAD para proceder com a contratação de empresa especializada em manutenção elétrica.
- **Incidentes de segurança relacionados a ataques cibernéticos:**
  - Considerando a complexidade e a variedade de ataques cibernéticos, o tratamento e resposta a este tipo de incidente requer alguns passos adicionais em comparação aos outros descritos anteriormente:

a. Detecção do Incidente

- **Monitoramento:** Utilizar sistemas de monitoramento de rede (como Zabbix, ou ferramentas de segurança que realizam análise de tráfego de rede) para detectar anomalias e atividades suspeitas que possam indicar um ataque cibernético.
- **Notificação:** Usuários devem informar o Setor de TI caso detectem qualquer atividade suspeita ou emergência. A comunicação pode ser feita por meio de um sistema de suporte (GLPI), por e-mail, ou, em caso de impossibilidade de acesso ao sistema, por outros meios de comunicação.

b. Identificação e Análise

- **Isolamento:** Se possível, isolar os sistemas ou redes afetadas para impedir a propagação do ataque.
- **Tipo de Ataque:** Analisar os logs e alertas gerados pelos sistemas de segurança para determinar o tipo de ataque (ex: malware, ransomware, DDoS, invasão, etc). Verificar o tipo de ataque cibernético que comprometa o desempenho, os dados ou configuração dos serviços essenciais.
- **Serviços Afetados:** Identificar quais serviços, sistemas ou equipamentos foram afetados pelo ataque. Isso pode incluir servidores, bancos de dados, aplicações web, estações de trabalho e outros ativos de TI.

c. Resposta ao Incidente

- **Intervenção:** Implementar ações planejadas para minimizar os danos e restaurar os serviços afetados. Isso pode incluir a remoção de malware, a restauração de dados a partir de backups, a aplicação de patches de segurança, a reconfiguração de sistemas ou servidores e outras ações de resposta.
- **Comunicação:** Informar as partes interessadas sobre o incidente, o impacto e as ações de resposta.
- **Quarentena:** Se necessário, colocar em quarentena ou banir da rede o tráfego com origem suspeita.

d. Recuperação

Restauração: Restaurar os sistemas e serviços afetados a partir de backups. Priorizar a restauração de sistemas críticos para garantir a continuidade das atividades prioritárias.

Verificação: Verificar a integridade dos sistemas e dados restaurados. Realizar testes para garantir que os sistemas estão funcionando corretamente e que não há ameaças persistentes.

- **Monitoramento:** Continuar monitorando os sistemas para detectar qualquer nova atividade suspeita ou vulnerabilidade.

e. Pós-Incidente

- **Documentação:** Elaborar um relatório detalhado do incidente, incluindo a causa, o impacto, as ações de resposta e as lições aprendidas.

- **Melhorias:** Identificar e implementar melhorias nos procedimentos de segurança, monitoramento e resposta a incidentes para evitar que incidentes semelhantes ocorram no futuro.
- **Backup:** Manter cópias de segurança (backup) atualizadas dos sistemas e dados, para garantir a recuperação dos dados em caso de perda.
- **Testes:** Realizar testes periódicos de restauração de dados e simulações de ataques cibernéticos para validar o plano de contingência e garantir que a equipe está preparada para lidar com incidentes de segurança

9. Controles Preventivos e Estratégias de Recuperação

- Realizar e manter backups de VMs e dados, em locais físicos distintos;
- Disponibilizar computadores e/ou notebooks para substituir equipamentos de usuários com problemas;
- Manter documentação técnica em local acessível em caso de incidentes para recuperação dos ambientes afetados; e
- Realizar testes de recuperação de desastre regulares para avaliar a eficácia do plano de contingência em situações de emergência reais e identificar áreas de melhoria.

10. Manutenções Preventivas

- Realizar manutenção preventiva periódica em nobreaks;
- Realizar manutenção preventiva periódica no sistema de climatização do CPD;
- Manter firmwares de servidores e equipamentos de TI atualizado com os últimos patches de segurança disponibilizados pelos fabricantes; e
- Manter sistemas operacionais atualizados com a última versão disponível sempre que possível.

11. Comunicação

- **Quem deve comunicar:** Qualquer servidor/usuário que detecte problemas de TI.
- **A quem comunicar:** Setor de TI da instituição.

- **Como comunicar:** Sistema de Suporte ou, na indisponibilidade deste, por outros meios como telefone ou e-mail.

12. Fluxograma

- Um fluxograma de atendimento e resposta a incidentes de TI pode ser estruturado da seguinte forma:

12.1. Identificação do Incidente

- Qualquer servidor ou usuário dos serviços providos pela TI detecta um problema ou anomalia nos sistemas, equipamentos ou infraestrutura de TI.
- O incidente pode variar de problemas com equipamentos periféricos a falhas em servidores de rede ou ataques cibernéticos.

12.2. Comunicação do Incidente

- O problema deve ser comunicado ao Setor de TI através do Sistema de Suporte.
- O sistema de suporte é usado para receber, organizar e manter o solicitante informado sobre o andamento do chamado.
- Em alguns casos, quando o sistema de suporte não estiver acessível, a comunicação pode ser feita por e-mail, por telefone ou diretamente no setor de TI.

12.3. Registro do Incidente

- Um chamado de suporte é aberto no sistema, registrando o problema e o solicitante.
- O chamado é então atribuído a um grupo de atendimento técnico. E posteriormente a um técnico do setor de TI responsável pelo atendimento.

12.4. Avaliação e Classificação do Incidente

- A equipe de TI avalia o incidente para determinar seu nível de impacto e urgência.
- Os incidentes são classificados em níveis, como Nível I (problemas menores que não afetam o trabalho do servidor) ou Nível II (problemas que impedem a utilização de equipamentos ou sistemas).
- A prioridade de atendimento é definida pela relação entre a urgência e o impacto do incidente. O impacto é determinado pelo número de usuários afetados, enquanto a urgência considera a criticidade da atividade.

12.5. Intervenção e Resolução do Incidente

A equipe de TI age para corrigir ou minimizar os danos causados pelo incidente, seguindo as ações planejadas no plano de contingência. Essa intervenção pode envolver ações como:

- Reparo ou substituição de equipamentos;
- Restauração de sistemas a partir de backups;
- Reconfiguração de ativos de rede;
- Ações de segurança para conter ataques cibernéticos; e
- Em alguns casos, o problema pode ser encaminhado para assistência técnica externa ou terceirizados, se necessário;

12.6. Comunicação da Resolução

- Após o atendimento, o solicitante é informado da conclusão ou resolução do problema através do sistema de suporte ou por e-mail.
- Em casos de incidentes maiores, informações sobre a solução e o tempo de inatividade podem ser comunicados a todos os servidores.

12.7. Monitoramento e Melhoria Contínua

- A equipe de TI monitora os sistemas e acessos dos usuários para identificar padrões de comportamento e prevenir futuros incidentes.
- Após a resolução do incidente, a equipe pode documentar os desafios superados, as soluções aplicadas e os aprendizados obtidos para melhorar os planos de contingência.
- Testes regulares são realizados para simular situações reais e garantir a eficiência do plano de contingência.

13. Publicação

- Este documento está disponível no site institucional.

14. Vigência/Validade

- O plano terá validade indeterminada e sofrerá revisões anuais ou em caso de mudanças significativas na infraestrutura de TI.