Ministério da Educação

Secretaria de Educação Profissional e Tecnológica,

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul

***Campus* Avançado Veranópolis**

PLANO DE CONTINGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO DO IFRS - *CAMPUS* AVANÇADO VERANÓPOLIS

Plano desenvolvido em 2019 e atualizado em 2021.

IFRS – *Campus* Avançado Veranópolis

1. OBJETIVO

Este plano tem por objetivo definir procedimentos para tratamento de incidentes de Tecnologia da Informação (TI), assim como a prevenção dos mesmos com foco em minimizar os impactos negativos que possam comprometer o bom andamento das atividades cotidianas do *Campus* Avançado Veranópolis.

Em caso de contingências e emergências que possam ocorrer durante as atividades na execução dos serviços de Tecnologia da Informação, o plano de contingência contém os procedimentos de correção e/ou eliminação dos problemas. Para tanto, este plano deve assegurar que os processos críticos tenham seus riscos identificados, avaliados, monitorados e controlados.

2. APLICAÇÃO

Este documento se aplica à todos os serviços e infraestrutura de TI executados no âmbito do IFRS *Campus* Avançado Veranópolis.

3. ESCLARECIMENTOS/DEFINIÇÕES

Acionamento/Chamado: é o processo de comunicação de incidentes para a equipe encarregada do controle e tratamento dos mesmos. O objetivo é contornar os incidentes no menor espaço de tempo possível buscando minimizar impactos na rotina de trabalho do *Campus*.

Administrador do Plano de Contingência: É o responsável pela manutenção e atualização dos dados e procedimentos do Plano de Contingência que poderá ser revisto e atualizado sempre que necessário para que o plano seja eficiente e esclarecedor.

Áreas Vulneráveis: São as áreas que sofrem efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas encontram-se o próprio Centro de Processamento de Dados – CPD, laboratórios de informática, salas administrativas, de professores, de coordenadores de curso, de atendimento assim como a biblioteca do Campus.

Contingência: Situação de risco com potencial de ocorrer, inerente as atividades, serviços e equipamentos, e que ocorrendo se transformará em um incidente.

Centro de Processamento de Dados - CPD: Ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, sistemas, ativos de rede como *switches*, roteadores dentre outros, de forma centralizada e de fácil gerenciamento.

Equipe de TI: São os servidores efetivos lotados no setor de TI do *Campus* Avançado Veranópolis e que respondem legalmente pelo setor no que diz respeito à infraestrutura, equipamentos e serviços de TI.

Incidente: É o evento não programado capaz de causar danos de diversas montas aos sistemas e aos equipamentos de TI do *Campus*.

Hipótese Acidental: Toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade, da qual possam resultar danos aos sistemas e/ouequipamentos de TI do *Campus*.

Intervenção: É a atividade de atuar durante a emergência, seguindo ações planejadas, visando minimizar e corrigir os possíveis danos aos equipamento e sistemas de TI do *Campus*.

Sistema de Suporte: Sistema GLPI (*Software* Livre de Chamados de Suporte) instalado em um servidor *web* do *Campus* e que pelo próprio é possível receber, organizar, registrar e manter o solicitante informado sobre o andamento dos chamados de suporte a incidentes.

Situação de Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho do trabalho de servidores do *Campus.*

TI: Tecnologia da Informação.

Usuários: Servidores do campus que utilizam equipamentos e consomem serviços de TI pelo uso de sistemas ou recursos.

4. RESPONSABILIDADES

4.1 Equipe do Setor de Tecnologia da Informação

A equipe do setor de TI é responsável por identificar o chamado, agir com objetivo de mitigar os impactos que por ventura venham a ocorrer decorrentes de incidentes, hipóteses acidentais e de situações de emergência que tenham potencial de afetar os sistemas, equipamentos ou infraestrutura de TI do *Campus* Veranópolis.

4.2 Servidores do *Campus*

Responsáveis por informar ao Setor de TI do *Campus,* caso detectem algum tipo de incidente, hipótese acidental ou emergência em alguma das áreas sensíveis.

5. NÍVEIS DE INCIDENTES

Nivel I – Hipótese acidental que pode ser controlada pela equipe de TI e que não afeta o andamento das atividades cotidianas do *Campus*. Ex: Incidente com roteador *wireless* que mediante falha é coberto por outro ponto e dessa forma, não prejudica os usuários.

Nível II – Hipótese acidental que impede a utilização de equipamento ou sistema e, dessa forma, acaba impedindo a continuidade do trabalho do usuário. Ex: Sistema em específico *ofline* que impede um ou um grupo limitado de usuários de trabalhar enquanto o incidente não é resolvido.

Nível III – Hipótese acidental que impacta o uso de vários sistemas ou equipamentos tendo impacto sobre todos os usuários do *Campus*. Ex: Rede de dados sem conexão que impede todos usuários de utilizarem sistemas.

6. PRINCIPAIS RISCOS

O Plano de Contingência de incidentes foi desenvolvido para ser acionado quando da ocorrência de cenários que apresentam risco à continuidade dos serviços essenciais do *Campus.* O quadro abaixo aponta os principais riscos e as causas dos mesmos.

EVENTO	CAUSA
Interrupção de energia	**Fator externo ao campus:** fora da alçada da equipe de do *Campus*.
Interrupção de energia	**Fator interno ao *Campus*:** proveniente de sobrecarga de energia, curto-circuíto, sinistro causado por intempérias ou incêndio.
Rompimento de fibra ótica	**Fator externo ao *Campus*:** rompimentos de fibra for a do *Campus* com potencial de impedir o acesso à rede mundial de computadores.
Rompimento de fibra ótica	**Fator interno ao *Campus*:** rompimento proveniente de incêndio, intempéria como temporal ou acidental em obras de reformas e construções.
Falha em sistemas	Os sistemas operantes no CPD podem estar suscetíveis a falhas que os tirem de operação. Ex: Base de dados corrompida por falha física ou logica.
Falha de *hardware*	Os *hardwares* do CPD assim como todos os utilizados pelos usuários estão suscetíveis a falhas físicas como queima de placa mãe, falha de memória, falha de processador, falha de disco rígido assim como problemas menores que comprometam fisicamente os equipamentos.
Indisponibilidade em ativos de rede	Os ativos de rede como *switches*, conversores e *access point* podem ficar indisponíveis por ocorrencia de problemas físicos ou lógicos comprometendo a rede interna.
Virus e *malwares*	A rede lógica do *Campus* está suscetível a infecção por virus e *malwares* que podem corromper serviços vitais comprometendo o funcionamento da rede.
Ataque cibernético	Ataques externos ou internos coordenados por *crackers* com intúito de derrubar serviços ou equipamentos podem ocorrer.
Falha humana	Forma incorreta de operar um equipamento ou ativo que possa provocar inoperabilidade do equipamento/serviço.
Ambiente inadequado de operação	Ambiente em que computadores, servidores e equipamentos funcionem em condições físicas inadequadas. EX: CPD operando em temperaturas climáticas altas proporcionando riscos de travamento/desligamento de equipamentos.
Falta de material de manutenção/reposição	Também faz parte do plano de contingência uma garantia de materiais e ferramentes de manutenção para correção de incidentes. A falta de materiais e ferramentas pode resultar na continuidade do incidente por períodos mais longos.

7. ESTRATÉGIAS DE CONTROLE, MONITORAMENTO E TRATAMENTO DE INCIDENTES

7.1 Interrupção de Energia

7.1.1 - Fator externo ao *Campus*:

1 - A equipe de TI iniciará contato com a operadora de energia para buscar informações e/ou abrir chamado quando for o caso de incidentes na rede elétrica nas proximidades do *Campus*.
2 - O setor de TI monitorará o CPD no tocante ao tempo de autonomia de carga do *nobreak* para que não haja corte brusco de energia no CPD podendo acarretar danos aos equipamentos.
3 - Havendo necessidade o desligamento manual do CPD será realizado com segurança caso a falta de energia persista por mais tempo do que a autonomia de carga das baterias do *nobreak*.

7.1.2 – Fator interno ao campus:

1 - O setor de TI buscará juntamente com a gestão do *Campus* todas as formas para que o incidente seja contornado o no menor tempo possível buscando acionar as partes competentes para a solução.
2 - O setor de TI monitorará o CPD no tocante ao tempo de autonomia de carga do *nobreak* para que não haja corte brusco de energia no CPD podendo acarretar danos aos equipamentos.
3 - Havendo necessidade de desligamento manual da energia do CPD, será realizado com segurança caso a falta de energia persista por mais tempo do que a autonomia de carga das baterias do *nobreak*.

7.2 Rompimento de Fibra Ótica

1 – Fator externo ao campus:

1 – O setor de TI contatará o Ponto de Presença da Rede Nacional de Pesquisa responsável pelo Rio Grande do Sul - POP/RS para abertura de chamado. Desse momento em diante, a responsabilidade pela identificação do incidente e solução do mesmo é do POP/RS restando ao setor de TI do *Campus* aguardar. Caso seja rompimento de fibra ótica, o POP/RS abrirá chamado com a operadora responsável pela rede de fibra ótica que chega até o *Campus*.

2 – Fator interno ao *Campus*:

1 - O setor de TI juntamente com a gestão do *Campus* não medirão esforços para que seja corrigido no menor tempo possível o incidente. O rompimento de fibra no é uma hipótese remota visto que a fibra percorre um caminho estratégico no trajeto até o CPD do *Campus*.

7.3 Falha em Sistemas

1 – A equipe de TI identifica por meio de monitoramento de falhas no CPD.
2 – A equipe de TI notifica os usuários sobre a inoperabilidade e projeta uma previsão para o reestabelecimento do serviço.
3 – A equipe de TI resolve o incidente no menor tempo possível e reestabelece os serviços indicando para os usuários sobre o reestabelecimento do serviço por *e-mail* ou ramal telefônico.
4 – Para falhas de sistemas há o reestabelecimento de *backups* de sistemas críticos para que em caso de dano grave, o sistema seja recuperado no menor espaço de tempo possível.

7.4 – Falha de *Hardware*

7.4.1 Computadores de laboratórios de informática:

1 – Incidentes com equipamentos e sistemas dos laboratórios serão reportados ao setor de TI por meio de envio de um *e-mail* de suporte pelo endereço suporte@veranopolis.ifrs.edu.br. Nesse caso o

responsável pelo uso do laboratório é quem abre o chamado. O envio do *e-mail* gera um chamado no sistema GLPI do campus.
Obs: Caso não seja possível acessar o *e-mail* ou o chamado seja de extrema urgência e comprometa as atividades, poderá o mesmo ser aberto via ramal telefônico.
2 - A partir da abertura do chamado é agendado o atendimento e há uma interação entre demandante do chamado e a equipe de TI. No decorrer do atendimento o usuário demandante receberá notificações por *e-mail* a cada ação executada do respectivo chamado. O demandante também pode acompanhar acessando o sistema de suporte diretamente.
3 - Caso o problema impeça o andamento das atividades de laboratório, a equipe de TI se deslocará até o local para uma análise e se for o caso, justificada a urgência e possibilidade de solução, o incidente poderá ser sanado *in-loco.*
4 – A equipe de TI atende ao chamado *in-loco* (se urgente) ou no próprio setor em atendimentos normais.
5 - Após o atendimento do chamado o solicitante é informado da conclusão/resolução do chamado via *e-mail* de sistema e é convidado a validar ou não o chamado;

6 - Para casos de urgência há *hardwares* da *backup* já prontos para serem substituídos minimizando dessa forma o impacto causado pelo incidente.

7.4.2 Equipamentos institucionais de servidores:

1 - Incidentes em equipamentos de uso dos servidores do *Campus* serão reportados ao setor de TI por meio de envio de um *e-mail* de suporte pelo endereço suporte@veranopolis.ifrs.edu.br. Da mesma forma que os chamados com equipamentos de laboratórios, o *e-mail* gera um chamado no sistema GLPI do *Campus*.
Obs: Caso não seja possível acessar o *e-mail* ou o chamado seja de extrema urgência e comprometa as atividades, poderá o chamado ser aberto via ramal telefônico.
2 - A partir da abertura do chamado é agendado o atendimento e há uma interação entre demandante do chamado e a equipe de TI com notificações por *e-mail* a cada ação executada do respectivo chamado.
O demandante também pode acompanhar acessando o sistema de suporte GLPI diretamente.
3 - Caso o problema impeça o andamento das atividades do servidor, a equipe de TI se deslocará até o local para uma análise e se for o caso, justificada a urgência e possibilidade de solução, o incidente poderá ser sanado *in-loco.*
4 - Caso o incidente resulte em um problema de maior monta e com demora de atendimento mediante a gravidade do incidente, o setor de TI poderá disponibilizar equipamento de *backup* provisório para o servidor continuar suas atividades funcionais.

7.5 Indisponibilidade em Ativos de Rede

1 – O chamado é aberto junto ao setor de TI.
2 – A equipe de TI identifica o ativo com incidente e realiza uma avaliação prévia.
3 – A equipe de TI informa aos setores via *e-mail* caso seja possível ou via ramal telefônico a situação do incidente e a previsão de reestabelecimento da normalidade.
4 – Há alguns ativos de rede de *backup* como *switches* e *acces point* para os casos que houver comprometimento do ativo pelo incidente, nesse caso, a solução envolve a substituição do ativo.
5 – A equipe de TI busca a solução mais viável e breve para reestabelecer os serviços.
6 – A equipe de TI comunica a todos os servidores sobre a solução do incidente e do reestabelecimento dos serviços.

7.6 Virus e Malwares

1 – Apesar da rede de dados do *Campus* ser protegida por *Firewalls* e com usuários identificados, esta está suscetível a infecções por vírus e *malwares* que podem comprometer o funcionamento da rede. Em caso de identificação de comportamentos suspeitos de vírus na rede, a equipe de TI de imediato abre um chamado para registro.
2 – A equipe de TI busca identificar a fonte de infecção e neutralizar a ameaça dentro do possível.
3 – Em caso de confirmação que algum equipamento esteja infectado por vírus, o equipamento é imediatamento isolado da rede até que esteja seguro para ser adicionado novamente.
4 – Em caso de ser equipamento institucional a equipe de TI toma as providências e contorna o problema; em caso de ser equipamento ou dispositivo de uso pessoal de servidores ou alunos, o proprietário é avisado e orientado para que providencie a limpeza da ameaça antes de ter o equipamento ou dispositivo adicionado novamente à rede.
5 – Em caso de identificação de infecção de equipamentos ou ativos de rede, a equipe de TI imediatamente realizará a desinfecção garantindo que o equipamento ou ativo volte a operar de forma a não oferecer mais risco à rede de dados do *Campus*.

7.7 Ataque Cibernético

1 – Por padrão de segurança, todas as portas de entrada externa para a nossa rede estão bloqueadas, porém, ainda assim a rede é passível de invasões externas bem como internas. A equipe de TI realiza dentro do possível, monitoramento da rede e em caso de identificação de invasão um chamado é registrado.
2 – Será avaliada a fonte do ataque e contornada a vulnerabilidade.
3 – Será realizada uma análise para novas políticas de segurança e revistas as atuais.
4 – O chamado é encerrado.

7.8 Falha Humana

1 – A falha humana também deve ser considerada no universo dos incidentes. Nesse caso a equipe de TI sempre busca orientar e capacitar os usuários sobre utilização de equipamentos e serviços para que o mau uso não resulte em incidentes.
Incidentes por falha humana acontecem e são tratados conforme um outro incidente qualquer mediante abertura de chamado.
2 – Recebendo o chamado a equipe de TI atua conforme procedimento já descrito em falhas de *hardware* ou sistema.
3 – O usuário é orientado acerca do incidente de falha humana como forma de previnir futuros incidentes e dependendo do nível de falha humana a gestão é comunicada.
4 – Uma análise de histórico de falhas humanas pode resultar em políticas de treinamento de usuários para que as falhas sejam minimizadas.

7.9 Ambiente Inadequado de Operação

1 – Preventivamente a equipe de TI busca neutralizar ambientes inadequados como equipamentos operando em terperaturas ambientais altas. Nesse caso, busca-se climatizar o ambiente do CPD do *Campus*. Caso incidentes ocorram o chamado é registrado.

2 – O chamado é atendido pela equipe de TI e, em caso de incidente que ocorreu por algum ambiente de operação inapropriado como muito próximo a redes elétricas etc, o passo seguinte é retirar os equipamentos do ambiente ou contornar a situação neutralizando a ameaça causada por operar em ambiente inapropriado.

7.10 Falta de material de manutenção/reposição

A neutralização de um incidente, hipótese acidental ou emergência depende de o setor estar precavido com materiais apropriados e peças básicas de reposição para ativos, equipamentos e computadores. Nesse caso, o setor de TI demanda material de consumo para que no caso de chamados tenha-se capacidade de atuar neutralizando o incidente.

8. CONTROLES PREVENTIVOS E ESTRATÉGIA DE RECUPERAÇÃO

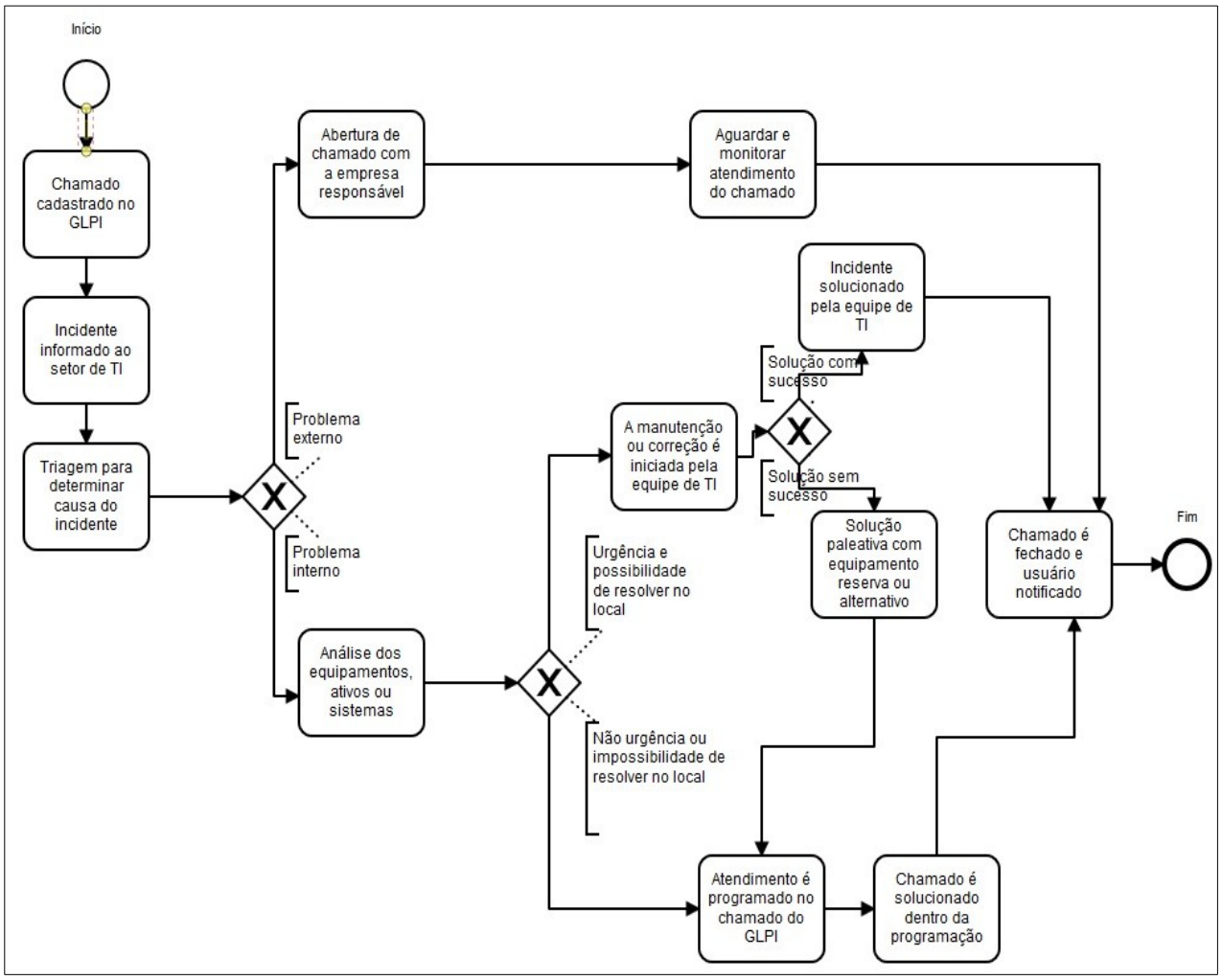
1 - O Setor de TI mantém *hardwares* de *backup* assim como imagens de sistemas de *backup* para restauração imediata no CPD mediante incidentes críticos que não possibilitem a recuperação dos que estavam em operação.
2 - Sempre que possível o setor de TI manterá *hardwares* – computadores e/ou *notebooks* – de *backup* para contornar imediatamente incidentes com computadores dos laboratórios ou de usuários servidores.
3 - Sempre que possível o setor de TI mantém ativos de rede como *switches* e *access points* de *backup* para susbstituição imediata em caso de incidentes que comprometam algum ativo de rede.
4 – O setor de TI, dentro do possível, manterá uma reserva de materiais para manutenção de equipamentos e ativos de rede visando resolver incidentes que demandem por substituição de peças.
5 - Os usuários servidores terão mais de uma impressora cadastrada em seus computadores para que em caso de incidente em uma das impressoras a outra possa ser utilizada sem prejudicar as atividades institucionais.
6 – Mediante demanda, necessidade ou como política de bom uso, o setor de TI promoverá anualmente, pelo menos uma das atividades informativa, de treinemento ou conscientização com a comunidade sobre o uso consciente e responsável da estrutura de TI.

9. MANUTENÇAÕ PREVENTIVA

1 - Anualmente o *no-break* e seu banco de baterias deverá receber manutenção preventiva realizada por empresa técnica especializada;
2 - Se possível, anualmente os projetores deverão receber manutenção preventiva especializada;
3 - Anualmente o sistema de climatização do CPD deverá receber manutenção preventiva especializada.
4 – Semestralmente, nos recessos escolares, os computadores dos laboratórios receberão manutenção preventiva e revisão para que estejam em condições ideais de uso no decorrer do semestre letivo subsequente assim como os computadores dos servidores em geral.

10. FLUXO DE TRATAMENTO DE INCIDENTES

O diagrama abaixo demonstra o fluxo que será seguido mediante hipótese acidental, incidente ou urgência mediante abertura de chamado.



11. COMUNICAÇÃO DE INCIDENTES

11.1 Quem deve comunicar

Qualquer servidor que detecte qualquer tipo de problema que diga respeito a sistemas, equipamentos, ativos de rede e/ou infraestrutura de TI.

11.2 A quem comunicar

A comunicação deve ser feita ao Setor de TI do *Campus* Avançado Veranópolis.

11.3 Como comunicar

Os problemas detectados devem ser reportados ao setor de TI por uma das alternativas:

a) Sistema de suporte GLPI através de email suporte@veranopolis.ifrs.edu.br;

b) Diretamente por ramal telefônico pelo número 2302 quando a situação for de extrema urgência com posterior abertura de chamado no sistema de suporte GLPI através do e-mail ou diretamente no sistema.

Veranópolis 02 de dezembro de 2021.