SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG

PROITI/CGTI - CENTRO DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

PLANO DE CONTINGÊNCIA, CONTINUIDADE E REDUNDÂNCIA N° 1, DE 27 DE FEVEREIRO DE 2023

1. Objetivo

O objetivo deste plano é fornecer segurança, previsibilidade e agilidade na solução de incidentes e falhas em equipamentos, sistemas e serviços de Tecnologia da Informação (TI), os quais podem ter impacto na comunidade, nos processos administrativos e acadêmicos, tanto em nível pessoal quanto institucional. O presente documento serve como um guia procedimental que deve ser seguido para garantir a integridade institucional, detalhando as principais ocorrências previstas, seus respectivos riscos e as medidas e ações a serem tomadas em ocasiões críticas de mitigação e suporte.

2. Aplicação

Este documento é aplicável a todos os sistemas, serviços e equipamentos de TI da Universidade Federal do Rio Grande - FURG, em todos os seus campi e prédios.

3. Definições

Área atingida: refere-se à área impactada pela extensão dos efeitos gerados por um evento de falha.

Área de risco: designa a área que sofre fortes efeitos negativos quando atingida pelas consequências de uma emergência; dependendo do incidente, pode incluir, por exemplo, laboratórios de informática, salas administrativas, datacenter e outros locais que possuam equipamentos de informática.

Backup: trata-se de uma cópia completa ou incremental de servidor, informação ou sistema, armazenada em um ou mais dispositivos.

Contingência: conjunto de ações e planos para lidar com possíveis eventos que possam afetar a disponibilidade, integridade e confidencialidade de sistemas e dados; é uma medida preventiva e de segurança para minimizar prejuízos em situações de emergência.

Datacenter: ambiente projetado para hospedar equipamentos de firewall, servidores, switches, roteadores, storages e no-breaks.

Dynamic Host Configuration Protocol (DHCP): Protocolo de Configuração de Host Dinâmico.

Domain Name System (DNS): Sistema de Nomes de Domínio.

Emergência: designa uma situação emergencial causada por incidente, que possui grandes chances de resultar em danos em ativos ou recursos de TI.

Firewall: sistema de segurança de rede de computadores que restringe o tráfego da Internet para, de ou em uma rede privada; esse software ou unidade de *hardware-software* dedicada funciona bloqueando ou permitindo pacotes de dados seletivamente.

Incidente: refere-se a um evento inesperado ou anormal, que pode ou não causar danos de diferentes

proporções aos ativos e recursos de TI.

Intervenção: atividade executada pelas equipes técnicas para solucionar um incidente, de acordo com os planos de ações para corrigir ou minimizar danos aos ativos e recursos de TI.

Objeto de restauro: serviço, sistema, configuração ou conjunto de arquivos que necessitam ser restaurados de backup institucional posterior a um desastre ou incidente.

Network Address Translation (NAT): -Tradução de Endereço de Rede.

SEI-FURG: Sistema Eletrônico de Informações da FURG.

Sistemas FURG: refere-se ao sistema institucional da FURG, que engloba os diferentes módulos e processos administrativos e acadêmicos (https://sistemas.furg.br).

TI: Tecnologia da Informação.

4. Responsabilidades

4.1 Equipes de Tecnologia da Informação

As áreas responsáveis pelo gerenciamento de incidentes de TI na FURG são incumbidas de agir preventivamente e ativamente em casos de incidentes, com o objetivo de evitar, controlar ou corrigir qualquer ocorrência que afete ativos ou recursos de TI institucionais, independentemente de sua localização, seja na FURG ou fora dela. É importante ressaltar que situações em que acordos ou termos de cooperação definam outros responsáveis ficam excluídas dessa responsabilidade.

4.2 Servidores

Responsáveis por notificar o setor de TI em caso de suspeita ou constatação de acontecimento, ato ou previsão de incidente. A comunicação deve ser realizada pelos canais oficiais ou em contato direto com os responsáveis, caso detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis dos Campi.

5. Classificação de Incidentes

Os possíveis incidentes cobertos por este plano podem ser classificados conforme a lista abaixo, auxiliando em especificar o tipo de atendimento requerido e na definição de sua criticidade.

1. Conteúdo abusivo: spam, assédio, etc;
2. Código malicioso: *bot, worm,* vírus, *trojan, spyware, scripts*;
3. Prospecção por informações: varredura, *sniffing*, engenharia social;
4. Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;
5. Intrusão: Acesso lógico indesejável, comprometimento de conta de usuário, comprometimento de aplicação;
6. Indisponibilidade de serviço, equipamento ou informação: negação de serviço, sabotagem, falha física de equipamento, defeito ou rompimento de fibras ou cabos, etc.;
7. Segurança da informação: acesso não-autorizado à informação, modificação não autorizada da informação;
8. Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;
9. Outros: incidente não categorizado.

6. Criticidade do Incidente

A classificação de criticidade de incidentes auxilia em determinar a prioridade nas ações de mitigação:

1. Alta (impacto grave): incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;

2. Média (impacto significativo): incidente que afeta sistemas ou informações não críticas, sem ou com pouco impacto negativo à instituição;
3. Baixa (impacto mínimo): possível incidente em sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

7. Principais Incidentes e Ações de Contingência

7.1 Procedimento de Restauração: Criticidade Alta

Procedimentos de recuperação de backup devem seguir os passos a seguir:

1. Analisar as condições de viabilidade de acordo com os manuais técnicos de instalação do objeto que necessita ser restaurado, seja totalmente ou parcialmente, para funcionalidades ou apenas arquivos;
2. Recriar o objeto de restauração em ambiente controlado e fora do acesso público até que possa ser completamente validado (o restauro deve buscar o ponto anterior mais próximo à data do incidente, exceto em casos em que se conclui que problemas já existiam e podem voltar a ocorrer se o ponto de restauração for utilizado);
3. Verificar as configurações, atualizações, vulnerabilidades de segurança e integrações existentes nos serviços ou equipamentos que compõem o objeto de restauro;
4. Depois que a restauração for concluída, validar o objeto de restauro com os responsáveis pela lógica de negócio e com a equipe técnica responsável pelo restauro;
5. Disponibilizar o objeto de restauro para uso da comunidade e comunicar o incidente às partes interessadas, bem como as consequências do incidente, quaisquer perdas de informação, danos a equipamentos ou problemas adicionais pertinentes à comunidade, com a maior transparência possível, omitindo apenas informações que possam vulnerabilizar a segurança da informação ou pessoas;
6. Realizar análise e auditoria no incidente para identificar meios de evitar novas ocorrências futuras, documentar e tomar as providências necessárias.

7.2 Problemas com Computadores nos Laboratórios: Criticidade Média

A gestão e organização dos laboratórios de ensino da instituição são conduzidas pelos técnicos de laboratório das Unidades Acadêmicas. Recomenda-se que estes realizem um cronograma de manutenção preventiva ao fim de cada semestre, para configuração e prevenção de problemas. Equipamentos com defeito devem ser registrados por meio de uma Ordem de Serviço ao CGTI, via Sistemas FURG, pela secretaria da unidade. Caso alguma informação ou equipamento necessite de atenção especial, essa informação deve ser incluída no pedido. A administração dos equipamentos de reserva é responsabilidade da unidade, e o conserto será realizado de acordo com a disponibilidade de peças e respeitando o processo de manutenção da Divisão de Atendimento e Suporte do CGTI. Instalações personalizadas de softwares específicos dos laboratórios são responsabilidade dos técnicos de laboratórios locais. Os equipamentos que passam por manutenção são devolvidos com a instalação padrão institucional. Para informações ou dúvidas, é necessário criar um chamado no sistema de solicitações do Sistemas FURG.

7.3 Problemas com Computadores Administrativos: Criticidade Média

Estações de trabalho administrativas com defeito precisam ter registro para manutenção por Ordem de Serviço ao CGTI, no Sistemas FURG, pela secretaria, após validação do(s) fiscal(is) setorial(is) de contrato de manutenção na unidade. Caso alguma informação ou equipamento necessite de atenção especial, deve ser informado no pedido. A gerência de equipamentos reservas é responsabilidade da unidade. O conserto será realizado via disponibilidade de peças e respeitará o processo de manutenção da Divisão de Atendimento e Suporte do CGTI. Instalações personalizadas de softwares específicos do fazer administrativo são de responsabilidade dos servidores interessados, no entanto o CGTI pode fornecer apoio técnico se possível e necessário. Os equipamentos que passam por manutenção são devolvidos com instalação padrão institucional. Para informações ou dúvidas, é necessária a criação de

um chamado no sistema de solicitações do Sistemas FURG.

7.4 Problemas com Equipamentos de Rede: Criticidade Alta

A Coordenação de Engenharia de Rede realiza o monitoramento dos equipamentos de rede institucionais e recebe notificações de problemas por meio do módulo de solicitações do Sistemas FURG. Caso os equipamentos apresentem falhas durante o período de garantia, a equipe acionará o fornecedor para substituição. Em caso de manutenção necessária, o equipamento será enviado para a empresa prestadora de serviços ou para a Divisão de Atendimento e Suporte. Caso o equipamento esteja fora da garantia e sem possibilidade de conserto, será encaminhado para análise e eventual Laudo de Baixo pela Divisão de Atendimento e Suporte.

Nos casos de substituição, um novo equipamento será fornecido pelo CGTI para suprir a funcionalidade do anterior. Em situações em que o estoque esteja abaixo do limiar de segurança ou inexistente, será iniciado imediatamente o processo de aquisição de novos equipamentos para atender às necessidades institucionais, respeitando os prazos administrativos de compra e contratação institucionais.

7.5 Problemas de Conectividade: Criticidade Alta

7.5.1 Rede Interna

Para casos de problemas de conectividade, é necessário que o usuário solicite análise e diagnóstico da equipe de Coordenação de Engenharia de Rede por meio do sistema de solicitações da FURG. Caso o diagnóstico indique um problema estrutural, a equipe confeccionará uma Ordem de Serviço para a Pró-Reitoria de Infraestrutura (Proinfra) acionar a empresa terceirizada que efetuará o reparo. Em caso de problemas com cabos ou interfaces de switch, a equipe de redes fará a substituição necessária para restabelecer a conectividade.

A equipe do setor de Engenharia de Rede do CGTI identifica problemas gerais de conectividade por meio de sistemas de monitoramento, que então realiza o diagnóstico em até um turno administrativo desde a descoberta do problema. Em caso de problema estrutural, a equipe confeccionará uma Ordem de Serviço para a Proinfra acionar a empresa terceirizada que efetuará o reparo, e caso seja um problema lógico, os equipamentos serão configurados adequadamente ou substituídos, se necessário.

7.5.2 Internet e Acesso Externo

Para problemas de conectividade gerais, é necessário seguir as seguintes verificações:

1. Coordenação de Engenharia de Rede: verificar se há queda de link junto da Rede Nacional de Ensino e Pesquisa (RNP) e oficializar chamado registrando o problema.
2. Divisão de Segurança da Informação: analisar se o firewall de borda está funcional e configurado adequadamente. Em caso de problema, o setor deverá reconfigurar o equipamento ou substituir hardware redundante para restabelecer o serviço.
3. Coordenação de Serviços de Rede: analisar se os serviços de DHCP, NAT e DNS estão funcionais e realizar procedimentos de correção imediatos para restaurar a conectividade.

Todas as equipes técnicas têm a responsabilidade de manter os interessados informados sobre os avanços nos chamados e nas Ordens de Serviço, assim como fornecer, quando possível, uma previsão de restabelecimento.

7.6 Problemas de Acesso: Criticidade Baixa

7.6.1 Sistemas FURG e SEI

Para solucionar problemas de acesso ao Sistema FURG, segue os seguintes procedimentos:

1. A Divisão de Atendimento e Suporte, por meio do contato direto ou por chamado com a comunidade, acionará a equipe da Coordenação de Serviços de Rede para verificar os servidores de autenticação institucionais, caso detecte um problema técnico e não de uso dos sistemas institucionais.
2. Cabe à Coordenação de Serviços de Rede analisar e ajustar o serviço de autenticação para restabelecer o acesso ao Sistema FURG, caso detectado algum problema;
3. A Coordenação de Sistemas de Informação, por sua vez, deve verificar a integridade das bases de dados, a adequação dos códigos-fonte e o funcionamento das integrações com meios de autenticação externos.

A equipe técnica responsável deve manter os interessados informados sobre os avanços nos chamados e nas Ordens de Serviço, assim como fornecer, quando possível, uma previsão de restabelecimento.

7.6.2 AVA

Para solucionar problemas de acesso nos serviços AVA, é necessário seguir os seguintes procedimentos:

1. A Divisão de Atendimento e Suporte, no contato direto ou por chamado encaminhado pela Secretaria de Educação à Distância (Sead), deverá questionar se o usuário verificou junto aos setores acadêmicos pertinentes se sua matrícula ou vínculo em disciplinas e cursos estão adequados e se consegue autenticar no Sistemas FURG. Caso perceba problema técnico e não de uso, a Divisão deverá acionar a equipe da Coordenação de Sistemas de Informação para realizar a análise e correção necessárias;
2. A Coordenação de Sistemas de Informação, por sua vez, deve verificar a integração entre o sistema acadêmico, projetos ou inscrições ao AVA para corrigir os acessos do usuário.

É importante que a equipe mantenha os interessados informados sobre os avanços no chamado e forneça, quando possível, uma previsão de restabelecimento do serviço.

7.7 Problemas com Falta de Energia Elétrica: Criticidade Média

Para garantir o fornecimento de energia elétrica no prédio do CGTI, é mantido pela Proinfra um gerador, sendo estes responsáveis por sua manutenção, configuração e abastecimento periódico. Em caso de falta de energia elétrica, é necessário constatar o acionamento do gerador do prédio e o restabelecimento do fornecimento de energia aos equipamentos do datacenter.

Os *no-breaks* do *datacenter* estarão em estado de alarme caso não estejam corretamente alimentados. Em caso de falha do gerador, é necessário entrar em contato imediatamente com a Proinfra, preferencialmente com a equipe técnica e, em seguida, com a chefia da unidade. Para esses casos emergenciais, após 20 (vinte) minutos sem o retorno da energia, é importante seguir o procedimento de desligamento seguro dos equipamentos do *datacenter*, a fim de evitar perdas de dados ou de equipamentos.

Além disso, é essencial verificar o funcionamento dos sistemas de ar-condicionado do *datacenter* durante as quedas de energia, a fim de identificar se estão funcionando normalmente ou se precisam de reinicialização ou manutenção. Caso haja problemas, a Proinfra deve ser acionada imediatamente.

7.8 Incidentes de segurança notificados por órgãos de controle: Criticidade Alta

No caso de incidentes notificados por órgãos como o Centro de Atendimento a Incidentes de Segurança (CAIS), recebidos por e-mail oficial institucional, estes são de responsabilidade da Divisão de Segurança da Informação do CGTI, que fará a análise do incidente, mapeará e notificará os envolvidos com intuito de sanar o mais rápido possível os problemas decorrentes do evento. Em caso das notificações internas não surtirem ações para solucionar as causas dos incidentes, a Divisão de Segurança da Informação tem a prerrogativa de solicitar aos outros setores do CGTI bloqueios ou inativações de serviços e equipamentos problemáticos.

7.9 Outros Problemas

Caso ocorra algum problema ou incidente que não esteja contemplado nas orientações deste documento, é importante que seja feita uma solicitação no Sistemas FURG para que as equipes técnicas do CGTI possam realizar uma análise apropriada. Serão buscados os encaminhamentos adequados para solucionar o problema e o solicitante será comunicado das providências adotadas.

8. Redundância de equipamentos e conectividade

8.1 Datacenter

Como boa prática e presando por uma melhor estrutura de TI para a instituição, é importante manter a infraestrutura de datacenter da instituição com redundância máxima. Para isso, são redundantes dentro do datacenter institucional: *no-breaks*; *switches core; switches* de *datacenter*; servidores, *firewall*; *storages*; equipamentos de *backup*; conexões entre equipamentos; alimentação de energia elétrica dos equipamentos; fornecimento de energia elétrica; ar-condicionados.

8.2 Rede de dados

A Coordenação de Engenharia de Rede mantém caminhos redundantes de fibra óptica que permitem melhor disponibilidade de conectividade para os prédios institucionais. São mantidos também equipamentos redundantes prontos para substituição em caso de problemas.

A conectividade dos prédios afastados da instituição é sempre mantida por dois contratos de enlaces, sendo estes por conectividade física ou por rádio.

9. Comunicação

É responsabilidade das equipes técnicas que cuidam dos ativos institucionais comunicar sobre os mesmos aos interessados.

Quando há solicitações ou e-mails, o responsável atribuído na solicitação ou endereçado na mensagem deve manter comunicação contínua com o solicitante. Em casos de exceção, a chefia é responsável pela comunicação. Os encaminhamentos devem ser feitos para casos já previamente acordados ou após alinhamentos entre as equipes. Deve-se informar ao solicitante que a solicitação está sendo encaminhada para a equipe responsável após análise.

Quando incidentes indisponibilizarem o acesso ou uso de serviços ou equipamentos institucionais, os interessados serão notificados de forma adequada por meio de grupos em serviços de mensagens em massa internos ou externos e via e-mail. A notificação deve informar sobre o incidente, seus impactos e as providências tomadas para mitigar o problema. Quando pertinente e possível, deve-se informar também um prazo estimado para o restabelecimento do serviço. A Divisão de Atendimento e Suporte é o setor responsável por realizar essas comunicações.

Todo incidente de criticidade média e alta que envolvam dados pessoais e dados pessoais sensíveis será comunicado ao Comitê Gestor de Proteção de Dados Pessoais - CGPD, para que este faça a comunicação com a Autoridade Nacional de Proteção de Dados - ANPD.

Para os serviços de TI institucionais, são considerados meios oficiais de comunicação os seguintes: Sistemas FURG; SEI-FURG; e-mail institucional do domínio @furg.br; portal institucional; grupo ComunicaCGTI de WhatsApp.

Documento assinado eletronicamente por **Diogo Paludo de Oliveira**, **Diretor**, em 27/02/2023, às 12:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.
