UNIVERSIDADE ESTADUAL DE LONDRINA

ASSESSORIA DE TECNOLOGIA DA INFORMAÇÃO

PLANO DE CONTINUIDADE DE NEGÓCIOS DE TECNOLOGIA DA INFORMAÇÃO

SUMÁRIO

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
28/04/2023	1.0	Criação e aprovação do PCN	GT PCN

1 INTRODUÇÃO

Este Plano de Continuidade de Negócios (PCN) de Tecnologia da Informação (TI) consiste em estabelecer as estratégias e procedimentos de caráter preventivo e de recuperação para garantir a execução das atividades da instituição, que utilizam recursos tecnológicos, com o objetivo de minimizar as interrupções.

Espera-se aprimorar a resiliência em relação aos serviços de TI para garantia do atingimento dos objetivos da instituição mesmo em situações de contingência. Neste contexto, as normas de segurança da informação apontam a prevenção como uma estratégia fundamental de resposta ao inesperado.

As situações improváveis devem ser interpretadas como uma possibilidade, e a partir desta premissa, os preparativos para recuperação devem estar definidos, mesmo com aceitação de alguma degradação com o intuito de manter a continuidade das atividades em modo de contingência até que seja possível a recuperação total.

Neste sentido, este documento contém os procedimentos a serem adotados pelas equipes técnica e administrativa de TI da instituição para assegurar a continuidade de negócios, a recuperação e resposta adequada aos incidentes.

2 METODOLOGIA

Para elaboração deste plano será definido o escopo, os ativos de TI, a análise dos riscos, a avaliação do impacto nos negócios mais críticos, as estratégias de prevenção relacionadas aos ativos e, por fim, a definição dos procedimentos visando o tratamento dos incidentes.

As estratégias preventivas visam garantir o máximo de disponibilidade e, com esta visão, espera-se que os casos de necessidade de acionamento deste PCN em relação à recuperação sejam reduzidos.

Mesmo aplicando os controles preventivos, a instituição não estará imune a ocorrências de incidentes já que há diversos pontos com risco de falha na

infraestrutura da instituição. Sendo assim, serão estabelecidos os procedimentos para tratamento dos incidentes pela equipe de resposta a incidentes seguindo fluxo de tratamento e comunicação determinados.

3 ESCOPO

Este plano tem como objetivo a continuidade de negócios específicos da área de TI com foco na estrutura básica da rede de comunicação de dados e todos os ativos que disponibilizam os serviços de TI localizados na estrutura primária da rede UEL (datacenter da ATI no Campus) e estruturas secundárias do Hospital Universitário, AEHU e Coordenadoria de Processos Seletivos.

4 ATIVOS DE TI

Neste tópico, serão mapeados todos os ativos que integram a infraestrutura necessária para a disponibilidade dos serviços de TI considerando a estrutura predial, dispositivos (*hardware*) e sistemas (*software*).

4.1 INFRAESTRUTURA PREDIAL

A instalação predial é uma infraestrutura básica que requer cuidado e manutenção das condições para acondicionamento adequado com o objetivo de garantir a guarda segura dos equipamentos centrais do *datacenter*.

Deve considerar cuidados para combate a incêndio, prevenção de alagamentos, segurança física contra invasões ou roubos, climatização e proteção das instalações elétricas.

4.2 SISTEMA DE ENERGIA ELÉTRICA

O fornecimento de energia elétrica ininterrupto é requisito essencial e crítico para o funcionamento do datacenter e da rede como um todo.

O sistema funciona em dois modos:

- Primário: quando há fornecimento de energia pela companhia de energia elétrica;
- Secundário/Contingência: Sistema alternativo composto por *nobreaks* e grupo gerador.

O sistema de contingência é o ponto mais crítico da solução uma vez que é acionado em situações pontuais de falta de energia no sistema principal e, sendo assim, não há margem para falhas. Em caso de funcionamento inadequado, pode ocorrer o desligamento abrupto do *datacenter* e isso impacta em todos os serviços de TI (rede, sistemas e Internet) por ser a estrutura central da rede de comunicação de dados. Portanto, devido às constantes falhas na rede elétrica é necessário manter um sistema de contingência em perfeitas condições.

Além da indisponibilidade dos serviços, o desligamento abrupto também pode ocasionar perda de dados, corrupção de arquivos e danos nos dispositivos computacionais já que estes são desenvolvidos para funcionamento ininterrupto. O desligamento é possível em condições controladas considerando programação prévia.

O desligamento abrupto é um cenário totalmente indesejável e deve ser evitado ao máximo e, sendo assim, diversos procedimentos preventivos são necessários para garantir alto nível de disponibilidade que é uma das premissas da segurança da informação. Este tema será analisado com mais profundidade na avaliação do impacto.

4.3 ATIVOS DE REDE DE COMUNICAÇÃO DE DADOS

A rede de comunicação de dados é composta por equipamentos centrais instalados no *datacenter* e equipamentos de distribuição e acesso, instalados nas unidades e conectados por meio de um anel de fibra óptica que percorre o todo o Campus Universitário.

Para manter os ativos de rede em condições adequadas há estratégias preventivas necessárias que englobam especificação técnica, processo licitatório,

instalação, o acompanhamento do tempo de vida e vários outros procedimentos técnicos periódicos. Neste processo deve-se priorizar os equipamentos de rede centrais cujas falhas têm potencial de maior impacto se comparado aos de distribuição.

Abaixo estão relacionados os principais dispositivos computacionais do datacenter:

- *Link* de Internet externo;
- *Firewall* de borda;
- Roteadores;
- *Switches core* (núcleo);
- Servidores;
- *Storage* (armazenamento de dados).

Na sequência estão relacionados os componentes da rede para conectividade e distribuição do acesso nas unidades. Por segmentar o acesso em unidades específicas, tem criticidade menor em relação aos equipamentos centrais, de forma que eventuais falhas afetarão grupos localizados de usuários:

- Anel e derivações de fibra óptica;
- *Nobreaks* dos pontos de convergência do anel óptico;
- *Switches* de distribuição;
- *Switches* de acesso;
- Pontos de acesso Wi-fi;
- Cabeamento de rede;
- Computadores, tablets, smartphones e outros dispositivos (*endpoints*).

4.4 Sistemas e Dados

A instituição disponibiliza uma grande quantidade de serviços de TI para as mais diversas funcionalidades por meio de sistemas que podem ser utilizados pela área administrativa e acadêmica.

Para garantir a disponibilidade desses sistemas há várias abordagens de prevenção de acordo com o tipo do sistema e seu fornecedor. De forma geral, os sistemas básicos e de infraestrutura de rede são disponibilizados pelos próprios fornecedores do *hardware* ou adquiridos à parte.

Já os de uso administrativo e acadêmico podem ser desenvolvidos pela própria equipe de desenvolvimento de sistemas da instituição ou obtidos por meio de contratação de empresas terceirizadas.

Algumas estratégias específicas para sistemas são necessárias, sem prejuízo daquelas relacionadas à infraestrutura básica. As ações podem variar de acordo com o tipo do sistema e a forma como foi disponibilizado.

4.4.1 Sistemas Básicos de Rede e Infraestrutura

Os sistemas básicos são aqueles serviços que juntamente com os dispositivos computacionais possibilitam a hospedagem dos serviços aos usuários finais. Alguns são visíveis somente pelas equipes de TI para gerenciamento e controle dos serviços e outros podem ser acessados diretamente pelo usuário final como um serviço. Podem ser classificados como:

- **Serviços de *hardware*:** são aqueles instalados para possibilitar o funcionamento do *hardware* (computadores, servidores e dispositivos em geral). Geralmente são fornecidos pelo fabricante ou por meio de *download* de *software* livre (ex. sistemas operacionais).

- **Serviços de infraestrutura:** monitoramento da rede, *firewall* (segurança cibernética), *backup*, banco de dados, base de dados dos usuários e virtualização.

- **Serviços aos usuários:** servidor de arquivos, gerenciamento de projetos e servidor de aplicação.

Especificamente sobre o monitoramento da rede, a equipe precisa dispor de ferramentas que permitam acompanhar o comportamento dinâmico do tráfego da informação visando a atuação preventiva na medida em que possibilita a realização do diagnóstico para posterior execução das estratégias de correção. Em caso de incidentes, colaboram para coleta de evidências e geram informações para melhorias na segurança por meio de arquivos de registro de eventos (*log*):

- *Firewall* (segurança cibernética);
- Monitoramento da rede;
- Sistemas operacionais.

Também há sistemas para atividades específicas relacionadas à gestão da estrutura computacional que possibilitam a criação e gerenciamento de servidores, serviços gestão e segurança dos usuários e programação de medidas de segurança. Consistem na estrutura para instalação e hospedagem dos sistemas e serviços que ficarão disponíveis ao usuário final:

- Software de virtualização de servidores (*hypervisor*);
- Sistema Gerenciador de Banco de Dados;
- Sistemas de gestão de identidade e acesso (LDAP, Keycloak, Controle de Acesso no Sistema UEL, Google OAuth, CAFe, autenticação Wi-Fi);
- Rede privada virtual (VPN para acesso remoto);
- Servidor de arquivos

4.4.2 Sistemas Próprios

Trata-se dos sistemas desenvolvidos pela própria equipe de analistas da UEL, para as mais diversas finalidades de gestão. Para funcionamento adequado, as estruturas citadas nos itens anteriores devem estar em pleno funcionamento. Seguem alguns exemplos:

- Sistema UEL;
- Sistema de Venda de Créditos do RU (Totem de autoatendimento);
- Aplicativo UEL Mobile;

- Sistemas do HU (Hospital Universitário);
- Sistemas da COPS (Processos Seletivos/Vestibular).

4.4.3 Sistemas Fornecidos por Terceiros

Quanto aos sistemas fornecidos por terceiros, há dois tipos de instalação: local ou em nuvem. Os sistemas instalados localmente dependem totalmente da infraestrutura de TI da UEL. Já os sistemas em nuvem dependem da estrutura básica de rede com acesso à Internet. Seguem alguns exemplos:

- Nuvem:
    - Google Workspace;
    - Microsoft 365;
    - Portal de Periódicos (OJS);
    - Protocolo Digital eProtocolo;
    - Sistema da Biblioteca Pergamum.

- Local:
    - Repositório Acadêmico - RA-UEL;
    - Sistema de Catracas (RU/BC/Moradia) - PRIME;
    - *Business Intelligence* (BI) - Qlik Sense;
    - Sistema de RH - Ergon;
    - Sistema de Gestão Hospitalar HU - DGS Brasil.

4.4.4 Dados

Os sistemas próprios e de terceiros realizam coleta e tratamento de dados. Estes são ativos digitais essenciais para o funcionamento do negócio. Armazenados em banco de dados e servidor de arquivos, são os ativos que circulam em meio à infraestrutura de rede de comunicação de dados.

5 AVALIAÇÃO DO IMPACTO

Conforme relatado anteriormente, são diversos os ativos que permitem a disponibilização de serviços de TI. O datacenter é a estrutura central que agrega os principais componentes, formando um ambiente de missão crítica com a exigência de prover 100% de disponibilidade dos serviços 7 dias por semana, 24 horas por dia.

No *datacenter* são concentrados os principais dispositivos de rede e de sistemas (servidores, *racks*, *switches* etc) que atendem aos usuários do Campus e unidades externas (HU, SAUEL, EAAJ e demais órgãos suplementares).

Desligamentos programados são admitidos desde que haja o devido planejamento, assim como aviso prévio à comunidade. São eventos raros e admissíveis em situações muito específicas e que devem seguir uma sequência de procedimentos pela equipe (*checklist*), levando entre 20 a 30 minutos para conclusão com tempo semelhante necessário para a reativação dos serviços.

Desligamentos abruptos podem danificar equipamentos de função crítica que, muitas vezes, têm custo elevado e eventuais falhas nos mesmos podem colocar em risco a continuidade das atividades da UEL. Em casos extremos pode incorrer em perda de dados. Não é possível estimar o tempo para a recuperação desses serviços em casos como estes, podendo levar dias ou até semanas para total restabelecimento. No caso de perda de dados, algumas situações podem ser irreversíveis.

Estes desligamentos mobilizam as equipes de TI para recuperação dos serviços, avaliação dos impactos, correções e eventuais compras de equipamentos em regime de urgência. A disponibilidade total leva em torno de 50 minutos no melhor cenário. As tarefas das equipes são interrompidas e os projetos são impactados. Os atendimentos de suporte se multiplicam, sobrecarregando toda a equipe.

Todos os serviços de TIC ficam indisponíveis, impactando todos os usuários de rede (cabeada ou sem-fio), sistemas e Internet, refletindo negativamente na confiança da comunidade nos serviços oferecidos. O público impactado envolve toda

a comunidade de 17.930 estudantes (graduação e pós-graduação), 4.273 servidores (docentes e servidores efetivos e temporários). Também há impacto nos serviços prestados ao cidadão, considerando os milhares de atendimentos realizados pelos órgãos suplementares da UEL que dependem dos serviços de TIC para funcionamento como HU, AEHU, COU, EAAJ, HV, Colégio de Aplicação, Museu entre outros.

Especificamente, ficam indisponíveis o Sistema UEL (controle administrativo, financeiro SICOR, acadêmico de graduação e pós-graduação, Hospital de Clínicas, Hospital Veterinário, PCU, SAUEL, SEBEC, EAAJ, Biblioteca, Portais do Estudante de Graduação e Pós-Graduação, Servidor e Docente), centenas de páginas de Internet, Aplicativo UEL Mobile e Sistema de Recursos Humanos (Ergon) e os Sistemas de Gestão Hospitalar do HU.

A indisponibilidade da Internet (cabeada ou sem-fio) impede os imensuráveis acessos aos diversos sistemas de informação externos como os sistemas governamentais, Protocolo Digital (eProtocolo), Internet Banking, Autoatendimento RU, ferramentas do Google utilizadas em atividades remotas, Microsoft 365 e vários outros. O impacto atinge todo o Campus e demais unidades administrativas externas. Especificamente no caso do HU fica interrompido o acesso aos sistemas do cartão nacional de saúde, regulação de leitos e exames laboratoriais (GSM-NAT). O Ambulatório de Especialidades (AEHU), que fica no Campus, fica totalmente sem comunicação com os sistemas hospitalares e prontuário eletrônico do paciente. O sistema de registro de ponto eletrônico do HU fica indisponível no AEHU, COU e HV. No caso do EAAJ, o acesso aos sistemas jurídicos ficam indisponíveis e o atendimento ao cidadão prejudicado.

A UEL participará como futuro ponto de agregação da REDECOMEP, terá como responsabilidade providenciar uma parte dos recursos técnicos para o funcionamento da rede, já que haverá convergência das conexões das instituições mencionadas junto ao datacenter da UEL/ATI. Eventuais falhas poderão impactar nos serviços de Internet nas instituições mencionadas quando a rede estiver ativa, amplificando ainda mais os impactos e o público atingido.

Com o advento da pandemia, muitas atividades administrativas e acadêmicas passaram a ser realizadas remotamente e foram mantidas neste formato mesmo após o retorno presencial. Pode ocorrer interrupção do serviço aos participantes que estiverem conectados à rede UEL, causando interrupção dos eventos, aulas, reuniões, apresentação de defesas entre outras atividades.

Neste contexto, este plano considera a estrutura básica como foco de atenção principal devido aos impactos mencionados nesta seção. São definidas estratégias para prevenir os desligamentos e serão estabelecidas rotinas para recuperação.

Este plano também prevê estratégias que vão além da estrutura básica para que sejam garantidas as premissas da segurança da informação (disponibilidade, integridade, confidencialidade e autenticidade). Na próxima seção serão tratadas as demais estruturas cujos riscos devem ser controlados por meio de estratégias a serem gerenciadas e executadas periodicamente pelas equipes de TI.

6 ESTRATÉGIAS DE PREVENÇÃO

O foco central deste PCN é o controle dos riscos por meio de procedimentos preventivos. Assim, espera-se melhor controle, qualidade dos serviços e baixa ocorrência de incidentes.

Parte crucial deste plano é a garantia da execução das estratégias e atividades preventivas em todas as dimensões dos serviços de TI. Caberá aos gestores das equipes de TI acompanhar semestralmente a execução das estratégias e atividades de acordo com suas atribuições aplicando um modelo de melhoria contínua.

O relatório com o detalhamento das atividades mínimas recomendadas encontra-se no Anexo I e engloba atividades voltadas ao cuidado das instalações físicas e infraestrutura elétrica, até questões técnicas específicas de TI como atualizações, *backup*, redundância. Também prevê ações de gestão administrativa para garantir a contratação, manutenção e execução de contratos.

Em caso de não adequação, os gestores das equipes de TI deverão fazer os encaminhamentos técnicos e administrativos necessários para atendimento pleno da estratégia. Importante que os encaminhamentos estejam alinhados com o cronograma dos planos de compras anuais da instituição quando for o caso.

Novos parâmetros podem ser adicionados ao relatório sempre que surgirem situações que possam resultar em amadurecimento das estratégias. Também, é recomendável manter relatórios e planejamentos das ações de forma detalhada quando a complexidade exigir.

7 PROCEDIMENTOS PARA TRATAMENTO DE INCIDENTES

7.1 Equipe de Respostas a Incidentes de Segurança Computacional (ERI)

A equipe técnica responsável pela resolução dos incidentes de segurança da informação será composta pela equipe abaixo e a comunicação com o grupo será realizada por meio de página na Internet disponível por meio do link https://www.uel.br/ati/eri.

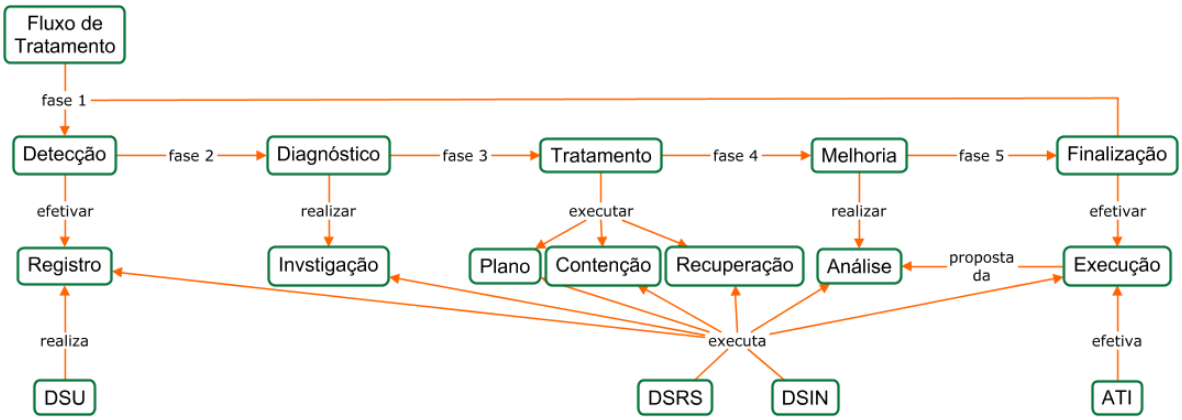
Sigla	Equipe	Responsabilidades
ATI	Assessor de TI (Direção)	● Coordenação ● Comunicação às autoridades superiores, Encarregado de Proteção de Dados Pessoais e ao Comitê de Segurança de TI
DSRS	Diretoria de Suporte a Redes e Sistemas	● Execução das ações de mitigação ● Proposição e execução de ações de melhoria após o incidente. ● Monitoramento pró-ativo.
DSIN	Divisão de Segurança da Informação	● Avaliação dos impactos do incidente ● Estabelecer medidas para mitigação e evitar reincidências ● Relatórios de incidentes periódicos ao CSTI ● Monitoramento pró-ativo
DSU	Diretoria de Suporte ao Usuário	● Recebimento e direcionamento dos incidentes ● Apoio à continuidade em modo de

Sigla	Equipe	Responsabilidades
		contingência ● Monitoramento pró-ativo

7.2 FLUXO DE TRATAMENTO DE INCIDENTES

O tratamento dos incidentes deverá seguir um fluxo determinado considerando o momento em que foi detectado até a sua finalização. A finalização considera um processo de melhoria contínua, ou seja, além de resolver a ocorrência, é necessário desencadear ações com o objetivo de entender o fato ocorrido, estabelecer e implementar as medidas de caráter corretivo com o objetivo de evitar reincidências.

Fase	Descrição	Responsáveis
1 - Detecção	Registro do incidente pela equipe, por meio das ferramentas de gestão de incidentes, ou passiva, por meio de relatos externos.	DSRS / DSIN / DSU
2 - Diagnóstico	Investigação e origem dos incidentes, coleta de evidências, escopo, priorização (matriz GUT), comunicação e documentação.	DSRS / DSIN
3 - Tratamento	Planejamento e execução das ações de contenção, recuperação com retorno dos serviços afetados e mitigação dos impactos.	DSRS / DSIN
4 - Melhoria	Análise e definição dos procedimentos para evitar reincidência do incidente (melhoria contínua).	DSRS / DSIN
5 - Finalização	Execução da melhoria proposta no item anterior.	DSRS / DSIN / ATI



7.2.1 Priorização

Para determinar a prioridade de um incidente, a ferramenta utilizada é a matriz GUT[1], que contém os 3 parâmetros baseados nas necessidades de um projeto ou incidente:

1) Gravidade: qual o impacto do problema?
2) Urgência: a solução pode esperar ou deve ser realizada imediatamente?
3) Tendência: o que acontece se nenhuma ação foi tomada?

Valor	Gravidade	Urgência	Tendência
5	Extremamente grave	Necessária ação imediata	A situação vai agravar rapidamente
4	Muito grave	Alguma urgência	A situação vai piorar em pouco tempo
3	Grave	O mais cedo possível	A situação vai piorar a médio prazo
2	Pouco grave	Pode esperar (aguardar)	A situação vai piorar, mas a longo prazo
1	Sem gravidade (sem risco)	Não tem pressa alguma (pode ser programada / agendada)	A situação não vai piorar e pode até melhorar

[1] *Elaboração do Plano Diretor de Tecnologia da Informação (PDTI) ENAP acessado em 06/03/2023.*

Para avaliar a pontuação do nível de prioridade, basta efetuar o cálculo GUT = G x U x T. Quando houver vários incidentes simultâneos, o que tiver o valor mais alto deverá ser priorizado.

7.3 Comunicação

A comunicação entre as equipes e autoridades é uma atividade essencial para que o tratamento dos incidentes seja realizado de forma tempestiva e de acordo com a legislação de proteção de dados pessoais.

Para a comunicação interna da equipe técnica, as ferramentas de comunicação do tipo *chat* são essenciais para acionamento das equipes responsáveis e a instituição deverá disponibilizar os recursos necessários, considerando:

- Definição de uma ferramenta principal e alternativas;
- Estabelecimento de equipe de plantão;
- Substitutos em cargos de chefia.

Em relação à comunicação com as autoridades, o Encarregado de Dados Pessoais (DPO) será informado quando os incidentes envolverem dados pessoais, apresentando relatório de avaliação detalhado. O DPO, por sua vez, avaliará a necessidade de comunicação à ANPD (Autoridade Nacional de Proteção de Dados). A comunicação deve ser feita por meio de formulário próprio disponível na página da ANPD por meio deste link:

7.4 Ferramentas

A equipe deverá dispor de ferramentas para a execução das tarefas de tratamento de incidentes em tempo adequado à legislação. Abaixo estão listadas algumas opções, mas outras poderão ser adicionadas conforme a necessidade:

Objetivo	Ferramenta
Comunicação equipe	● Aplicativo de mensagens instantâneas Google Chat (principal); ● Grupo ERI Whatsapp; ● Lista telefônica da equipe (alternativo); ● Outros meios disponíveis (alternativo).
Comunicação oficial às autoridades	● Protocolo digital eProtocolo.
Comunicação público interno / externo	● Página da ERI na Internet. ● E-mail de contato com a equipe.
Coleta / análise de evidências	● Firewall; ● Monitoramento; ● Análise de *logs*; ● Sistema de detecção/prevenção de intrusão; ● Técnicas de forense digital; ● Sistemas internos.
Registro do incidente	● Formulário Anexo II; ● Repositório dos registros de incidentes.
Recuperação	● *Backup* de dados; ● Site alternativo.

7.5 CENÁRIOS DE RECUPERAÇÃO

As estratégias de prevenção devem ser atendidas plenamente, porém, não há garantia de que serão suficientes para afastar todo o tipo de incidente. Conforme detalhado no Anexo I, os fatores de risco são diversos e a cobertura total de todos os itens é um desafio a ser assumido pela instituição como um todo.

Com a prevenção, espera-se afastar os incidentes mais graves que podem ocasionar perda ou vazamento de dados, tempo de inatividade e custos de reputação. Também, é objetivo reduzir os incidentes menos graves, liberando a equipe de TI para desenvolver novos projetos e melhorias ao invés de despender tempo resolvendo urgências, ou seja, “apagando incêndios”.

De qualquer maneira, a instituição deve estar preparada porque um incidente pode ocorrer a qualquer momento. Os planos de recuperação detalhados deverão

considerar as especificidades das equipes da ATI, COPS/DDI e HU/GTI e serão resguardados e mantidos restritos para a ERI, por questões de segurança.

Com o objetivo de assegurar o sucesso das operações com o restabelecimento dos serviços, para cada cenário de incidente deve-se estabelecer uma sequência de procedimentos técnicos, treinamento da equipe e testes periódicos. A lista abaixo contém os principais cenários que podem exigir a execução das operações de recuperação:

- Acesso não autorizado a sistemas de informação;
- Alteração/exclusão não autorizada de dados;
- Descarte incorreto de documentos ou dispositivos eletrônicos;
- Divulgação indevida de dados pessoais;
- Envio de dados a destinatário incorreto;
- Exploração de vulnerabilidade em sistemas de informação;
- Falha em equipamento (*hardware*);
- Falha no sistema de contingência de energia elétrica;
- Falha em sistema de informação (*software*);
- Negação de Serviço (DoS);
- Perda/roubo de documentos ou dispositivos eletrônicos;
- Roubo de credenciais / Engenharia Social;
- Violação de credencial por força bruta
- Publicação não intencional de dados pessoais;
- Sequestro de dados (ransomware) com ou sem transferência e/ou publicação de informações;
- Vírus de Computador / *Malware*.

8 CONSIDERAÇÕES FINAIS

Neste documento, foi apresentado um plano de continuidade de negócios específico da área de TI contendo o contexto e as estratégias para garantir o bom funcionamento dos serviços e as premissas da segurança de dados e informações. Com isso, o plano pretende obter o máximo de proteção dos dados pessoais em atendimento à legislação vigente.

Com base nas orientações mencionadas no plano, as equipes que trabalham com TI na instituição poderão criar planos técnicos específicos de acordo com as suas atribuições visando a um processo de melhoria contínua, já que o contexto de segurança cibernética está em constante mudança com novas tecnologias e ameaças cada vez mais complexas e frequentes.

Por fim, essencial para o sucesso do plano é a execução e o acompanhamento pelos gestores envolvidos, sendo que os formulários indicados no Anexo I e II são ferramentas importantes para atingir os objetivos, pois permitem o controle da documentação dos procedimentos. Outro ponto importante é o comprometimento necessário dos gestores de TI, para as questões técnicas, e da alta gestão, para fornecer suporte e patrocínio das ações de melhoria que forem detectadas no decorrer do processo.

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				
Alagamentos	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/devolução de chaves, troca de senhas de acesso etc)				

Estratégia	Atividades	Frequência	Responsável	Está adequado? (S/N/NA)	Providências necessárias
	Vigilância predial contra roubo, invasão ou depredação				
	Controle de acesso de visitantes/prestadores de serviço				
Instalações elétricas internas	Verificação da instalação elétrica (preventivo curto circuito etc)				
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 do grupo	Manter contrato de manutenção ativo				

Estratégia	Atividades	Frequência	Responsável	Está adequado? (S/N/NA)	Providências necessárias
gerador	Fiscalização e gestão do contrato				
	Manutenção preventiva mensal				
	Manutenção corretiva				
	Abastecimento combustível				
	Teste de funcionamento				
Nobreaks	Manter contrato de manutenção ativo				
	Fiscalização e gestão do contrato				
	Manutenção preventiva				
	Manutenção corretiva				
	Teste de funcionamento				
	Teste de autonomia				

4. Ativos de rede

Estratégia	Atividades	Periodicidade	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				

Estratégia	Atividades	Periodicidade	Responsável	Está adequado? (S/N/NA)	Providências necessárias
Backup	Manter cópia de segurança				
	Simulação de recuperação do *backup*				
Sistemas de Redundância	Garantir redundância em todos os dispositivos				

5. Conectividade

Estratégia	Atividades	Periodicidade	Responsável	Está adequado? (S/N/NA)	Providências necessárias
Gestão dos serviços de conectividade Internet (Campus e órgãos suplementares)	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				

Estratégia	Atividades	Periodicidade	Responsável	Está adequado? (S/N/NA)	Providências necessárias
	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	Periodicidade	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				

Estratégia	Atividades	Periodicidade	Responsável	Está adequado? (S/N/NA)	Providências necessárias
	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 (*backup*)	Manter cópia de segurança para os dispositivos críticos (servidores, 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	Periodicidade	Responsável	Está adequado? (S/N/NA)	Providências necessárias
Gestão de mudanças	Planejamento das mudanças mais significativas				
	Controle das solicitações por meio do sistema Atendimento UEL				
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				

Estratégia	Atividades	Periodicidade	Responsável	Está adequado? (S/N/NA)	Providências necessárias
	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				
Controle de acesso	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	Periodicidade	Responsável	Está adequado? (S/N/NA)	Providências necessárias
Contratos	Avaliar a adequação do serviço a ser contratado conforme padrões técnicos definidos pela ATI				
	Manter contrato vigente e gerenciar renovações				

	Acompanhar a aderência do serviço em relação aos padrões da UEL/ATI quando houver alguma alteração				
	Fiscalizar o pleno cumprimento do contrato				

9. Providências necessárias

Providência	Encaminhamento

10. Observações gerais

Londrina, ____ de _____ de _____.

RESPONSÁVEL PELA UNIDADE

Cargo

ANEXO II - RELATÓRIO DE REGISTRO E TRATAMENTO DE INCIDENTE

1. IDENTIFICAÇÃO

Data	Hora	Responsável pelo registro	Origem
Fonte da detecção do incidente		☐ Identificado pela equipe de TI própria ☐ Notificação do operador de dados ☐ Denúncia de titulares/terceiros ☐ Notícias ou redes sociais ☐ Notificação da ANPD ☐ Outro _____	
Descrição da forma como o incidente foi conhecido			

2. DEFINIÇÃO

Descrição	
Escopo	☐ Dados ☐ Dados Pessoais ☐ Infraestrutura de rede ☐ Segurança ☐ Serviços de TI ☐ Outro _____
Tipo	☐ Acesso não autorizado a sistemas de informação ☐ Alteração/exclusão não autorizada de dados ☐ Descarte incorreto de documentos ou dispositivos eletrônicos ☐ Divulgação indevida de dados pessoais ☐ Envio de dados a destinatário incorreto ☐ Exploração de vulnerabilidade em sistemas de informação ☐ Falha em equipamento (*hardware*) ☐ Falha no sistema de contingência de energia elétrica ☐ Falha em sistema de informação (*software*) ☐ Negação de Serviço (DoS) ☐ Perda/roubo de documentos ou dispositivos eletrônicos ☐ Publicação não intencional de dados pessoais ☐ Roubo de credenciais / Engenharia Social ☐ Sequestro de dados (ransomware) com transferência e/ou publicação de informações ☐ Sequestro de Dados (*ransomware*) sem transferência de informações

	☐ Violação de credencial por força bruta ☐ Vírus de Computador / *Malware* ☐ Outro tipo de incidente cibernético Outro tipo de incidente não cibernético
Princípios da SI afetados	☐ Autenticidade ☐ Confidencialidade ☐ Disponibilidade ☐ Integridade
Reincidência	☐ Sim ☐ Não
Informações complementares	

3. DIAGNÓSTICO

Data/hora		**Responsável**	
Análise			
Priorização	**Gravidade (G)**		**Pontuação GUT G x U x T**
	Urgência (U)		
	Tendência (T)		
Impacto			
Necessário informar DPO?	☐ Sim ☐ Não	**eProtocolo**	**Data**
Ações necessárias			
Natureza dos dados pessoais afetados			
Informações sobre os titulares de dados pessoais envolvidos			

4. Tratamento

Data/hora conclusão			**Responsável**	
Ações realizadas				
Informações complementares				
Notificação ao DPO	**Data**		**Protocolo**	

5. Melhoria

Data/hora		**Responsável**	
Medidas de segurança necessárias	☐ Atualização de Sistemas ☐ Controle de acesso físico ☐ Controle de acesso lógico ☐ Cópias de segurança (backups) ☐ Criptografia/Pseudonimização ☐ *Firewall* ☐ Gestão de ativos ☐ Monitoramento de uso de rede e sistemas ☐ Múltiplos fatores de autenticação ☐ Plano de resposta a incidentes ☐ Políticas de segurança da informação e privacidade ☐ Processo de Gestão de Riscos ☐ Proteção de endpoint (Antivírus) ☐ Registro de incidentes ☐ Registros de acesso (logs) ☐ Segregação de rede ☐ Testes de invasão ☐ Outras _____		
Ações necessárias específicas			
Informações complementares			

Londrina, ____ de _____ de _____.

RESPONSÁVEL PELO REGISTRO

Cargo