Resolução 014

Resolução que aprova os Planos de Contingência e Segurança da Informação, de Expansão e Atualização de Equipamentos de TI e Regulamento de Uso da Rede Wifi

2023

| CONSAD

FACULDADE CATÓLICA DE RONDÔNIA

RESOLUÇÃO Nº 014 DE 2023 - CONSAD
RESOLUÇÃO QUE APROVA OS PLANOS DE CONTINGÊNCIA E SEGURANÇA DA INFORMAÇÃO, DE EXPANSÃO E ATUALIZAÇÃO DOS EQUIPAMENTOS DE TI E REGULAMENTO DE USO DA REDE WIFI

Aprova Resolução que aprova os Planos de Contingência e Segurança da Informação, de Expansão e Atualização de Equipamentos de TI e Regulamento de de Uso da Rede Wifi da Faculdade Católica de Rondônia, revogando as disposições em contrário.

Art. 1º Ficam aprovados os Planos de Contingência e Segurança da Informação e de Expansão e Atualização de Equipamentos de TI e Regulamento de Uso da Rede Wifi da Faculdade Católica de Rondônia, nos termos do documento em anexo à presente resolução.

Art. 2º A organização administrativa para o cumprimento dos planos deve ser empreendida conjuntamente pelo setor de tecnologia da informação, coordenação de infraestrutura e direção administrativa.
Parágrafo Único. Eventuais adequações orçamentárias ou contratação de pessoal deve ter proposta encaminhada pela direção administrativa ao CONSAD para deliberação.

Art. 3º Esta Resolução entra em vigor nesta data, revogadas as disposições em contrário, estabelecendo-se o prazo de 12 (doze) meses para o cumprimento integral dos termos do manual.

Porto Velho, 20 de dezembro de 2023

Reitora
Presidente CONSAD

Plano de Expansão e Atualização de Equipamentos de TI

2023

| Direção Administrativa

FACULDADE CATÓLICA DE RONDÔNIA

PLANO DE EXPANSÃO E ATUALIZAÇÃO DE EQUIPAMENTOS DE TI

CAPÍTULO I
DA FINALIDADE E OBJETIVO

Por meio deste documento, a Faculdade Católica de Rondônia (FCR) formaliza e comunica os métodos, técnicas e estratégias adotadas para a atualização e manutenção dos recursos tecnológicos utilizados na instituição. Este documento também tem como objetivo auxiliar na execução das metas objetivas e mensuráveis descritas no Plano de Desenvolvimento Institucional (PDI).

Atualmente, o campus conta com um laboratório de informática com 53 computadores e mais de 98 computadores distribuídos em diversas áreas, todos conectados à infraestrutura de rede cabeada da instituição. Além disso, a FCR disponibiliza acesso à rede Wi-Fi para estudantes, funcionários e visitantes, conforme regulamentado pelo uso da rede sem fio, que segue os princípios educacionais da instituição. Ao todo, são 19 pontos de acesso espalhados pelo prédio, possibilitando conectividade sem fio na execução das atividades acadêmicas e administrativas.

Visando cumprir todos os aspectos relacionados à manutenção, instalação e atualização dos equipamentos tecnológicos, a equipe de tecnologia da informação analisa constantemente a infraestrutura da instituição. Esse processo leva em consideração níveis de qualidade tanto para os acadêmicos quanto para os colaboradores, garantindo a efetividade das operações diante das inovações tecnológicas. Também são incluídos objetivos de otimização e aperfeiçoamento, além da implementação de modelos de infraestrutura, espaço físico e sistemas que promovam a acessibilidade e o atendimento diferenciado para pessoas com deficiências e/ou necessidades educacionais especiais.

CAPÍTULO II
PLANEJAMENTO DE EXPANSÃO E ATUALIZAÇÃO

Para garantir que a atualização dos equipamentos esteja alinhada com os objetivos estratégicos de nossa instituição, é necessário seguir uma abordagem estruturada e bem definida. Primeiramente, é essencial realizar uma análise detalhada das necessidades de crescimento da Faculdade Católica de Rondônia (FCR). Isso inclui a expansão de cursos, o aumento do número de alunos e novas demandas tecnológicas que possam surgir. Identificar as tecnologias emergentes que podem beneficiar a instituição, como novas ferramentas de ensino, softwares educacionais avançados e hardware de última geração, é crucial para manter a FCR na vanguarda da inovação.

Além disso, é imperativo assegurar que todas as atualizações de equipamentos e sistemas estejam em conformidade com a Lei Geral de Proteção de Dados (LGPD). Isso garante a proteção e privacidade dos dados de alunos, professores e colaboradores, cumprindo os requisitos legais e evitando possíveis sanções. Estabelecer metas específicas e mensuráveis para a atualização dos equipamentos também é uma etapa fundamental, essas metas são definidas neste documento.

O planejamento financeiro é outra peça chave. Determinar o orçamento disponível e alocar os recursos necessários para a implementação do plano de atualização é vital. Isso inclui os custos de aquisição de novos equipamentos, instalação, treinamento e suporte contínuo. Garantir que os recursos sejam utilizados de forma eficiente e que as aquisições atendam às necessidades reais da instituição é crucial para o sucesso do plano.

Atualmente, a FCR conta com o seguinte quadro de equipamentos alocados em diferentes espaços:

Equipamentos	Alocação	Quantitativo
Computadores desktop	Salas de aula, sala dos professores, ambientes administrativos, salas de reunião, coordenações, etc.	151
Duas telas (Monitores)	Coordenações e ambientes administrativos.	20
Notebooks	Ambientes administrativos.	10
Scanners	Ambientes administrativos e secretarias.	6
Impressoras	Reitoria, secretaria das coordenações e Núcleo de Prática Jurídicas (NPJ).	4
Nobreaks	Sala de Tecnologia da Informação.	3
Projetores	Clínica de psicologia, laboratório de informática, auditório e TI.	6
Microfones	Setor administrativo (o microfone fica disponível para o uso em salas de aula) e auditório.	5
Webcams	Coordenações, setor administrativo, reitoria, etc.	26
Televisores	Salas de reunião, salas de aula e reitoria.	60
Access Points	Nos corredores espalhados por todo campus.	19
Servidores	Sala de Tecnologia da Informação.	2
Apresentador multimídia	Auditório e setor administrativo.	2
Amplificadores de áudio	Auditório e secretária.	2
Switches de mesa	Reitoria e sala de reunião, salas administrativas.	7
Switches	Setor de T.I e shafts.	13
Tablets	Tablets para consulta de acervo na biblioteca	5

Para o período de vigência deste plano temos como meta a seguinte programação de expansão dos recursos tecnológicos no geral:

Equipamentos	Nº de aquisições	Alocação
Computadores	9	Setor administrativo, setor de relacionamento com o aluno, clínica escola de psicologia, laboratório de saúde, salas de preparação de aula.
Monitores	10	Setor administrativo
Notebooks	10	Setor de TI, biblioteca, clínica escola de psicologia, salas de reunião, auditório e setor administrativo.
NoBreaks	9	Shafts e sala de TI.
Tablets	5	Biblioteca
Scanners	2	Secretaria Administrativo e Reitoria.
Câmeras Fotográficas	2	Estúdio de produções multimídia

A aquisição de novos equipamentos tem como principal objetivo a expansão da infraestrutura existente ou a manutenção de equipamentos de backup, assegurando a continuidade das operações em caso de falhas. Todos os equipamentos atualmente em uso são novos e estão em perfeito estado de funcionamento. A necessidade de novas aquisições é avaliada com base na expansão das atividades institucionais ou na eventual substituição de equipamentos danificados. Essa avaliação é realizada pela equipe técnica responsável, garantindo que as aquisições atendam às demandas específicas da instituição.

CAPÍTULO III
MONITORAMENTO E MANUTENÇÃO

O monitoramento e a manutenção contínua dos equipamentos de TI são cruciais para garantir a eficiência e a longevidade dos recursos tecnológicos da instituição. O processo de monitoramento envolve a observação regular e sistemática do desempenho dos equipamentos, identificando potenciais problemas antes que se tornem críticos. A manutenção, por sua vez, inclui ações preventivas e corretivas, como atualizações de software, substituição de componentes desgastados e ajustes de configurações. Esses processos garantem que os equipamentos funcionem de maneira otimizada, reduzindo o risco de falhas e interrupções nas atividades acadêmicas e administrativas. O monitoramento e manutenção ajuda a prolongar a vida útil dos equipamentos e a assegurar que a infraestrutura de TI continue a atender às necessidades da instituição, por esse motivo utilizamos métricas para definir se um equipamento precisa de manutenção ou ser descontinuado, segue parâmetros e métricas que são utilizadas:

Métricas	Descrição	Indicador
Taxa de Utilização da CPU	Monitore a utilização média da CPU dos computadores.	Se a utilização média da CPU estiver consistentemente acima de 80%, pode ser um sinal de que o computador está sobrecarregado e precisa de atualização.
Utilização de Memória	Monitore a utilização média de memória RAM dos computadores.	Se a utilização média da memória RAM estiver consistentemente acima de 80%, pode indicar a necessidade de aumento de memória ou otimização dos sistemas.
Temperatura Interna	Monitore a temperatura interna dos componentes principais do computador, como CPU e GPU.	Temperaturas consistentemente acima das recomendações dos fabricantes podem indicar problemas de resfriamento e a necessidade de manutenção preventiva.
Tempo de Resposta	Meça o tempo que os computadores levam para iniciar e carregar aplicativos comuns.	Um aumento significativo no tempo de resposta indica que o desempenho está degradado.
Taxa de Falhas de Hardware	Registre a frequência de falhas de hardware como falhas de disco rígido, memória, etc.	Um aumento na taxa de falhas pode indicar que os componentes estão se aproximando do fim de sua vida útil.
Feedback do Usuário	Colete feedback dos usuários sobre a performance e a usabilidade dos computadores.	Comentários negativos recorrentes sobre lentidão ou dificuldades de uso podem indicar a necessidade de atualização.
Compatibilidade de Software	Verifique a compatibilidade dos computadores com os softwares mais recentes utilizados pela instituição.	Se os computadores não conseguem rodar os softwares necessários ou exigem versões mais antigas, pode ser necessário considerar uma atualização.
Tempo de Inatividade	Monitore o tempo de inatividade não planejado dos computadores.	Um aumento no tempo de inatividade pode indicar problemas de hardware ou software que precisam ser resolvidos.
Frequência de Reparo	Registre a frequência com que os computadores precisam de reparos.	Uma alta frequência de reparos pode indicar que os computadores estão obsoletos e precisam ser substituídos.
Atualizações de Firmware/Bios	Verifique se os computadores ainda recebem atualizações de firmware ou BIOS dos fabricantes.	Se as atualizações cessaram, isso pode indicar que o hardware está obsoleto.
Compatibilidade com Novas Tecnologias	Avalie se os computadores são compatíveis com novas tecnologias e periféricos.	A falta de compatibilidade pode indicar a necessidade de atualização do hardware.
Garantia	Verifique o status da garantia dos computadores.	Computadores fora da garantia podem precisar de planos de manutenção preventiva mais rigorosos ou substituições programadas.

CAPÍTULO IV
REVISÕES E GERAÇÃO DE RELATÓRIOS

Para garantir a eficácia do plano de expansão e atualização de equipamentos de TI, é essencial estabelecer prazos regulares para revisões e geração de relatórios. Esses processos ajudam a monitorar o desempenho dos equipamentos, identificar necessidades de atualização e assegurar que as metas estabelecidas sejam alcançadas de forma eficiente, na sequência é compartilhada planilha dos prazos para revisões e geração dos relatórios dos equipamentos.

Prazos	Descrição
Revisões Anuais	Anualmente, todos os computadores do campus são avaliados detalhadamente. Durante essas avaliações, são gerados relatórios que incluem: Taxa de Utilização da CPU, Utilização de Memória, Taxa de Falhas de Hardware, Temperatura Interna, Atualizações de Firmware e BIOS. Esses relatórios são compilados anualmente para cada equipamento.
Inspeções Semestrais e Monitoramento Contínuo	Além das avaliações e da geração de relatórios anuais, é realizada uma inspeção semestral em todos os computadores para identificar quaisquer problemas. Durante essas inspeções, a equipe de TI verifica fisicamente os equipamentos. Os computadores também são monitorados continuamente e verificados imediatamente quando apresentam problemas ou recebem feedback negativo.
Revisões Mensais	São feitas revisões mensais detalhadas nos equipamentos que nos fornecem informações contínuas do estado de funcionamento. Essas revisões incluem ligar o computador, testar softwares e verificar informações relacionadas a utilização de CPU e utilização de memória.

Através dessas práticas regulares de revisão e monitoramento, a infraestrutura de TI da FCR é constantemente avaliada e melhorada, garantindo um ambiente tecnológico eficiente e confiável, capaz de atender às demandas dinâmicas da instituição.

CAPÍTULO V
ACOMPANHAMENTO E ATUALIZAÇÃO DO PLANO

O Setor de Tecnologia da Informação, com a aprovação da direção administrativa, é responsável pela elaboração dos processos de aquisição e contratação de bens e serviços de TI, com o objetivo de acompanhar o crescimento institucional e as inovações tecnológicas. Para isso, são adotadas revisões anuais do planejamento, levando em consideração relatórios e avaliações, detalhadas aqui neste documento, que fornecem descrições detalhadas sobre o desempenho dos equipamentos e a eficácia das soluções de TI em atender às necessidades da comunidade acadêmica. A análise dos relatórios e feedbacks permite verificar o andamento das ações planejadas e identificar possíveis lacunas ou áreas de melhoria. Os acompanhamentos definidos por este plano, permitem a avaliação contínua dos equipamentos e a comunicação entre colaboradores e alunos estabelecendo uma base sólida para o ajuste do planejamento. Essa abordagem centrada no usuário permite que o planejamento de TI seja adaptado conforme o ambiente em constante mudança da instituição de ensino.

O presente plano é revisado e atualizado anualmente, podendo sofrer correções ou adequações a qualquer momento. Essa flexibilidade permite que o plano seja ajustado conforme as necessidades emergentes da instituição e as mudanças no cenário tecnológico. Além disso, a incorporação de feedback dos usuários finais e a análise de métricas de desempenho garantem que as atualizações atendam efetivamente às expectativas e necessidades de todos os stakeholders. Essa prática contínua de revisão e atualização assegura que a infraestrutura de TI da FCR permaneça moderna, eficiente e capaz de suportar o desenvolvimento acadêmico e administrativo de maneira sustentável.

Porto Velho, em 20 de dezembro de 2023

Diretor Administrativo

Plano de Contingência e da Segurança da Informação

2023

| Diretoria Administrativa

FACULDADE CATÓLICA DE RONDÔNIA

PLANO DE CONTINGÊNCIA E DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I
DA FINALIDADE E OBJETIVO

Este Plano de Contingência e de Segurança da Informação da Faculdade Católica de Rondônia (FCR) tem como finalidade fornecer medidas rápidas e eficazes para proteger os processos críticos de TI relacionados aos sistemas essenciais da instituição. Através da implementação de estratégias e procedimentos bem definidos, o plano busca minimizar os impactos negativos que falhas nos serviços de TI podem causar nas operações acadêmicas e administrativas, assegurando a continuidade dos serviços de TI em situações de contingência.

O objetivo deste plano é garantir que as operações acadêmicas e administrativas da FCR não sejam interrompidas por falhas técnicas. Isso inclui minimizar os impactos das falhas, proteger dados e informações sensíveis contra perda e acesso não autorizado, e estabelecer procedimentos claros de comunicação durante emergências. Além disso, o plano assegura a conformidade com normas e regulamentações aplicáveis, garantindo altos padrões de segurança e proteção de dados.

Este documento se aplica a todos os serviços e sistemas de Tecnologia da Informação que são executados na FCR. É importante destacar que cada um dos sistemas terceirizados, como bibliotecas virtuais, sistema educacional, servidores na nuvem e demais serviços terceirizados, possuem seus próprios planos de contingência elaborados pelas respectivas empresas. O plano da FCR é especificamente para os links de internet, energia elétrica e outros itens internos.

CAPÍTULO II
DAS RESPONSABILIDADES

A equipe de Tecnologia da Informação deve fornecer suporte técnico, auxiliando os docentes, discentes e colaboradores em todo trabalho computacional ou que envolva os sistemas corporativos e acadêmicos da instituição. A responsabilidade da equipe inclui administrar o local físico, garantir a segurança e a integridade dos dados, manter a infraestrutura de TI operante e informar a um nível superior sobre os problemas identificados para uma solução rápida e precisa. Além disso, a equipe deve monitorar continuamente os sistemas para prevenir incidentes e realizar backups regulares dos dados.

Os docentes são responsáveis por reportar imediatamente quaisquer problemas técnicos que afetem suas atividades de ensino ao setor de TI, através dos canais estabelecidos (e-mail ti@fcr.edu.br). Devem também seguir as diretrizes e políticas de segurança de TI, proteger as informações sensíveis dos alunos e utilizar os recursos de TI de forma adequada e segura.

Os discentes devem comunicar prontamente qualquer dificuldade técnica ou problema de acesso aos sistemas educacionais ao setor de TI. Devem respeitar as políticas de uso aceitável dos recursos de TI da instituição, proteger suas credenciais de acesso e evitar comportamentos que possam comprometer a segurança dos sistemas de TI.

Os técnico-administrativos são responsáveis por informar o setor de TI ao detectar algum tipo de emergência ou problema técnico que possa afetar suas atividades ou a infraestrutura de TI. Devem seguir as políticas de segurança de TI, proteger dados sensíveis e utilizar os recursos de TI de forma eficiente e segura. Além disso, devem colaborar com a equipe de TI na implementação de medidas de segurança e contingência.

CAPÍTULO III
DOS NÍVEIS DE INCIDENTES

Os níveis de incidentes classificam as falhas em cinco categorias de acordo com sua gravidade e impacto. O Nível I inclui problemas menores que podem ser controlados pela equipe de TI sem afetar significativamente o trabalho, como problemas com periféricos de computadores. O Nível II abrange falhas que impedem o uso de um equipamento ou sistema específico, necessitando de ações como reiniciar o computador ou substituir componentes defeituosos. O Nível III envolve falhas que afetam toda a organização, como queda de energia ou internet, exigindo a ativação de links de contingência e uso de geradores. O Nível IV se refere a problemas que afetam sistemas utilizados por docentes e discentes, como software acadêmico indisponível, requerendo manutenção corretiva e comunicação com os usuários. O Nível V é o mais grave, envolvendo comprometimento de servidores e dados por ataques, necessitando de isolamento, varredura e restauração de backups.

Nível	Descrição	Exemplo	Solução
Nível I	Hipótese acidental que pode ser controlada pela equipe de TI e que não afeta o andamento do trabalho da organização.	Problemas com equipamentos periféricos de computadores.	Substituir ou reparar o equipamento periférico defeituoso.
Nível II	Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo colaborador.	Problemas com o funcionamento do computador (não liga, travando) ou sistema offline.	Reiniciar o computador, verificar e substituir componentes defeituosos, restaurar o sistema offline.
Nível III	Hipótese acidental que impede o uso de sistemas ou equipamentos de toda a organização, impedindo o desenvolvimento do trabalho de todos os colaboradores.	Falha na conexão com a internet ou queda de energia elétrica.	Ativar o link de internet de contingência, utilizar o gerador de energia, contatar o fornecedor de internet/energia.
Nível IV	Hipótese acidental que impede o uso de sistemas para docentes ou discentes, afetando tanto a equipe interna quanto seus respectivos clientes.	Software acadêmico ou portal do aluno indisponível.	Reiniciar o servidor do software acadêmico, realizar manutenção corretiva e informar os usuários sobre o status.
Nível V	Hipótese acidental que impede o uso de sistemas para docentes, discentes e colaboradores, suspendendo ou impedindo todo o trabalho da organização.	Servidores e dados comprometidos por vírus ou ataques.	Isolar o servidor afetado, realizar varredura completa, restaurar backups, reforçar medidas de segurança.

CAPÍTULO IV
DOS PRINCIPAIS RISCOS E ESTRATÉGIAS DE CONTROLE

Listaram-se os principais riscos que podem afetar a continuidade dos serviços de TI na Faculdade Católica de Rondônia. Identificar esses riscos é crucial para preparar respostas adequadas e minimizar os impactos, são eles:

Risco	Descrição	Solução
Interrupção de Energia Elétrica	Causada por fatores externos ou internos, como curto-circuitos, incêndios ou infiltrações.	Utilizar o gerador de energia de 300 kVa e o nobreak na sala de TI para garantir a continuidade das operações.
Falhas na Climatização do DataCenter	Superaquecimento dos ativos devido a falha no sistema de climatização.	Realizar manutenção regular do sistema de climatização e monitorar a temperatura do DataCenter.
Indisponibilidade de Rede/Circuitos	Rompimento de cabeamento devido a obras internas, desastres ou acidentes.	Identificar equipamentos ou cabos com problema e fazer a manutenção.
Falha Humana	Acidentes ao manusear equipamentos.	Treinamento contínuo dos funcionários sobre manuseio adequado e segurança dos equipamentos de TI.
Ataques Internos	Ataque aos ativos do DataCenter e equipamentos de TI por usuários insatisfeitos.	Implementar medidas de segurança internas e monitoramento de atividades suspeitas.
Falhas de Hardware e Software	Necessidade de reposição de peças ou reparo e necessidade de atualização ou reinstalação de sistemas.	Identificar o problema, realizar manutenção ou troca, acionar garantias ou realizar aquisições emergenciais.
Ataques Cibernéticos	Ataque virtual que comprometa o desempenho, os dados ou as configurações dos servidores essenciais.	Isolar o servidor afetado, realizar varredura completa, restaurar backups e reforçar medidas de segurança.
Problemas de Conexão com a Rede Interna	Conexão de rede interna apresenta falhas.	Identificar a área afetada, analisar a conexão do servidor central e verificar servidores DHCP e autenticação.
Problemas de Conexão com a Internet	Conexão com a internet apresenta falhas.	Identificar a área afetada, analisar a conexão, ativar link de contingência e abrir chamado com a operadora.
Problemas com Computadores Administrativos	Computadores administrativos com problemas de funcionamento.	Informar o setor de TI, agendar atendimento, fornecer computador provisório se necessário.

CAPÍTULO V
DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação na Faculdade Católica de Rondônia (FCR) é tratada com extrema seriedade e implementada através de um conjunto abrangente de medidas técnicas e

administrativas. O controle de acesso é uma das principais estratégias, garantindo que apenas usuários autorizados possam acessar informações sensíveis, utilizando autenticação multifator e permissões baseadas em função. Além disso, a criptografia de dados é empregada tanto para dados em trânsito quanto para dados em repouso, assegurando que informações sensíveis sejam protegidas contra acessos não autorizados.

O monitoramento contínuo dos sistemas e redes é realizado para detectar e responder rapidamente a atividades suspeitas ou tentativas de intrusão, utilizando ferramentas de detecção e prevenção de intrusões. A FCR realiza revisões periódicas de segurança para identificar possíveis vulnerabilidades e verificar a conformidade com as políticas de segurança, ajustando e aprimorando continuamente as práticas de segurança conforme necessário. Políticas rigorosas de backup são implementadas para garantir que os dados possam ser recuperados rapidamente em caso de perda ou corrupção, com backups regulares sendo armazenados em locais seguros.

Dentro dessa questão, utilizamos os serviços da PrimusWeb, onde são armazenadas as aplicações do GVcentris e do Pergamum. A PrimusWeb oferece suporte 24x7 e garante a alta disponibilidade dos serviços de hospedagem, com backup integral dos servidores e replicação de dados para recuperação de desastres. Esse suporte garante que as aplicações críticas da FCR estejam sempre protegidas e disponíveis.

O GVcentris, fornecido pela Gvdasa, é o sistema educacional da FCR, totalmente adequado às normas da Lei Geral de Proteção de Dados (LGPD). Esse sistema centraliza e protege as informações educacionais dos alunos, assegurando conformidade legal e segurança das informações.

Outro componente importante da segurança de informação é o firewall Fortigate 60F, que oferece inúmeras vantagens, incluindo inspeção de tráfego em alta velocidade, prevenção contra intrusões, filtragem de conteúdo e controle de aplicações. O Fortigate 60F também proporciona proteção avançada contra ameaças, como malwares e ataques de rede, além de permitir a criação de políticas de segurança personalizadas para diferentes segmentos da rede. Com essa robusta solução de firewall, a FCR assegura um ambiente de rede seguro e resiliente, protegendo os dados e garantindo a disponibilidade contínua dos serviços de TI.

A FCR também promove programas de treinamento e conscientização para todos os usuários, enfatizando a importância da segurança da informação e as melhores práticas para proteger os dados. Medidas de segurança física incluem o controle de acesso a áreas onde equipamentos críticos são armazenados, bem como a utilização de sistemas de alarme para prevenir acessos não autorizados.

Em caso de incidentes de segurança, a FCR tem um plano de resposta bem definido, com procedimentos claros para identificação, contenção, erradicação e recuperação, conforme disposto no Capítulo III (Dos Níveis de Incidentes) e no Capítulo IV (Dos Principais Riscos e Estratégias de Controle). A equipe de TI é treinada para agir rapidamente, minimizando os impactos de qualquer incidente. Com essas estratégias, a FCR assegura um ambiente de TI seguro e resiliente, protegendo dados e garantindo a continuidade dos serviços acadêmicos e administrativos, aderindo às melhores práticas de segurança da informação para proteger a instituição contra diversas ameaças.

CAPÍTULO VI
DA COMUNICAÇÃO

Uma comunicação eficaz é fundamental durante situações de contingência e segurança da informação para garantir uma resposta coordenada e eficiente. Todos os colaboradores, incluindo docentes, discentes e técnico-administrativos, são responsáveis por comunicar imediatamente qualquer problema detectado nos sistemas, equipamentos e/ou infraestrutura de TI. É crucial que qualquer anomalia, por menor que seja, seja reportada rapidamente para evitar maiores danos e garantir a continuidade dos serviços.

Toda comunicação relacionada a problemas de TI deve ser direcionada ao setor de Tecnologia da Informação (TI) da FCR, que fica localizado no segundo pavimento, lado sul, primeira porta à esquerda. A equipe de TI é a responsável por gerenciar e solucionar os incidentes reportados, garantindo que as medidas necessárias sejam tomadas o mais rápido possível.

A comunicação de problemas deve ser feita através de comunicação a algum membro da equipe de TI de forma presencial, por requerimento no sistema ou diretamente por e-mail para o setor de TI (ti@fcr.edu.br). A equipe de TI é responsável por receber, organizar e priorizar os chamados, além de manter o solicitante informado sobre o andamento e a resolução do problema. É essencial que todos os envolvidos sigam esses procedimentos para assegurar uma resposta rápida e coordenada, minimizando os impactos das falhas e garantindo a continuidade das operações na FCR. Essas práticas são igualmente importantes para manter a segurança da informação, protegendo dados sensíveis contra acessos não autorizados e outras ameaças.

CAPÍTULO VII
DA ATUALIZAÇÃO DO PLANO

Para garantir a eficácia contínua do Plano de Contingência e de Segurança da Informação da Faculdade Católica de Rondônia (FCR), é essencial que ele seja revisado e atualizado regularmente. A revisão ocorre no início do ano ou sempre que houver mudanças significativas na infraestrutura de TI, nos procedimentos operacionais ou nas regulamentações aplicáveis.

A equipe de Tecnologia da Informação é responsável por conduzir essas revisões, identificando áreas que precisam de melhorias e incorporando novas práticas e tecnologias de segurança. Feedback dos usuários e resultados de relatórios de segurança também devem ser considerados para garantir que o plano esteja sempre alinhado com as melhores práticas e as necessidades da instituição.

Cada atualização do plano deve ser documentada detalhadamente, incluindo as alterações feitas, as razões para essas mudanças e os benefícios esperados. É crucial que todas as partes interessadas, incluindo docentes, discentes e técnico-administrativos, sejam informadas sobre as atualizações do plano e instruídas sobre qualquer novo procedimento ou protocolo.

Além disso, simulações e treinamentos devem ser realizados periodicamente para assegurar que todos os colaboradores estejam preparados para seguir o plano de contingência

atualizado de maneira eficaz. Essas atividades ajudam a identificar quaisquer lacunas no plano e oferecem oportunidades para melhorias contínuas. Garantindo revisões regulares e atualizações do plano, a FCR se compromete a manter um ambiente de TI seguro e resiliente, capaz de responder rapidamente a incidentes e proteger a integridade, confidencialidade e disponibilidade das informações da instituição.

Porto Velho, em 20 de dezembro de 2023

Diretor Administrativo

Regulamento do uso da rede Wi-Fi

2023

| Direção Administrativa

FACULDADE CATÓLICA DE RONDÔNIA

Regulamento do uso da rede Wi-Fi

1. Finalidades e Objetivos

1.1 Este regulamento tem como objetivo estabelecer diretrizes claras e abrangentes para garantir a utilização segura, eficiente e ética dos recursos de rede sem fio da Faculdade Católica de Rondônia. Além disso, essa regulamentação visa administrar o acesso à rede wi-fi, definindo critérios para os acessos, a segurança das senhas, a permissão de dispositivos e o monitoramento da atividade na rede. Ao estabelecer essas diretrizes, visamos criar uma cultura de responsabilidade e conscientização entre os usuários, promovendo a conformidade com as normas estabelecidas, e assim garantindo a continuidade e qualidade do serviço de disponibilização do acesso à internet visando o benefício coletivo da organização.

2. Direito de uso

2.1 É direito do usuário o uso dos recursos da rede wi-fi disponíveis, com a finalidade acadêmica e atividades administrativas, como por exemplo, para pesquisa e acesso aos software institucionais, assim garantindo um ambiente de produção e o uso e compartilhamento de conhecimento. O mesmo é válido para os seguintes níveis de usuários:

- Alunos devidamente matriculados na instituição;
- Professores e/ou demais funcionários ativos na instituição;
- Visitantes autorizados pela instituição.

3. Campo de aplicação

3.1 As normas de acesso à rede wi-fi englobam todos os usuários que buscam utilizar os recursos da rede sem fio fornecidos. Aplica-se a todos os dispositivos, como laptops, smartphones, tablets e quaisquer outros aparelhos que necessitem de conectividade à rede wi-fi, garantindo uma experiência segura e em conformidade com o exercício da instituição.

3.2 A rede wi-fi está disponível em todos os ambientes do campus da Faculdade Católica de Rondônia - FCR, situada na Av. Governador Jorge Teixeira, 4100.

4. Acesso

4.1 A autenticação - para fazer o acesso todos os usuários devem ser autenticados utilizando o login e senha do e-mail institucional.

4.3 Monitoramento - A organização responsável pela rede wireless reserva-se o direito de monitorar o tráfego de rede e tomar as medidas necessárias para garantir a segurança e o cumprimento desta regulamentação.

4.3 A disponibilidade do serviço - O serviço de internet está disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana nas dependências da FCR. Entretanto, poderá sofrer quedas de desempenho ou interrupções devido às seguintes circunstâncias externas:

- Manutenções técnicas e/ou operacionais que exijam o desligamento ou reinicialização temporária do sistema;

- Eventos imprevisíveis, inesperados, forças maiores;
- Em casos de defeitos, falhas ou panes nos equipamentos , onde os mesmos serão trocados conforme o prazo estipulado no plano de contingência;
- Ocorrências de falhas simultâneas nos 3 (três) links de acesso à internet;
- Em função de condições técnicas e/ou ambientais que podem interferir com o sinal emitido pelos roteadores, não há garantia na manutenção dos mesmos em condições adversas e os usuários devem ficar cientes da possibilidade de perda de comunicação ou de informações.

5. Normas de uso da rede sem fio

5.1 Ao fazer o acesso a rede sem fio da FCR o usuário está aderindo e concordando com a regulamentação e a política de uso da instituição.

5.2 Os usuários são responsáveis por utilizar a rede sem fio de maneira consciente, respeitando os direitos dos demais usuários e aderindo a todas as leis e regulamentos vigentes.

5.3 Responsabilidade dos usuários:

- O login e a senha de acesso são de total responsabilidade do usuário, ficando vedado o compartilhamento de informações sobre a utilização da rede a pessoas não cadastradas;
- As configurações e atualizações de softwares ou hardwares ou quaisquer aparelhos que façam uso da rede sem fio é de inteira responsabilidade do usuário. Sendo aconselhável que os mesmos mantenham os seus antivírus sempre atualizados, uma vez que em nenhum caso a FCR se responsabilizará por qualquer dano e/ou prejuízo que o usuário possa sofrer ao utilizar a rede wi-fi.

5.4 São atos proibidos ao usuários:

- Criar falsa identidade ou assumir, com ou sem autorização, a identidade de outro usuário. Uma vez que as informações de login são pessoais e intransferíveis;
- Ligação de aparelhos a fim de redistribuir o acesso à rede wi-fi;
- Download de músicas, jogos, filmes, programas sem finalidade acadêmica;
- Utilizar o serviço para fins ilícitos e/ou proibidos;
- Utilizar a internet e e-mail institucional para participar de atividades de pesquisa de mercado, pirâmides, correntes, spam ou mensagens não solicitadas com fins comerciais ou políticos;
- Acessar sites pornográficos, games online, bate papo, sites de relacionamento, vídeos ou quaisquer outros sites que seu conteúdo não seja informativo ou educacional;
- Transmitir e/ou divulgar qualquer material que viole direitos de terceiros, incluindo direitos de propriedade intelectual;
- Obter ou tentar obter acesso não autorizado a outros sistemas ou rede de computadores conectados ao serviço;
- Utilizar de quaisquer meios para burlar sites com acesso não autorizado;
- Utilizar os recursos computacionais da FCR para ganho indevido;
- Manipular, alterar, deturpar ou suprimir os dados identificadores dos direitos autorais da FCR e de seus funcionários, assim como as marcas digitais, logotipos,

banners, símbolos, assinaturas digitais, ou os dispositivos de funcionalidade e proteção dos sites mantidos pela instituição;

- Consumir inutilmente os recursos computacionais da FCR de forma intencional.

6. Penalidades

6.1 O usuário é responsável por qualquer atividade relacionada ao seu login e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação judicial ou administrativa apresentada à instituição e que o envolva.

6.2 Caso alguma violação de regra seja identificada o usuário sofrerá com as seguintes penalidades de acordo com o nível de gravidade e tipo de usuário, por exemplo:

- Alunos: Advertência verbal ou suspensão do acesso, a depender da gravidade da situação, podendo ter o suspensão do acesso por prazo de no mínimo 15 dias até um suspensão permanente;
- Funcionários : Advertência verbal, Advertência Formal ou suspensão de uso da rede wifi;
- Terceiros: Advertência verbal até a suspensão do acesso.

7. Disposições Finais

7.1 Caso o usuário perceba o uso indevido de sua senha de acesso por terceiros, ou não consiga fazer o acesso, bem como quaisquer outros problemas com a rede sem fio, deverá fazer contato com o setor de TI via e-mail institucional (ti@fcr.edu.br) ou pelo formulário de suporte: https://forms.gle/zpv1Ra1EFjaRrnai7.

7.1 O login de acesso à rede sem fio só terá validade enquanto o vínculo do usuário com a instituição perdurar;

7.2 Só é permitido o acesso simultâneo em 1 aparelho por usuário;

7.3 O usuário compromete-se a fazer uso do seu acesso de forma segura e confidencial, zelando por sua confidencialidade, declarando-se ciente de que não poderá, a qualquer título, vender, transferir, ceder ou emprestar a terceiros;

7.4 A FCR reserva-se o direito de, a qualquer tempo, suspender, alterar ou cancelar as configurações de acesso da rede sem fio, sem necessidade de aviso prévio, caso ocorra qualquer situação que impeça e/ou prejudique a execução desse serviço;

7.5 Este regulamento está sujeito às alterações sem aviso prévio. Sendo necessário, as alterações serão comunicadas aos setores competentes e aos demais interessados.

Porto Velho, 20 de dezembro de 2023.

Direção Administrativa