

Cartilha Digital de Segurança e Privacidade de Dados

Normas e orientações para a comunidade do IFRO, baseadas na **LGPD** e no **ECA Digital**, construídas colaborativamente pelas turmas de Sistemas para Internet, Segurança da Informação, SO para Redes Livre I e Redes de Computadores.

[Consultar Normas](#)

Sobre esta Cartilha

Esta cartilha digital é o produto do projeto de extensão "**Cidadania Digital e Proteção Integral: Implementação de Redes Seguras e Promoção do ECA Digital**", desenvolvido pelo **IFRO — Campus Porto Velho Zona Norte**.

O conteúdo foi elaborado de forma colaborativa por alunos dos cursos de **Tecnologia em Sistemas para Internet** e **Tecnologia em Redes de Computadores**, integrando conteúdos de Segurança da Informação, Legislação em TI, Segurança de Redes e SO para Redes Livre I.

O objetivo é conscientizar a comunidade escolar — estudantes, responsáveis e servidores — sobre boas práticas de segurança digital, proteção de dados pessoais, ECA Digital e uso de redes seguras no ambiente institucional, em conformidade com a legislação brasileira vigente.



LGPD

Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais. Regula o tratamento de dados pessoais no Brasil.



ECA Digital

Lei nº 15.211/2025 — Proteção de crianças e adolescentes no ambiente digital. Em vigor desde março de 2026.

Para quem é esta cartilha?

As normas se aplicam a toda a comunidade do IFRO. Selecione seu perfil para identificar as orientações mais relevantes.



Estudantes

Orientações sobre uso seguro de laboratórios, rede Wi-Fi, proteção de dados pessoais e conduta em grupos digitais.



Pais e Responsáveis

Informações sobre consentimento para uso de imagem, proteção de menores e canais de denúncia contra cyberbullying.



Servidores

Responsabilidades no tratamento de dados, uso de plataformas homologadas e gestão segura de informações acadêmicas.

Normas de Segurança e Privacidade — LGPD

Normas internas do IFRO baseadas nos princípios da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), aplicadas ao cotidiano da instituição.



Controle de Acesso e Autenticação

Política de Senhas Fortes

Todos os usuários dos sistemas institucionais (SUAP, e-mail institucional, laboratórios) deverão utilizar senhas fortes, contendo letras maiúsculas, minúsculas, números e caracteres especiais. É terminantemente proibido o compartilhamento de credenciais de acesso.

Na prática: Ao acessar o SUAP ou o e-mail institucional, alunos e servidores devem criar senhas complexas e nunca compartilhá-las com colegas, mesmo que para "facilitar" o acesso a trabalhos em grupo.

Obrigatório

Autenticação em Dois Fatores (2FA)

Sempre que disponível, a autenticação em dois fatores deverá ser habilitada nos sistemas acadêmicos e institucionais, adicionando uma camada extra de proteção contra acessos indevidos.

Na prática: Ao fazer login no SUAP, além da senha, o sistema enviará um código de confirmação para o celular ou e-mail pessoal do usuário, impedindo que terceiros acessem a conta mesmo que descubram a senha.

Recomendado

Login Individual na Rede Wi-Fi

O acesso à rede Wi-Fi institucional deverá ser realizado exclusivamente por meio de credenciais individuais vinculadas ao SUAP, eliminando redes abertas e garantindo a identificação de cada usuário conectado.

Na prática: Ao se conectar à rede "IFRO-Alunos", o estudante deverá inserir seu usuário e senha do SUAP. Redes abertas sem autenticação não serão mais disponibilizadas.

Obrigatório



Segregação de Rede para Dispositivos Pessoais (BYOD)

Os dispositivos pessoais de alunos (notebooks, smartphones) devem ser conectados a uma rede Wi-Fi logicamente separada da rede administrativa, por meio de regras de firewall e VLANs. Isso impede que aparelhos pessoais tenham acesso aos servidores e bancos de dados institucionais.

Na prática: Ao usar o smartphone pessoal na biblioteca, o aluno será conectado à rede "IFRO-Alunos", que não possui rota de acesso aos servidores administrativos, protegendo os registros acadêmicos de toda a comunidade.

Obrigatório

Filtragem de Conteúdo e Regras de Firewall

A rede escolar deverá possuir sistema de filtragem de conteúdo capaz de bloquear o acesso a sites com conteúdo pornográfico, violento, discriminatório, de apostas ou outros inadequados ao público infantojuvenil, conforme exigido pelo ECA Digital.

Na prática: Um aluno de 14 anos que tente acessar sites de apostas online pelo Wi-Fi do campus terá o acesso automaticamente bloqueado. A filtragem será atualizada periodicamente.

Obrigatório

Criptografia e Segurança da Rede Sem Fio

Todas as redes sem fio do campus devem utilizar criptografia WPA2 ou superior, com senhas de rede complexas e rotacionadas periodicamente. O compartilhamento de credenciais de acesso é proibido.

Na prática: Cada aluno possui login individual — emprestar as credenciais para visitantes ou terceiros constitui violação das normas e poderá resultar em suspensão temporária do acesso.

Obrigatório



Bloqueio Automático por Inatividade

Os computadores dos laboratórios e setores administrativos devem ser bloqueados automaticamente após 5 minutos de inatividade, evitando que terceiros acessem dados pessoais ou acadêmicos caso o usuário se afaste do equipamento.

Na prática: Se um aluno de 16 anos deixa o computador e vai ao banheiro sem encerrar a sessão, o sistema bloqueará automaticamente a tela, exigindo nova autenticação para continuar.

Obrigatório

Limpeza de Dados a Cada Reinicialização

Ao reiniciar, todos os dados pessoais do usuário anterior — histórico de navegação, downloads, arquivos temporários, cookies e senhas salvas — devem ser automaticamente eliminados pelo sistema.

Na prática: Quando o próximo aluno ligar o computador, não encontrará nenhum vestígio da sessão anterior: nenhum arquivo, nenhuma senha, nenhum histórico do Chrome.

Obrigatório

Restrição de Gravação Local

Os computadores de uso coletivo devem possuir restrições de privilégio via Active Directory, impedindo que usuários salvem arquivos fora de suas pastas de perfil pessoal. Arquivos pessoais devem ser armazenados na nuvem institucional ou em dispositivos próprios.

Na prática: Se um aluno tentar salvar um documento na raiz do Disco C (onde qualquer pessoa teria acesso), o sistema bloqueará a ação e orientará o uso da pasta de perfil segura.

Obrigatório

Encerramento Obrigatório de Sessão

Ao finalizar o uso dos equipamentos, todos os usuários devem realizar o logoff completo do sistema e de todas as contas acessadas (e-mail, SUAP, redes sociais), garantindo que nenhum dado pessoal permaneça acessível.

Na prática: Antes de deixar o laboratório, o aluno deve clicar em "Sair" de todas as contas e realizar o logoff do Windows, protegendo seus dados pessoais e acadêmicos.

Obrigatório



Comunicação Digital e Grupos Institucionais



Uso Restrito a Assuntos Pedagógicos

 Confidencialidade

Os grupos de comunicação institucional (WhatsApp, Teams, Telegram, fóruns do AVA) devem ser utilizados exclusivamente para assuntos acadêmicos e administrativos. Conteúdos recreativos, correntes e mensagens fora do escopo pedagógico devem ser evitados.

Na prática: No grupo de WhatsApp da turma, o representante deve compartilhar apenas avisos acadêmicos, horários de provas e materiais de estudo — nunca dados pessoais de colegas.

Obrigatório

Proibição de Divulgar Dados Pessoais

É proibido compartilhar notas, documentos escolares, fotos, números de telefone ou qualquer informação pessoal de alunos e servidores em grupos de comunicação sem autorização prévia e específica dos envolvidos (ou de seus responsáveis, no caso de menores).

Na prática: Um professor não pode enviar a lista de notas da turma no grupo de WhatsApp. As notas devem ser comunicadas individualmente pelo SUAP ou sistema acadêmico oficial.

Obrigatório

Regras de Conduta e Moderação

Todos os ambientes virtuais de comunicação institucional devem possuir regras de conduta claras, proibindo intimidação, piadas ofensivas, exposição de imagens não autorizadas e qualquer forma de assédio ou discriminação.

Na prática: Se um aluno publicar memes ofensivos ou comentários discriminatórios no grupo da turma, o moderador (representante de turma ou professor) deve advertir e, se necessário, encaminhar o caso à coordenação.

Obrigatório



Uso de Imagem e Consentimento



Termo de Consentimento Obrigatório

 Confidencialidade

Ao inscrever projetos em feiras, eventos ou atividades do campus, o sistema de inscrição deverá exigir o aceite digital explícito do aluno — ou de seu responsável legal, no caso de menores — autorizando a publicação de fotos e dados do participante.

Na prática: Antes de publicar fotos da feira de tecnologia no Instagram do campus, a equipe de comunicação deve verificar se todos os participantes (ou seus responsáveis) assinaram o termo de consentimento digital.

Obrigatório

Proteção Especial para Menores de Idade

A divulgação de fotos, vídeos ou informações pessoais de estudantes menores de 18 anos requer autorização por escrito do responsável legal, conforme exigido pela LGPD e pelo ECA Digital. Sem essa autorização, a instituição fica proibida de publicar imagens que identifiquem o menor.

Na prática: Se um aluno de 15 anos não possui autorização dos pais, seu rosto deve ser ocultado ou a foto não deve ser publicada, mesmo que o evento seja institucional.

Obrigatório

Restrição de Compartilhamento em Redes Sociais

Fotos, vídeos e informações de alunos e servidores só podem ser publicados em redes sociais institucionais ou pessoais após verificação das autorizações necessárias, respeitando a privacidade de todos os envolvidos.

Na prática: Um professor que fotografa uma atividade em laboratório não pode postar no seu Instagram pessoal sem a autorização de todos os alunos retratados na imagem.

Obrigatório



Canais de Denúncia e Combate ao Cyberbullying

Integridade



Canal Anônimo e Sigiloso de Denúncias

O IFRO deve disponibilizar um canal oficial e sigiloso, integrado ao SUAP, para que qualquer membro da comunidade escolar possa denunciar anonimamente situações de cyberbullying, vazamento de fotos, perfis falsos difamatórios ou outras formas de violência digital.

Na prática: Um aluno que está sendo vítima de intimidação em um grupo de WhatsApp pode anexar prints de forma anônima pelo SUAP. A equipe multidisciplinar (psicólogos, assistentes sociais, coordenação) é acionada para intervir.

Recomendado

Protocolo "Porto Seguro" para Violência Virtual

Mesmo que a violência digital ocorra fora da rede do IFRO (em redes sociais externas como Instagram ou WhatsApp), a instituição tem o dever de acolher a vítima e intervir pedagogicamente, conforme o princípio de proteção integral do ECA.

Na prática: Se um aluno menor de idade é vítima de perfis falsos difamatórios no Instagram criados por colegas, o IFRO não pode ignorar sob a justificativa de que "aconteceu fora da rede da escola". A equipe deve acolher e agir.

Recomendado

Comunicação com Pais e Responsáveis

Em caso de incidentes envolvendo menores de idade, os pais ou responsáveis legais devem ser notificados imediatamente, de forma pedagógica, convidando a família para uma conversa sobre o uso saudável das tecnologias.

Na prática: Se um estudante se envolve em uso inadequado da rede, o SUAP envia uma notificação automatizada aos pais, não como punição, mas como convite para diálogo sobre cidadania digital.

Obrigatório



Educação e Conscientização Digital



Programa Anual de Capacitação

Integridade

O IFRO deve implementar um programa anual de capacitação em segurança digital e proteção de dados, destinado a professores, servidores, alunos e responsáveis legais, abordando princípios da LGPD, uso seguro da internet, prevenção ao cyberbullying e boas práticas de segurança.

Na prática: No início de cada semestre, a equipe de TI e a coordenação realizam palestras sobre segurança digital para todas as turmas, incluindo demonstrações práticas de como identificar golpes de phishing.

Recomendado

Cyber-Mentoria: Graduação para o Técnico

Os alunos dos cursos superiores de tecnologia (TSI e Redes) podem atuar como "Mentores de Segurança Digital" para as turmas do ensino técnico integrado, realizando oficinas práticas sobre proteção de contas, engenharia social e privacidade nas redes sociais.

Na prática: Alunos do 5º período de Redes ensinam estudantes do 1º ano do técnico integrado a configurar a verificação em duas etapas no Instagram e a reconhecer tentativas de golpe por WhatsApp.

Recomendado

Notificação Obrigatória de Incidentes

Qualquer suspeita de vazamento de dados, acesso indevido ou golpe digital deve ser comunicada imediatamente ao setor de TI da instituição, que adotará medidas preventivas e corretivas conforme a LGPD.

Na prática: Se um aluno receber uma mensagem de e-mail falsa solicitando sua senha do SUAP (phishing), deve informar imediatamente a equipe de TI para que o domínio seja bloqueado e os demais usuários sejam alertados.

Obrigatório



Plataformas e Ferramentas Digitais



Proibição de Plataformas Não Homologadas



Os professores ficam proibidos de exigir que alunos criem cadastros em aplicativos e sites de terceiros que não possuam acordo de proteção de dados firmado com a instituição. Toda a vida acadêmica deve ser concentrada nos sistemas oficiais do IFRO (SUAP, AVA/Moodle, e-mail institucional).

Na prática: Um professor não pode exigir que alunos criem conta em um site externo para entregar trabalhos. As entregas devem ser realizadas pelo Moodle ou SUAP, protegendo os dados dos estudantes.

Obrigatório

Uso Acadêmico dos Recursos Computacionais

O acesso a jogos eletrônicos, redes sociais recreativas e plataformas de streaming nos computadores dos laboratórios e na rede Wi-Fi institucional é restrito, sendo liberado apenas quando vinculado a atividades pedagógicas supervisionadas.

Na prática: Se um estudante tentar acessar um jogo online ou o TikTok durante o horário de aula, o firewall bloqueará o acesso e exibirá uma mensagem orientando o foco nas atividades acadêmicas.

Obrigatório

Proteção de Crianças e Adolescentes — ECA Digital

Destaques da Lei nº 15.211/2025 (ECA Digital), em vigor desde março de 2026, aplicados ao contexto do IFRO para a proteção integral de estudantes menores de 18 anos no ambiente digital.



Verificação de Idade

Plataformas e serviços digitais devem implementar mecanismos confiáveis de verificação de idade, impedindo que menores acessem conteúdos impróprios. A simples autodeclaração não é mais suficiente.



Supervisão Parental

Menores de 16 anos devem ter contas conectadas a um responsável legal, com ferramentas para gerenciar tempo de uso, limitar conteúdos e controlar gastos em plataformas digitais.



Privacidade por Padrão

Produtos digitais devem vir com as configurações mais protetivas possíveis ativadas por padrão para usuários jovens, garantindo privacidade e segurança desde o primeiro acesso.



Proibição de Perfilamento

É proibida a publicidade direcionada baseada em perfilamento comportamental de crianças e adolescentes. Plataformas não podem monetizar dados comportamentais de menores.



Proibição de Loot Boxes

A lei proíbe expressamente caixas de recompensa aleatória (loot boxes) em jogos voltados ao público infantojuvenil, protegendo menores de práticas predatórias de monetização.



Responsabilidade das Plataformas

Empresas são corresponsáveis pela segurança dos menores, devendo remover conteúdos prejudiciais (bullying, exploração, automutilação) de forma ágil e reportar crimes às autoridades.

Principais Ameaças Digitais

Conheça as ameaças mais comuns enfrentadas por estudantes e servidores no ambiente digital e saiba como se proteger.



Phishing

E-mails, mensagens ou sites falsos que imitam fontes confiáveis para roubar senhas e dados pessoais.

IMPACTO:

Roubo de credenciais do SUAP, e-mail e contas pessoais.

PREVENÇÃO:

Verifique sempre o remetente, não clique em links suspeitos e nunca forneça senhas por e-mail.



Engenharia Social

Manipulação psicológica para convencer pessoas a revelar informações confidenciais ou realizar ações indevidas.

IMPACTO:

Acesso indevido a sistemas, vazamento de dados acadêmicos.

PREVENÇÃO:

Desconfie de pedidos urgentes, confirme solicitações por outro canal e nunca compartilhe credenciais.



Malware

Softwares maliciosos (vírus, ransomware, spyware) que infectam dispositivos via downloads, pendrives ou sites comprometidos.

IMPACTO:

Computadores comprometidos, perda de arquivos, roubo de dados.

PREVENÇÃO:

Mantenha o antivírus atualizado, evite downloads de fontes não oficiais e não conecte pendrives desconhecidos.



Vazamento de Dados

Exposição não autorizada de informações pessoais, acadêmicas ou institucionais, seja por falha técnica ou descuido humano.

IMPACTO:

Violação de privacidade, danos à reputação, sanções legais pela LGPD.

PREVENÇÃO:

Não salve dados pessoais em PCs compartilhados, encerre sessões e use nuvem institucional.



Cyberbullying

Intimidação, humilhação ou assédio sistemático praticado por meio de plataformas digitais, redes sociais ou aplicativos de mensagem.

IMPACTO:

Danos psicológicos graves, evasão escolar, isolamento social.

PREVENÇÃO:

Denuncie pelo canal anônimo do IFRO, não retalie e procure ajuda da equipe multidisciplinar.



Exposição em Redes Sociais

Compartilhamento excessivo de informações pessoais (localização, rotina, dados escolares) em perfis públicos de redes sociais.

IMPACTO:

Exposição a predadores, roubo de identidade, perda de privacidade.

PREVENÇÃO:

Configure seus perfis como privados, não divulgue localização em tempo real e revise as permissões dos aplicativos.

Redes Seguras e Infraestrutura da Cartilha Digital

Esta seção integra os dados técnicos da cartilha de Redes de Computadores, mantendo o foco do projeto de extensão: proteção integral, segurança em redes escolares, hardening de sistemas livres e publicação da Cartilha Digital em ambiente web.



Segurança em redes escolares

As redes escolares concentram sistemas acadêmicos, dados pessoais, plataformas educacionais e recursos administrativos. Por isso, a proteção deve considerar confidencialidade, integridade e disponibilidade.



Servidor Debian 13

A infraestrutura proposta utiliza ambiente virtualizado com Debian Server, dimensionamento de memória, CPU e disco, além de organização de diretórios para hospedagem da Cartilha Digital.



Apache, SSH e SFTP

O servidor web Apache disponibiliza o site, enquanto o SSH e o SFTP apoiam administração remota, transferência segura de arquivos e manutenção controlada do conteúdo publicado.



Firewall e hardening

As práticas de hardening reduzem a exposição do sistema, reforçam permissões, restringem acessos e orientam a aplicação de regras de firewall para proteger a infraestrutura.



Monitoramento e validação

Os testes incluem verificação do Apache, análise de recursos, validação da estrutura de arquivos, monitoramento básico e confirmação do funcionamento do site estático.



ECA Digital e proteção integral

O projeto relaciona segurança técnica e responsabilidade social, difundindo orientações sobre proteção de crianças e adolescentes no ambiente digital.

Etapas técnicas incorporadas ao site

Instalação inicial do Debian Server em ambiente virtualizado.

Configuração inicial do servidor web da Cartilha Digital.

Estruturação de diretórios, serviços e permissões no Linux.

Publicação do site estático, validação de acesso e ajustes finais.

Aplicação de hardening, firewall, monitoramento e testes básicos de proteção.

Legislação de Referência

Conheça as leis brasileiras que fundamentam as normas desta cartilha.



LGPD — Lei Geral de Proteção de Dados

Lei nº 13.709, de 14 de agosto de 2018

Regula o tratamento de dados pessoais no Brasil, tanto no meio físico quanto digital, protegendo os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade. Estabelece princípios como finalidade, adequação, necessidade, transparência e segurança, além de garantir ao titular o direito de acesso, correção, eliminação e portabilidade de seus dados.

[Ler a lei na íntegra → →](#)



ECA Digital — Proteção Digital de Crianças e Adolescentes

Lei nº 15.211, de 15 de setembro de 2025

Estabelece novo marco regulatório para a proteção de crianças e adolescentes no ambiente virtual. Exige verificação de idade, supervisão parental, privacidade por padrão, proíbe perfilamento publicitário e loot boxes, e responsabiliza plataformas pela remoção ágil de conteúdos prejudiciais. Em vigor desde 17 de março de 2026.

[Ler a lei na íntegra → →](#)



ECA — Estatuto da Criança e do Adolescente

Lei nº 8.069, de 13 de julho de 1990

Lei fundamental que dispõe sobre a proteção integral da criança e do adolescente, assegurando direitos à vida, saúde, educação, dignidade e convivência familiar. A Lei 15.211/2025 (ECA Digital) complementa este estatuto com proteções específicas para o ambiente digital.

[Ler a lei na íntegra → →](#)



ANPD — Autoridade Nacional de Proteção de Dados

Órgão da administração pública federal

A ANPD é o órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil, bem como atuar na proteção de crianças e adolescentes em ambientes digitais, conforme diretrizes do ECA Digital.

[Acessar o portal oficial → →](#)

Relatórios e Arquivos do Projeto

Arquivos disponibilizados para consulta e download. Os documentos registram a cartilha de segurança em redes, o relatório técnico de infraestrutura e a versão em PDF da cartilha publicada no site.



Relatório Técnico: Infraestrutura e Hospedagem

Documenta a preparação do ambiente Debian, configuração do Apache, SSH/SFTP, permissões, testes, publicação e validação do servidor web.

[Baixar PDF](#)



Cartilha: Segurança em Redes e ECA Digital

Apresenta fundamentos de segurança da informação, redes escolares, ameaças, vulnerabilidades, análise de riscos e boas práticas de proteção.

[Baixar PDF](#)



Cartilha do Site em PDF

Versão em PDF do conteúdo publicado neste site, organizada para consulta offline, impressão e compartilhamento com a comunidade escolar.

[Baixar PDF](#)

Projeto de Extensão

Cidadania Digital e Proteção Integral: Implementação de Redes Seguras e Promoção do ECA Digital

Disciplinas integradas: Segurança da Informação, Legislação em TI, Segurança de Redes e SO para Redes Livre I

Equipes

Design e Implementação:

Turma de TSI — 5º Período

Normas, infraestrutura e relatórios:

Turmas de Redes de Computadores e TSI

Instituição

Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

Campus Porto Velho Zona Norte

portal.ifro.edu.br