Boletim de Serviço Eletrônico em 29/10/2019

INSTITUTO FEDERAL
Rondônia

MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

RESOLUÇÃO Nº 57/REIT - CONSUP/IFRO, DE 15 DE OUTUBRO DE 2019

Dispõe sobre a aprovação da Política de Segurança da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO).

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA, no uso de suas atribuições legais e em conformidade com o disposto no Estatuto, considerando o Processo nº 23243.024340/2018-14, considerando ainda a aprovação unânime do Conselho Superior durante a 27ª Reunião Ordinária, em 26/09/2019;

R E S O L V E:

Art. 1º APROVAR a Política de Segurança da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia, anexo a esta Resolução.

Art. 2º Esta Resolução entra em vigor nesta data.

UBERLANDO TIBURTINO LEITE
Presidente do Conselho Superior
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia.

Documento assinado eletronicamente por **Uberlando Tiburtino Leite**, **Reitor**, em 15/10/2019, às 15:05, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0720347** e o código CRC **62883B3B**.

ANEXO I DA RESOLUÇÃO Nº 57/CONSUP/IFRO/2019

POSIC - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA

CAPÍTULO I

APRESENTAÇÃO

Art. 1º O Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), autarquia federal vinculada ao Ministério da Educação (MEC), instituída por meio da Lei nº 11.892, Artigo 5.º, Inciso XXXII, de 29 de dezembro de 2008, sendo detentor de autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar, equiparado às universidades federais. É uma instituição de educação superior, básica e profissional, pluricurricular e multicampi, especializada na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino para os diversos setores da economia, na realização de pesquisas e no desenvolvimento de novos produtos e serviços, em estreita articulação com os setores produtivos e com a sociedade, dispondo de mecanismos para a educação continuada.

§ 1º Tem como missão promover educação profissional, científica e tecnológica de excelência, por meio da integração entre ensino, pesquisa e extensão, com foco na formação de cidadãos comprometidos com o desenvolvimento humano, econômico, cultural, social e ambiental sustentável.

§ 2º Apresenta a visão de "Consolidar a atuação institucional, sendo reconhecido pela sociedade como agente de transformação social, econômica, cultural e ambiental de excelência".

§ 3º. Baseia-se nos valores da “Ética, transparência, comprometimento, equidade, democracia, respeito e efetividade".

CAPÍTULO II

DA FINALIDADE

Art. 2º A Política de Segurança da Informação e Comunicação do Instituto Federal de Rondônia é uma declaração formal acerca do seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os envolvidos internamente e externamente ao IFRO, que podem ser:

I - Servidores

II - Alunos

III - Colaboradores

IV - Estagiários

V -Prestadores de serviço que exerçam atividades no âmbito da Instituição ou;

VI - Qualquer cidadão que tenha acesso a dados ou informações no âmbito do Instituto.

§ 1º. O seu propósito é estabelecer diretrizes gerais que servirão como base para as normas, procedimentos e instruções referentes à segurança da informação, atribuindo responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes a Instituição.

§ 2º. Tem como finalidade também:

I - Orientar quanto a adoção de controles e processos para atendimento dos requisitos de Segurança da Informação;

II - Resguardar as informações do IFRO, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade.

Art 3º. Para esta política, o grupo de trabalho responsável pela elaboração da Política de Segurança da Informação e Comunicação estabeleceu as **diretrizes gerais** necessárias para que o comitê gestor de segurança da informação e a equipe de segurança da informação possam desenvolver as ações de gestão da segurança da informação em todo o IFRO. **Normas complementares** deverão ser propostas para que as diretrizes gerais possam ser alcançadas e haja uma potencialização do nível de segurança da informação do IFRO.

§ 1º. Este documento apresenta de forma estruturada a política que o IFRO deve seguir no que tange a Segurança da Informação e Comunicação, fruto de um trabalho participativo entre o grupo de trabalho formado pelos representantes das áreas finalísticas e meio do IFRO.

§ 2º. O grupo de trabalho é formado pelos representantes de todas as Pró-reitorias, Diretorias Sistêmicas e representante dos professores e campus, conforme portaria nº. 517, desta forma alcançando todas as áreas da instituição.

Art 4º. O Decreto 9.637, de 26 de Dezembro de 2018, Institui a Política Nacional de Segurança da Informação, no âmbito da administração pública federal com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional. Diante disso, o Departamento de Segurança da Informação e Comunicações (DSIC) disciplina este tema, por meio da publicação de normas que são consideradas obrigatórias.

CAPÍTULO III

ALINHAMENTO ESTRATÉGICO

Art. 5º. O alinhamento estratégico da POSIC 2019-2021 do IFRO é realizado por meio do atendimento aos objetivos estratégicos “Assegurar estruturas e práticas de segurança da informação” e “Fortalecer o alinhamento entre o planejamento de Tecnologia da Informação, às estratégias do IFRO e a estratégia geral de Tecnologia da Informação” demonstrados no Plano de Desenvolvimento Institucional 2018-2022 do IFRO. Esse tema, também é abordado no Plano Estratégico de TI 2014-2019 do IFRO.

Art. 6º A Política também possui alinhamento com documentos norteadores que extrapolam o IFRO. Dessa forma, este documento possui também a finalidade de “Garantir a Segurança da Informação e Comunicações” da Estratégia Geral de Tecnologia da Informação (EGTI) do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação). Isto contribui para a realização das seguintes iniciativas estratégicas:

I - Promover o desenvolvimento de políticas de segurança da informação e comunicações.

II - Estimular a adoção de práticas de gestão de incidentes de segurança da informação e comunicações.

III - Implementar práticas de gerenciamento de riscos e continuidade de negócios.

CAPÍTULO IV

ABRANGÊNCIA

Art. 7º. A abrangência desta política alcança todos os servidores, prestadores de serviço, estagiários e alunos do IFRO, que deverão seguir as diretrizes da segurança da informação para o gerenciamento e administração segura dos seus ativos, abrangendo todos os usuários da informação, incluindo qualquer organização/instituição/empresa que possuem, possuíram ou virão a possuir acesso às informações do IFRO e/ou fizeram ou farão uso dos recursos computacionais compreendidos na infraestrutura do IFRO.

CAPÍTULO V

ESCOPO

Art. 8º. O escopo da Política de Segurança da Informação e Comunicação do IFRO refere-se:

I - Aos aspectos estratégicos, estruturais e institucionais, preparando a base para elaboração dos demais documentos publicados pelo comitê gestor de segurança da informação como normas complementares;

II - Aos requisitos de segurança humana, com respeito a segurança da informação;

III - Aos requisitos de segurança física, em ambientes de esquipamentos e instalações de processamento/armazenamento de informação;

IV - Aos requisitos de segurança lógica e virtual;

V - À sustentação dos procedimentos, dos processos de trabalho e dos ativos que influenciarão diretamente nos serviços oriundos da Informação e Comunicação do IFRO.

CAPÍTULO VI

VIGÊNCIA, VALIDADE E ATUALIZAÇÃO

Art. 9º. Esta Política passa a vigorar a partir da data de sua publicação e deverá ser atualizada a cada três anos.

§ 1º. O Comitê Gestor de Segurança da Informação, a fim de que a POSIC e/ou seus instrumentos normativos, não fiquem ultrapassados ou desatualizados, deve revê-la periodicamente ou quando se fizer necessário, sendo ainda obrigatória a revisão anual.

CAPÍTULO VII

PUBLICAÇÃO

Art. 10. A Política e as Normas de Segurança da Informação e Comunicação e suas atualizações devem ser divulgadas pelos canais de comunicação do IFRO a todos os servidores, usuários, prestadores de serviço, contratados e colaboradores que habitualmente integram o quadro funcional do IFRO dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Art. 11. Após aprovação, as normas e procedimentos serão divulgados aos interessados pela área responsável por sua proposição e manutenção.

CAPÍTULO VIII

CONCEITOS E DEFINIÇÕES

Art. 12. Para os efeitos desta política são estabelecidos os seguintes conceitos e definições:

I. **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;

II. **Ameaça**: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização;

III. **Análise de riscos:** uso sistemático de informações para identificar fontes e avaliar riscos;

IV. **Ataque**: Qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede;

V. **Atividade:** processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

VI. **Ativo**: qualquer bem, tangível ou intangível, que tenha valor para a Instituição. Neles incluem-se: Ativos de informação; Ativos de software; Ativos físicos; Serviços; Pessoas e suas qualificações, habilidades e experiências; Reputação e a imagem da instituição;

VII. **Ativos de Informação:** os meios de armazenamento, transmissão e processamento; os sistemas de informação; além das informações em si, bem como os locais em que se encontram esses meios e as pessoas que têm acesso a eles;

VIII. **Avaliação de riscos:** processo de comparar o risco estimado com critérios predefinidos para determinar a importância do risco;

IX. **Autenticidade:** princípio de segurança que atesta com exatidão a origem da informação e a responsabilidade pela criação ou divulgação da mesma;

X. **Celeridade:** às ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;

XI. **Ciclo de Vida da Informação:** Todo e qualquer momento vivido pela informação, até mesmo situações de riscos, é designado de ciclo de vida da informação;

XII. **Classificação da informação:** identificação dos níveis de proteção que as informações demandam; atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas;

XIII. **Comitê Gestor de Segurança da Informação e Comunicação:** responsável pelas ações de segurança da informação e comunicação no âmbito da Instituição;

XIV. **Comunicação do risco:** troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

XV. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado ou não credenciado;

XVI. **Contingência:** descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

XVII. **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XVII. **Cópia de Segurança (Backup):** copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

XIX. **Correio Eletrônico:** é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

XX. **Criptografia:** é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");

XXI. **Criticidade:** Grau de importância que um requisito, módulo ou erro possui no sistema;

XXII. **Custodiante** do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

XXIII. **Dados:** Conjunto de valores ou ocorrências em um estado bruto com o qual são obtidas informações com o objetivo de adquirir benefícios;

XXIV. **Desastre:** evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos em sua capacidade de prestar serviços essenciais ou críticos, por um período de tempo superior ao prazo de recuperação;

XXV. **Descarte:** eliminação correta de informações, documentos, mídias e acervos digitais;

XXVI. **Diretriz:** descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;

XXVII. **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade que possua a devida autorização de acesso;

XXVIII. **Equipe de Segurança da Informação e Comunicação:** Grupo de Trabalho responsável por assessorar a implementação das ações de segurança da informação e comunicação no âmbito da Instituição;

XXIX. **Equipe de Tratamento e Resposta de Incidentes:** equipe responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança;

XXX. **Ética:** preservação dos direitos dos agentes públicos, sem comprometimento da Segurança da Informação e Comunicações;

XXXI. **Falha**: Defeito ou uma condição anormal em um componente, equipamento, subsistema ou sistema, que pode impedir o seu funcionamento como planejado, uma situação chamada de fracasso;

XXXII. **Gestor da Informação:** pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

XXXIII. **Gestor de Segurança da Informação e das Comunicações:** é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF;

XXXIV. **Incidente de segurança da informação:** um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004];

XXXV. **Informação:** ativo principal a ser resguardado por esta política;

XXXVI. **Integridade**: a informação não deve ser alterada sem autorização da Instituição;

XXXVII. **Impacto:** mudança adversa no nível obtido dos objetivos de negócios;

XXXIII. **Não-Repúdio:** garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

XIL. **Risco:** a possibilidade de um ativo estar sujeito a vulnerabilidades e incidentes (ameaças explorando essas vulnerabilidades), comprometendo a continuidade das atividades de uma organização ;

XL. **Probabilidade:** estudo das chances de ocorrência de um resultado, que são obtidas pela razão entre casos favoráveis e casos possíveis;

XLI. **Política:** intenções e diretrizes globais formalmente expressas pela direção;

XLII. **Política de Segurança da Informação e Comunicação (POSIC):** documento aprovado pela autoridade responsável da Instituição, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

XLIII. **Rede** Corporativa: conjunto de todas as redes locais sob a gestão da instituição;

XLIV. **Sistemas de Informação:** modelo, automatizado ou manual, de processos responsáveis por coletar e transmitir dados que sejam úteis ao desenvolvimento de produtos ou serviços das empresas, organizações e de demais projetos;

XLV. **Software:** são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

XLVI. **Site:** Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

XLVII. **Tratamento da informação:** recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XLVIII. **Tratamento de Incidentes de Segurança em Redes Computacionais:** serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XLIX. **Trilhas de Auditoria:** são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (*logs*) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

L. **VPN (Virtual Private Network):** (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;

LI. **Vulnerabilidade:** Fragilidade de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças.

CAPÍTULO IX

DIRETRIZES GERAIS

Art. 13. É dever de todos zelar pela Segurança da Informação e Comunicações.

Art. 14. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do IFRO adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações.

Art. 15. Todos os envolvidos interna ou externamente ao IFRO devem observar as seguintes diretrizes gerais desta política.

I - **Acesso, Proteção e Guarda da Informação:** O acesso à informação deve ser regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Instituição é considerada seu patrimônio e deve ser protegida seja ela em meio físico ou meio digital;

II - **Acesso a Internet:** todos os servidores têm o direito de acesso à internet, com utilização exclusiva para fins diretos e complementares às atividades do setor, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham a contribuir para o desenvolvimento de seus trabalhos. O acesso à Internet pelo corpo discente da Instituição deverá observar estritamente os objetivos acadêmicos constantes dos programas de cursos;

III - **Auditoria, Conformidade e Monitoramento:** Deverão ser levantados regularmente os aspectos legais de segurança aos quais as atividades da Instituição estão submetidas, de forma a evitar responsabilizações decorrentes da não observância de tais aspectos por desconhecimento ou omissão;

IV - **Capacitação e Aperfeiçoamento:** Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação. O IFRO deverá prover continuamente a capacitação, reciclagem e o aperfeiçoamento de todos os usuários da instituição, por meio de programas de divulgação, sensibilização, conscientização e capacitação em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança dentro da instituição;

V - **Classificação e Tratamento das informações:** Toda informação criada, manuseada, armazenada, transportada ou descartada do IFRO deverá ser classificada de acordo com a Lei nº 12.527; Para que o nível adequado de proteção da informação seja estabelecido, é necessário que todas as informações, existentes e futuras, sejam devidamente classificadas; A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do IFRO. Essa proteção deve ser de acordo com o valor, sensibilidade e criticidade da informação, devendo ser desenvolvido, para este fim, sistema de classificação da informação. Os dados, as informações e os sistemas de informação do IFRO devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens;

VI - **Comunicação**: O acesso a internet confere à comunidade de usuários um mecanismo de comunicação; O uso de mecanismos de comunicação institucionais, via internet, é muito importante e deve ser alvo de regulamentação complementar;

VII - **Gestão de Informação:** Deverão ser estabelecidas normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação que serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que serão especificados pelo IFRO;

VIII - **Gestão de Ativos:** A entrada e saída de ativos de informação do IFRO deverá ser registrada e autorizada por autoridade competente mediante procedimento formal; Deverá ser provido registros e procedimentos específicos, tais como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas institucionais, à rede interna e à internet;

IX - **Gestão de Incidentes:** É estabelecida uma área que consiste em receber, filtrar, classificar e responder as solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências;

X - **Gestão de Riscos:** É estabelecido um processo de Gestão de Risco, contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação, produzindo subsídios para a Gestão de Continuidade dos Negócios. Os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco, como ameaça, vulnerabilidade, probabilidade e impacto;

XI - **Patrimônio Intelectual:** As informações, os sistemas e os métodos criados pelos servidores da Instituição, no exercício de suas funções, são patrimônios intelectuais da Instituição não cabendo a seus criadores qualquer forma de direito autoral;

XII - **Plano de Continuidade:** É estabelecido um processo de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da Instituição possam ser mantidas ou recuperadas após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações;

XIII - **Termo de Responsabilidade e Sigilo:** É o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a politica de segurança da Instituição, os quais deverão ser signatários;

XIV - **Segurança Física:** Controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da Instituição e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança;

XV - **Utilização dos Recursos de Informação:** Os recursos disponibilizados pelo IFRO são fornecidos com o propósito único de garantir o desempenho das atividades da Instituição. O uso dos recursos de tecnologia da informação e comunicações disponibilizados pela IFRO é passível de monitoramento e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade;

XVI - **Uso de e-mail:** o serviço de correio eletrônico disponibilizado pelo IFRO constitui recurso do Instituto disponibilizado na rede de comunicação de dados para aumentar a agilidade, segurança e economia da comunicação oficial e informal;

CAPÍTULO X

REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 16. Para elaboração desta política de segurança da informação e comunicação, considerou-se as seguintes referências legais e normativas:

- Constituição da República Federativa do Brasil de 1988;
- Lei nº 5.172, de 25 de outubro de 1966, que dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios.
- Lei nº 7.170, de 14 de dezembro de 1983, que dispõe sobre o os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências.
- Lei nº 7.232, de 29 de outubro de 1984, que dispõe sobre a Política Nacional de Informática, e dá outras providências.
- Lei nº 7.492, de 16 de junho de 1986, que dispõe sobre os crimes contra o sistema financeiro nacional, e dá outras providências.
- Lei nº 8.027 de 12 de abril de 1990, que dispõe sobre as normas de conduta a serem observadas pelos servidores públicos civis da União, das Autarquias e das Fundações Públicas;
- Lei nº 8.137, de 27 de dezembro de 1990, que dispõe sobre os crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências.
- Lei nº 8.112 de 11 de dezembro de 1990, que trata do regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
- Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;
- Lei nº 8.429, de 2 de junho de 1992, que dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional;
- Lei nº 9.279, de 14 de maio de 1996, que dispõe sobre o pedido de patente originário do Brasil cujo objeto interesse à defesa nacional será processado em caráter sigiloso.
- Lei nº 9.296, de 24 de julho de 1996, que dispõe sobre crime de interceptação de comunicações telefônicas, de informática ou telemática, ou quebra de segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
- Lei nº 9.605, de 12 de fevereiro de 1998, que dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências.
- Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto Lei no 2848/40 (Código Penal Brasileiro), de modo a prever a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
- Lei nº 11.892, DE 29 DE DEZEMBRO DE 2008, que Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências;

- Lei nº 12.737, de 30 de novembro de 2012, que dispões sobre a tipificação criminal de delitos informáticos;
- Lei n° 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Lei n° 13.709/2018 (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- LEI COMPLEMENTAR Nº 75, DE 20 DE MAIO DE 1993, que dispões sobre Competência do Ministério Público da União para requisitar informações, exames, perícias e documentos de autoridades da Administração Pública direta ou indireta e ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública, bem como a responsabilização pelo uso dessas informações.
- Decreto-Lei nº 2848, de 07 de dezembro de 1940, que dispõe sobre o Código Penal.
- Decreto-Lei nº 3.689, de 3 de outubro de 1941, que dispõe sobre o Código de Processo Penal.
- Decreto-Lei nº 5.452, de 01 de maio de 1943, que dispõe sobre a Consolidação das Leis do Trabalho.
- Decreto nº 1.048, de 21 de janeiro de 1994, que trata do Sistema de Administração dos Recursos de Informação e Informática da Administração Pública Federal;
- Decreto 1.171 de 24 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;
- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal;
- Decreto nº 6.029, de 1º de fevereiro de 2007, que trata do Sistema de Gestão da Ética do Poder Executivo Federal;
- Decreto nº 7.845 de 14 de novembro de 2012, Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- Decreto nº 9.637, de 26 de Dezembro de 2018, que Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.
- Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação/MPOG, de 11 de setembro de 2014;
- Instrução Normativa GSI/PR nº 01 de 13 de junho de 2008;
    - Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 14 de outubro de 2008;
    - Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 3 de julho de 2009;
    - Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
    - Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
    - Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
    - Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
    - Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010;
    - Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
    - Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
    - Norma Complementar nº 11/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
    - Norma Complementar nº 12/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
    - Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;

- Norma Complementar nº 14/IN01/DSIC/GSI/PR, de 10 de fevereiro de 2012;
- Norma Complementar nº 15/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 16/IN01/DSIC/GSI/PR, de 21 de novembro de 2012;
- Norma Complementar nº 17/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 18/IN01/DSIC/GSI/PR, de 10 de abril de 2013;
- Norma Complementar nº 19/IN01/DSIC/GSI/PR, de 16 de julho de 2014;
- Norma Complementar nº 20/IN01/DSIC/GSI/PR, de 15 de dezembro de 2014;
- Norma Complementar nº 21/IN01/DSIC/GSI/PR, de 10 de outubro de 2014;

- Acórdão 1603/2008 TCU-Plenário - Levantamento de auditoria. situação da governança de tecnologia da informação - ti na administração pública federal. ausência de planejamento estratégico institucional. deficiência na estrutura de pessoal. tratamento inadequado à confidencialidade, integridade e disponibilidade das informações. recomendações
- Resolução nº 61/CONSUP/IFRO, de 18 de dezembro de 2015 - Dispõe sobre o Estatuto do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO
- Resolução nº 65/CONSUP/IFRO, de 29 de dezembro de 2015 - Dispõe sobre o Regimento Geral do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO;
- RESOLUÇÃO N° 18/CONSUP/IFRO, DE 01 ABRIL DE 2016 - Dispõe sobre o Regimento Interno do Colégio de Dirigentes do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia.
- PLANO DE DESENVOLVIMENTO INSTITUCIONAL – PDI 2018-2022
- NBR ISO/IEC 27001:2006 - define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI);
- NBR ISO/IEC 27002:2006 - código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação;
- NBR ISO/IEC 27003:2011 - diretrizes para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI);
- NBR ISO/IEC 27004:2010 - define métricas de medição para a gestão da segurança da informação; e
- NBR ISO/IEC 27005:2011 - define as diretrizes para o processo de gestão de riscos de segurança da informação.

CAPÍTULO XI

DAS PENALIDADES

Art. 17. O não cumprimento das determinações da POSIC sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do IFRO;

Art. 18. O descumprimento das disposições constantes nesta Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

Art. 19. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente;

CAPÍTULO XII

DA ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 20. A estrutura da Segurança da Informação e Comunicação do IFRO é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

I - **Política de Segurança da Informação e Comunicação (POSIC):** constituída neste documento, define a estrutura, as diretrizes, os papéis e responsabilidades referentes à segurança da informação e Comunicação e será detalhada em um conjunto de Normas específicas;

II - **Normas Complementares de Segurança da Informação (Normas)**: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem observados em diversas instâncias em que a informação seja tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas no documento "Atividade de Normatização" do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República; e

III - **Procedimentos de Segurança da Informação e Comunicações (Procedimentos):** instrumentalizam o disposto nas Normas, permitindo sua direta aplicação nas atividades do IFRO, cabendo a cada gestor a responsabilidade de gerá-los. Cada procedimento poderá ainda ser detalhado em instruções. Estes procedimentos e instruções serão de uso interno, não sendo obrigatória sua publicação.

CAPÍTULO XIII

COMPETÊNCIAS E RESPONSABILIDADES

Art. 21. Como forma de garantir o sucesso da gestão da segurança da informação no IFRO, é necessário a definição dos papéis de todos os envolvidos, bem como suas respectivas responsabilidades conforme descrito:

I - **Conselho Superior (CONSUP) -** Será responsável pela aprovação da Política de Segurança da Informação e Comunicação e suas respectivas diretrizes.

II - **Reitor do IFRO -** responsável pelo Instituto Federal, que compete:

a) Designar um Gestor de Segurança da Informação e Comunicação do IFRO e seu substituto;

b) Viabilizar o desenvolvimento dos trabalhos do Comitê Gestor de Segurança da Informação e Comunicação e da Equipe de Segurança da Informação.

c) Assegurar os recursos necessários para a implementação e gestão da POSIC do IFRO.

III - **Comitê Gestor de Segurança da Informação e Comunicação (CGSIC) -** é o órgão responsável pela elaboração e revisão periódica da Política de Segurança da Informação e Comunicação (POSIC) e normas relacionadas, tendo sua organização, composição, competências e funcionamento estão definidos neste Regimento e no seu Regimento próprio, que compete:

a) esclarecimento sobre questões não contempladas na POSIC e normas relacionadas;

b) monitorar a execução do Plano Estratégico de Tecnologia da Informação - PETI e Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC, sob a perspectiva da segurança da informação para sugerir e recomendar alterações que se façam necessárias;

c) dirimir dúvidas e deliberar sobre questões não contempladas pela política de segurança da informação ou pelas normas a ela relacionadas;

d) promover a cultura de segurança da informação e comunicação no IFRO, com a realização de campanhas de conscientização dos usuários quanto à política de segurança da informação;

e) avaliar as informações recebidas do monitoramento e da análise crítica dos incidentes de segurança da informação e comunicações, e recomendar ações apropriadas como resposta para os incidentes de segurança da informação e comunicações;

f) proposição, acompanhamento e divulgação dos planos de ação para aplicação da POSIC, incluindo a conscientização de usuários;

g) emitir pareceres e manifestar-se sobre qualquer assunto relativo à política de segurança da informação e quando solicitado pela administração superior;

h) proposição da implantação de soluções para eliminação ou minimização de riscos;

i) Propor programa orçamentário específico para as ações de segurança da informação e comunicação;

j) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República;

k) elaboração de propostas de normas complementares e políticas de uso dos recursos de informação, em todo o seu ciclo de vida, tecnológicos ou não, tais como:

i. acesso aos recursos de rede, inclusive internet;

ii. uso adequado de correio eletrônico (e-mail), estações de trabalho e dispositivos móveis fornecidos pelo IFRO;

iii. uso e instalação softwares

iv. monitoramento e auditoria dos recursos de tecnologia da informação; e. plano de continuidade do negócio; e

v. tratamento e resposta a incidentes em redes computacionais.

IV - **Gestor de Segurança da Informação e Comunicações -** é o representante do Comitê Gestor de Segurança da Informação e deve fazer o elo entre o Comitê Gestor de Segurança da Informação e Comunicação e a Equipe de Segurança da Informação e Comunicação, e tem as seguintes atribuições:

a) Coordenar o Comitê Gestor de Segurança da Informação e Comunicação;

b) Acompanhar atividades da Equipe de Segurança da Informação e Comunicações.

c) Propor programa orçamentário específica junto com o Comitê Gestor para capacitação da equipe de segurança e para as ações de segurança da informação e comunicação;

d) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional;

e) Propor normas relativas à segurança da informação e comunicação

f) Definir o plano de continuidade da Segurança da Informação e Comunicação

V - **Equipe de Segurança da Informação e Comunicação -** Grupo de Trabalho formado por representante de todos os setores da instituição e responsável por assessorar a implementação das ações de segurança da informação e comunicação no âmbito da Instituição e possui as seguintes atribuições:

a) Auxiliar na elaboração, atualização e divulgação das normas complementares relativas a esta Política de Segurança da Informação.

b) Apoiar ativamente o cumprimento da Política de segurança da Informação e Comunicação do IFRO

c) Auxiliar o Comitê Gestor de Segurança da Informação e Comunicação em suas deliberações

d) Conduzir a gestão tática e operação da Segurança da Informação

e) Apoiar na seleção de controles e soluções técnicas

f) Efetuar a Gestão dos incidentes de Segurança da Informação, garantindo tratamento e resolução adequados;

g) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicação;

h) Auditar atividades dos usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário;

i) Promover cultura de Segurança da Informação e Comunicação;

j) Elaborar o plano de continuidade de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre

k) Elaborar um plano de comunicação em caso de incidentes que envolvam a imagem institucional do IFRO.

l) Propor o Termo de Responsabilidade e Sigilo a ser adotado pela instituição

VI - **Equipe de Tratamento e Resposta a Incidentes -** Grupo de Trabalho responsável por executar as ações de respostas a incidentes de segurança da informação e comunicação. Formado pela equipe de TI dos Campi e da Reitoria

a) Monitorar atividades dos usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário e equipe de segurança da informação e comunicação

b) Promover cultura de Segurança da Informação e Comunicação;

c) Executar o Plano de Continuidade e Comunicação da instituição no caso de situação de falhas e desastres.

Parágrafo único: Fica instituído o Comitê Gestor de Segurança da Informação e Comunicação (CGSIC), formado pelos membros do Colégio de Dirigentes do IFRO (CODIR).

CAPÍTULO XIV

DAS DISPOSIÇÕES FINAIS

Art. 22. Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicação do IFRO devem ser direcionados ao Comitê Gestor de Segurança da Informação.

Art. 23. A presente política entra em vigor a partir da data de sua publicação.

ANEXO II - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DE COMUNICAÇÃO DO IFRO

Aprovado pela Resolução nº 57/CONSUP/IFRO, de 15 de outubro de 2019

I. IDENTIFICAÇÃO DA INSTITUIÇÃO

1.Dos Dados do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (Reitoria)

Quadro 1 - Dados Gerais do IFRO (Reitoria)

Nome	Instituto Federal de Educação, Ciência e Tecnologia de Rondônia	**Sigla**	IFRO
CNPJ	10.817.343/0005-01		
Lei	Lei nº 11.892, de 29 de dezembro de 2008		
Logradouro	Av. Tiradentes	**Nº**	3009
Bairro	Setor Industrial	**Cidade**	Porto Velho
Estado	Rondônia	**CEP**	76.804-124
E-mail	reitoria@ifro.edu.br	**Fone**	(69)2182-9601

Fonte: IFRO (2019)

Dos Dirigentes ligados a Reitoria:

Quadro 2 - Reitor e Pró-reitores do IFRO

Reitor	Uberlando Tiburtino Leite
Pró-reitor de Ensino	Edslei Rodrigues de Almeida
Pró-reitor de Pesquisa e Inovação e Pós-Graduação	Gilmar Alves Lima Júnior
Pró-reitor de Extensão	Maria Goreth Araújo Reis
Pró-reitor de Administração e Planejamento	Jéssica Cristina Pereira Santos
Pró-reitor de Desenvolvimento Institucional	Maria Fabíola Moraes da Assumpção Santos

Fonte: IFRO (2019)

Comissão responsável instituída pela Portaria nº 2686/REIT CGAB/IFRO, de 18 de dezembro de 2018, para a elaboração da Política de Política de Segurança da Informação e Comunicação:

Joilson Dantas Siqueira Silva	Diretoria de Gestão de Tecnologia da Informação - DGTI / Reitoria
Ana Cristina de Souza Falcão	Pró-Reitoria de Pesquisa, Inovação e Pós-Graduação PROPESP / Reitoria
Cledenice Blackman	Pró-Reitoria de Ensino - PROEN / Reitoria
Dennis Weberton Vendruscolo Gonçalves	Assessoria de Comunicação e Eventos - ASCOM / Reitoria
Erlan Fonseca de Souza	Diretoria de Gestão de Tecnologia da Informação - DGTI / Reitoria
Evandro Souza de Paula Cordeiro	Diretoria de Gestão de Tecnologia da Informação - DGTI / Reitoria
Ewerton Rodrigues Andrade	*Campus* Porto Velho Calama
Flavia Cristina do Nascimento Anziliero	Gabinete/Reitoria
Gislaine Cristina Rodrigues de Souza	Ouvidoria
Jaqueline Almeida de Andrade	Diretoria de Gestão de Pessoas - DGP/Reitoria
Jardel de Souza Pereira	Pró-Reitoria de Desenvolvimento Institucional - PRODIN/Reitoria
John Alison Ribeiro da Costa Maia	Pró-Reitoria de Administração - PROAD/Reitoria
Rogério Shockness da Silva	Pró-Reitoria de Extensão - PROEX / Reitoria

Fonte: IFRO (2018)