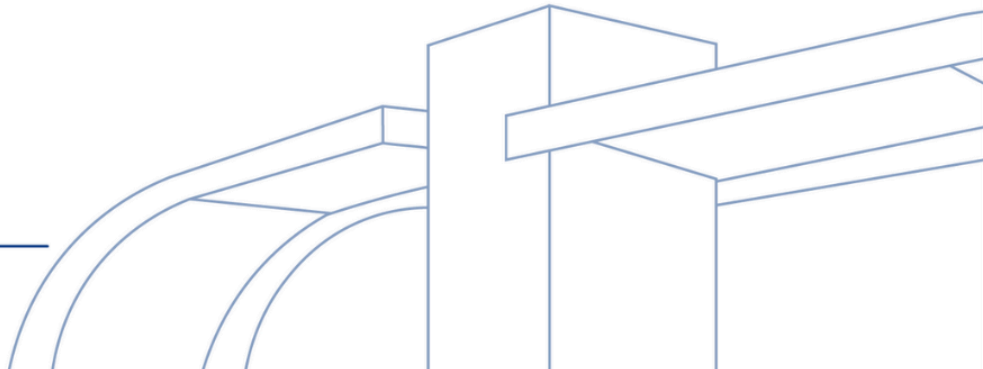
PoSIC

Política de Segurança da Informação e Comunicação

UFJ
UNIVERSIDADE
FEDERAL DE JATAÍ



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

UNIVERSIDADE FEDERAL DE JATAÍ

Prof. Dr. Christiano Peres Coelho

Reitor

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Wesley Carmo Ramos

Diretor

EQUIPE TÉCNICA DE ELABORAÇÃO

Nelcione Valério Dias

Gestor de Segurança da Informação

Wesley Carmo Ramos

Gestor de Tecnologia da Informação

Marcelo Silva Freitas

Encarregado de Dados Pessoais

Gustavo Oliveira de Melo

Coordenador de Infraestrutura

Walter Alves Costa

Coordenador de Desenvolvimento

Gabriel Vilela de Sousa

Coordenador de Suporte

EQUIPE REVISORA

COMITÊ DE APOIO À ELABORAÇÃO E REVISÃO DE ATOS NORMATIVOS - (CAN)

Profa. Dra. Alana Flávia Romani

Vice-Reitora

DIRETORIA DE ASSUNTOS ADMINISTRATIVOS - (DAA)

Prof. Dr. Hugo Luís Pena Ferreira

Diretor de Assuntos Administrativos

Histórico de versões

Data	Versão	Descrição	Autor
05/11/2025	1.0	Política de Segurança da Informação e Comunicação	Equipe Técnica de Elaboração

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE JATAÍ
REITORIA

Rodovia BR 364 – Km 192 Zona de Expansão Urbana
Caixa Postal. 03, CEP: 75801-615 Jataí-GO
(64) 3606-8202

RESOLUÇÃO CONSUNI/UFJ Nº -------/2025, DE ----- DE ---------- DE 2025

Dispõe sobre a Política de Segurança da Informação e Comunicação – PoSIC da Universidade Federal de Jataí.

O CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DE JATAÍ, no uso de suas atribuições legais e estatutárias, reunido em sessão plenária realizada no dia XX de XXXX de 2025, e considerando o que consta do processo nº 23854.007186/2025-49,

RESOLVE:

Art. 1º Fica aprovada a Política de Segurança da Informação e Comunicação da Universidade Federal de Jataí – UFJ, na forma do Anexo a esta Resolução, que estabelece princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.
Art. 2º Esta Resolução entra em vigor a partir de sua aprovação.

Prof. Dr. Christiano Peres Coelho
Reitor da Universidade Federal de Jataí

ANEXO DA RESOLUÇÃO CONSUNI/UFJ Nº -------/2025, DE ----- DE ---------- DE 2025
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DA UNIVERSIDADE FEDERAL DE JATAÍ

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Esta Política de Segurança da Informação e Comunicação – PoSIC aplica-se a todas as unidades organizacionais da Universidade Federal de Jataí – UFJ e deverá ser observada por todos os usuários de informação, colaborador, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de termo de responsabilidade ou documento equivalente, para acessar os ativos institucionais sob responsabilidade da Universidade Federal de Jataí.

Art. 2º Faz parte do escopo dessa política institucional a apresentação de forma clara de todas as diretrizes relacionadas à segurança da informação e comunicação dessa instituição.

§ 1º Esta PoSIC tem por objetivo estabelecer diretrizes, competências e responsabilidades relacionadas à segurança da informação e da comunicação no âmbito da UFJ e de suas diversas instâncias, sendo que normas, procedimentos, e mecanismos específicos para uso de serviços ou de ativos institucionais serão tratados em documentos específicos complementares a esta política.

§ 2º Esta PoSIC, acompanhada de suas eventuais normativas complementares, aplica-se às unidades administrativas e acadêmicas, conforme estabelecido no estatuto e regimento da UFJ, abrangendo servidores técnico-administrativos, corpo docente e discente, prestadores de serviços, colaboradores temporários e terceirizados, estagiários, jovens aprendizes, consultores externos e todos os que, de alguma forma, tenham acesso aos ativos institucionais, sejam eles físicos, lógicos ou documentais.

§ 3º Todas as pessoas mencionadas no § 2º são responsáveis pela proteção dos ativos de informação, de propriedade ou sob a custódia da UFJ, e devem estar comprometidos com o cumprimento desta PoSIC e de seus documentos complementares.

Art. 3º São objetivos da Política de Segurança da Informação e Comunicação da UFJ:

I – estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II – estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III – estabelecer competências e responsabilidades quanto à segurança da informação;

IV – nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação; e

V – promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da UFJ.

CAPÍTULO II
DOS PRINCÍPIOS E DIRETRIZES

Art. 4º As ações de segurança da informação da UFJ são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como os seguintes princípios:

I – disponibilidade, integridade, confidencialidade e autenticidade das informações;

II – não repúdio, assegurando que a autoria e o recebimento de comunicações, transações e ações possam ser comprovados de forma inequívoca, impedindo que as partes envolvidas neguem posteriormente sua participação;

III – resiliência, enquanto capacidade de projetar processos, sistemas e controles aptos a resistir e a se recuperar de incidentes, falhas ou desastres, garantindo a restauração rápida e segura das operações;

IV – economicidade da proteção dos ativos de informação;

V – respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

VI – observância da publicidade como preceito geral e do sigilo como exceção;

VII – responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VIII – alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico da UFJ, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

IX – conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis;

X – educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação;

XI – clareza na formulação das normas e diretrizes, garantindo que sejam objetivas, compreensíveis e de fácil aplicação por todos os usuários;

XII – defesa em camadas, adotando múltiplos níveis de controles de segurança para que, mesmo que uma camada seja comprometida, outras mantenham a proteção dos ativos; e

XIII – assegurar a aplicação e a manutenção das melhores práticas e padrões de mercado em todos os segmentos de Tecnologia da Informação, abrangendo o ciclo de vida completo do desenvolvimento de software, a gestão da infraestrutura e a excelência nos serviços de suporte.

Art. 5º As ações de segurança da informação da Universidade Federal de Jataí – UFJ são norteadas pelas seguintes diretrizes:

I – classificar a informação tratada no âmbito da instituição, sendo que o tratamento de toda e qualquer informação deve garantir os níveis de proteção adequados conforme sua classificação e as regras estabelecidas pela PoSIC-UFJ;

II – implementar os controles necessários para impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das operações, além de prevenir o acesso físico não autorizado, danos e interferências nas informações e em seus recursos de processamento da organização;

III – regulamentar, planejar e realizar a gestão de incidentes em segurança da informação com o objetivo de implantar processos, disponibilizar recursos e executar ações de prevenção, tratamento e resposta a qualquer evento adverso relacionado à segurança da informação, garantindo que os incidentes de segurança da informação sejam comunicados à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR, cujas responsabilidades e competências estão definidas em seção específica neste documento;

IV – regulamentar, planejar e executar o processo de mapeamento de ativos de informação com o objetivo de subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação;

V – implementar os controles adequados para assegurar que os recursos humanos e partes externas estejam em conformidade com suas atribuições, e estejam também conscientes e cumpram com as suas responsabilidades pela segurança da informação, antes e durante a contratação;

VI – implementar os controles adequados para proteger os interesses da instituição em caso de mudança ou encerramento da contratação de recursos humanos e partes externas, de forma que os recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros, devam ser destinados, exclusivamente, a fins diretos e complementares às atividades administrativas e acadêmicas da instituição, reservando, à UFJ, o direito de monitorar e controlar o uso dos recursos operacionais e de comunicações disponibilizados, assim como revogar permissões de acesso caso sejam identificadas irregularidades;

VII – regulamentar, planejar, implantar e gerenciar controles físicos e lógicos adequados para restringir o acesso à informação e aos recursos de processamento da informação às pessoas e entidades devidamente autorizadas, como forma de prevenção de incidentes de segurança;

VIII – elaborar o Plano de Gestão de Riscos de Segurança da Informação, devendo ser implementado e executado o processo de gestão de riscos de segurança da informação em compatibilidade com a gestão de riscos institucional, a missão e os objetivos estratégicos da universidade, os processos internos, os requisitos legais e a PoSIC-UFJ;

IX – elaborar o Plano de Gestão de Continuidade de Negócios em Segurança da Informação, que tem a finalidade de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres, devendo ser implementado e executado com base nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e em diretrizes institucionais sobre gestão de continuidade de negócio;

X – regulamentar, planejar e executar o processo de mudanças nos aspectos de segurança da informação, que tem a finalidade de mitigar eventuais resistências e obter mudanças eficazes e eficientes em decorrência da evolução de processos e tecnologias da informação, respaldando-se no processo de gestão de riscos de segurança da informação; e

XI – propiciar e subsidiar as condições necessárias para a realização de auditoria e avaliação de conformidade nos aspectos de segurança da informação, conforme a legislação vigente e as diretrizes institucionais.

Art. 6º As diretrizes supracitadas constituem os principais pilares da gestão de segurança da informação, norteando a elaboração de políticas, planos e normas complementares no âmbito da UFJ e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º As normas, procedimentos, manuais e metodologias de segurança da informação da UFJ devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º As ações de segurança da informação devem:

I – considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da UFJ;

II – ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da UFJ;

III – ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e

IV – visar à prevenção e tratamento de incidentes.

Art. 9º O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o risco de potenciais prejuízos à UFJ, à comunidade acadêmica e ao valor do ativo institucional a ser protegido.

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada na UFJ compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no caput, que tramitam pelo ambiente computacional da UFJ, são passíveis de monitoramento e auditoria pela UFJ, respeitados os limites legais.

Art. 11. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. O acesso aos recursos de tecnologia da informação da UFJ será concedido após a leitura e concordância do Termo de Responsabilidade/Uso e Aviso de Privacidade, indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da UFJ.

Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da UFJ, devem ser públicas e amplamente divulgadas a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os usuários devem ser continuamente sensibilizados quanto aos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º A fim de atender às ações previstas no § 1º, devem ser divulgados materiais educacionais sobre segurança da informação, produzidos institucionalmente ou por órgãos/equipes de segurança competentes.

Art. 13. Todos os contratos de prestação de serviços firmados pela UFJ conterão cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação, bem como de suas normas decorrentes.

§ 1º Os contratos e instrumentos congêneres deverão assegurar a aplicação integral desta Política e de suas normas a todos os terceiros que tenham acesso ou manuseiem ativos da instituição, prevendo cláusulas sobre sigilo, confidencialidade, uso adequado das informações e gestão de riscos.

§ 2º A parte contratada será responsável por manter níveis adequados de segurança e garantir que seus colaboradores cumpram as diretrizes estabelecidas, sob pena de sanções previstas em lei e nas normas internas.

Art. 14. A UFJ adota o Plano de Privacidade e Segurança da Informação – PPSI como framework estruturante para a aplicação, monitoramento e aprimoramento de suas práticas de proteção de dados pessoais e de segurança da informação, o qual se baseia em normas internacionais de gestão da segurança da informação.

Parágrafo único. A gestão de normas baseadas em padrões internacionais deverá ser considerada como via para o aumento de maturidade na gestão da segurança da informação, para alcançar certificações ISO/IEC específicas da área.

CAPÍTULO III
DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 15. A estrutura de Gestão de Segurança da Informação é composta por:

I – Alta Administração, na forma do Comitê Estratégico de Governança, Riscos e Controles – CGRC;

II – Comitê de Gestão Integrada de Dados e Segurança da Informação – CGDSI;

III – Gestor de Segurança da Informação;

IV – Gestor de Tecnologia da Informação e Comunicação;

V – Encarregado pelo Tratamento de Dados Pessoais;

VI – Responsável pela Unidade de Controle Interno;

VII – Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e

VIII – usuários de Informação.

Art. 16. Compete à Alta Administração, na forma do Comitê Estratégico de Governança, Riscos e Controles – CGRC:

I – instituir e designar os órgãos, comitês e gestores responsáveis pela governança e gestão da segurança da informação, assegurando que suas atribuições e composições estejam alinhadas às necessidades institucionais;

II – fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da Universidade Federal de Jataí, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

III – assegurar que as ações, políticas e controles de segurança da informação estejam alinhados ao Plano de Desenvolvimento Institucional, aos objetivos estratégicos e às metas organizacionais da Universidade Federal de Jataí, de forma a garantir que a proteção dos ativos de informação contribua efetivamente para o cumprimento da missão institucional e para a continuidade dos serviços essenciais;

IV – atuar como instância superior de decisão para dirimir casos omissos, dúvidas de interpretação e situações excepcionais relacionadas à Política de Segurança da Informação, incluindo deliberações sobre infrações graves e medidas corretivas cabíveis; e

V – formalizar e aprovar, no âmbito da gestão estratégica, a proposta da Política de Segurança da Informação e Comunicação, submetendo-a à deliberação do Conselho Universitário.

Art. 17. Compete ao Comitê de Gestão Integrada de Dados e Segurança da Informação – CGDSI:

I – assessorar na implementação das ações de segurança da informação;

II – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III – participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV – propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V – deliberar sobre normas internas de segurança da informação;

VI – implementar mecanismos para mitigar os riscos identificados no tratamento de dados pessoais por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais – RIPD;

VII – estabelecer procedimentos para registro, cancelamento e provisionamento de usuários nos sistemas institucionais que realizam tratamento de dados pessoais;

VIII – criar e gerir políticas e mecanismos de backup e trilhas de auditoria para garantir o ciclo de vida dos dados e informações pessoais;

IX – promover formas para coletar e analisar informações relacionadas a vulnerabilidades e ameaças à segurança da informação, produzindo a inteligência de ameaças e a gestão de vulnerabilidades;

X – estabelecer controle de acesso e autenticação segura às informações pessoais;

XI – definir processo formal para registro e cancelamento de usuários nos sistemas de informação institucionais, em especial os que realizam tratamento de dados pessoais;

XII – implantar a gestão de incidentes de segurança da informação; e

XIII – executar outras atribuições necessárias à implementação da Política de Segurança da Informação da UFJ.

Art. 18. Compete ao Gestor de Segurança da Informação:

I – Integrar o Comitê de Gestão Integrada de Dados e Segurança da Informação;

II – coordenar a elaboração da Política de Segurança da Informação e Comunicação e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

III – assessorar a Alta Administração na implementação da Política de Segurança da Informação e Comunicação;

IV – estimular ações de capacitação e de profissionalização, na forma de programa permanente de conscientização e treinamento, em temas relacionados à segurança da informação, por meio da disponibilização de materiais e cursos, produzidos institucionalmente ou por órgãos/equipes de seguranças competentes;

V – promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI – incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VII – propor à Alta Administração os recursos necessários às ações de segurança da informação;

VIII – coordenar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX – verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X – acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI – manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Parágrafo único. O Gestor de Segurança da Informação da UFJ será designado em ato administrativo próprio, de acordo com a legislação vigente.

Art. 19. Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Art. 20. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados – ANPD, conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Art. 21. Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 22. Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I – facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na UFJ;

II – monitorar as redes computacionais;

III – detectar e analisar ataques e intrusões;

IV – tratar incidentes de segurança da informação;

V – identificar vulnerabilidades e artefatos maliciosos;

VI – recuperar sistemas de informação;

VII – promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;

VIII – suspender temporariamente, se necessário, a utilização de sistemas em caso de ataque ou sistemas legados ao qual coloque dados pessoais da comunidade acadêmica expostos ou informações institucionais em risco;

IX – realizar o bloqueio de acesso de qualquer usuário, a qualquer tempo, que possua vínculo nos sistemas utilizados pela UFJ, uma vez detectados riscos de segurança;

X – notificar a Autoridade Nacional de Proteção de Dados e os titulares afetados em casos de incidentes relacionados a dados pessoais; e

XI – outras competências constantes em portaria própria da ETIR-UFJ.

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em ato administrativo próprio emitido pela Alta Administração, de acordo com a legislação vigente.

Art. 23. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e as demais normas específicas de segurança da informação da UFJ.

Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 24. Compete ao Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC observar integralmente as diretrizes e princípios estabelecidos nesta PoSIC, garantindo que todas as medidas de privacidade, segurança da informação, continuidade de serviços e aquisição de equipamentos de TIC estejam alinhadas ao Programa de Privacidade e Segurança da Informação – PPSI e disponham dos recursos necessários para sua implementação, além de refletir os requisitos institucionais e normativos, assegurando conformidade com as regulamentações aplicáveis e promovendo a governança eficaz da infraestrutura tecnológica da UFJ.

Art. 25. A Política de Segurança da Informação e Comunicação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

Art. 26. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I – tratamento da informação;

II – segurança física e do ambiente;

III – gestão de incidentes em segurança da informação;

IV – gestão de ativos;

V – gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, grupo de e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI – controles de acesso;

VII – gestão de riscos;

VIII – gestão de continuidade; e

IX – auditoria e conformidade.

§ 1º O Comitê de Gestão Integrada de Dados e Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento conforme a legislação vigente e boas práticas de segurança de informação.

Art. 27. As políticas, normas, procedimentos, orientações ou manuais de que trata o § 2º do art. 26 devem abordar, no mínimo, aspectos relacionados:

I – à conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

II – à classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III – à proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

IV – ao uso aceitável da informação e à utilização de mídias de armazenamento;

V – à entrada e saída de ativos de informação das instalações da organização;

VI – aos perímetros de segurança da organização;

VII – aos controles de acesso baseados no princípio do menor privilégio;

VIII – as etapas de identificação, contenção, erradicação, recuperação e atividades pós-incidente;

IX – aos critérios para a comunicação de incidentes aos titulares de dados pessoais e a ANPD;

X – ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;

XI – à Política de Gestão de Ativos da organização, abordando aspectos relacionados:

a) à proteção dos ativos e sua classificação de acordo com a criticidade do ativo para a organização;

b) à manutenção de inventário atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança;

c) ao uso aceitável de ativos, vedado o uso para fins particulares de seu responsável;

d) ao mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências;

e) ao monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; e

f) à investigação de sua operação e uso quando houver indícios de quebra de segurança ou privacidade;

XII – à utilização adequada dos recursos operacionais e de comunicações fornecidos pela UFJ, a serem utilizados para fins profissionais, relacionados às atividades dos órgãos, em conformidade com os princípios éticos e profissionais da UFJ, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação da instituição;

XIII – aos procedimentos para o uso de e-mail, grupo de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV – ao acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XV – ao uso de mídias sociais, à divulgação de informações nas mídias sociais, ao uso de contas pessoais para fins profissionais e à interação com estranhos nas mídias sociais;

XVI – às políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a conformidade com as leis e regulamentos aplicáveis;

XVII – às políticas e procedimentos para o controle de acesso, tais como recomendações de uso de senha forte, rotatividade de senha, uso de Múltiplo Fator de Autenticação – MFA, controles de autorização, baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação da UFJ;

XVIII – às políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando:

a) a análise do ambiente da UFJ, dos seus ativos de informação e das ameaças à segurança da informação;

b) a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência;

c) a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento; e

d) o tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos;

XIX – às políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Contingência para garantir que a UFJ possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Contingência para garantir sua eficácia;

XX – às políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças; e

XXI – às políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

§ 1º As unidades organizacionais da UFJ devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

§ 2º Todas as ações, realizadas pelas unidades da UFJ, que envolvam a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis a esta temática.

§ 3º As atividades, produtos e serviços desenvolvidos na UFJ devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

CAPÍTULO IV

DOS MECANISMOS E ESTRATÉGIAS DE CONTROLE E MONITORAMENTO

Art. 28. Como instrumento de referência, a UFJ adota o Framework PPSI, em conjunto com seus indicadores (iSeg e iPriv) e controles de segurança, para a medição da maturidade e da efetividade das ações de privacidade e segurança no âmbito institucional, assegurando conformidade à LGPD e às regulamentações nacionais pertinentes.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 29. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela UFJ para acesso, guarda e divulgação de material incompatível com o ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 30. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados pela Secretaria de Tecnologia da Informação – SeTI, exceto especificidades descritas na Política de Gestão de Ativos.

Art. 31. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários, exceto especificidades descritas na Política de Controle de Acesso.

Art. 32. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 33. As unidades organizacionais da UFJ devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 34. As denúncias de violação a esta Política podem ser comunicadas à ETIR.

Art. 35. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pela Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 36. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Parágrafo único. Eventuais ações corretivas para mitigação de riscos à segurança da informação estarão enunciadas em normas específicas, decorrentes das diretrizes gerais de segurança da informação enumeradas nesta Resolução.

Art. 37. O acesso às informações produzidas ou custodiadas pela UFJ, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades de seus colaboradores.

Parágrafo único. Em caso de dados ou informações importantes ao setor, mas que não sejam possíveis de serem acessados devido à saída de algum colaborador ou servidor, o Gestor de Segurança da Informação deverá ser contatado para poder tomar alguma providência.

Art. 38. Esta Política será revisada periodicamente, pelo menos a cada quatro anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente da UFJ, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 39. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e Comunicação e seus documentos devem ser submetidas ao Comitê de Gestão Integrada de Dados e Segurança da Informação.

Art. 40. Cabe a todo usuário que utiliza ou possua acesso aos sistemas da UFJ a observância das regras e fica vedado alegar desconhecimento da PoSIC da UFJ e suas normas complementares.

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação— Requisitos. Rio de Janeiro, 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 jul. 2024.

BRASIL. Presidência da República. Casa Civil. Instituto Nacional de Tecnologia da Informação. Portaria N° 79, de 31 de dezembro de 2018. Política de Segurança da Informação e Comunicações do Instituto Nacional de Tecnologia da Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 02 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação – PNSI. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.html. Acesso em: 17 jun. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-%20219115663. Acesso em: 01 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 01, de 27 de maio de 2020. Brasília, DF, GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/ptbr/composicao/SSIC/dsic/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 01 jul. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 03, de 28 de maio de 2021. Brasília, DF, GSI/PR, 2021. Disponível em: https://www.gov.br/gsi/pt-br/ssic/legislacao/copy_of_IN03_consolidada.pdf. Acesso em: 01 jul. 2024.

BRASIL. Presidência da República. Agência Nacional de Proteção de Dados - ANPD. Guia Orientativo - Tratamento de dados pessoais pelo Poder Público. Junho 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 01 jul. 2022.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. Guia do Framework de Privacidade e Segurança da Informação. Março 2024. Disponível em:https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf . Acesso em: 25 jun. 2024.

UNIVERSIDADE FEDERAL DO PARANÁ. Política de Segurança da Informação e Comunicação da UFPR (POSIC). Resolução nº 38/22 – COPLAD, aprovada em 14 dez. 2022. Curitiba: UFPR, 2022. Disponível em: https://ufpr.br/agtic/posic-politica-de-seguranca-da-informacao-e-comunicacao-da-ufpr/. Acesso em: 06 mai. 2025.

UNIVERSIDADE DE BRASÍLIA. Política de Segurança da Informação e Comunicação da Universidade de Brasília – PoSIC/UnB. Resolução da Câmara de Planejamento e Administração nº 004/2018 – PoSIC, atualizada pela Resolução nº 002/2024 – CONSUNI, Brasília: UnB, 2018. Disponível em: https://sti.unb.br/normativos-copy/. Acesso em: 06 mai. 2025.

UNIVERSIDADE FEDERAL DE VIÇOSA. Política de Segurança da Informação e Comunicações da UFV (POSIC-UFV). Viçosa: UFV, [ano de publicação]. Disponível em: https://www1.dti.ufv.br/politicas-normas-e-procedimentos/. Acesso em: 06 mai. 2025.

UNIVERSIDADE FEDERAL DE MINAS GERAIS. Política de Segurança da Informação – Posin. Belo Horizonte: UFMG, aprovada em setembro de 2023. Disponível em: https://www.ufmg.br/dti/posin. Acesso em: 06 mai. 2025.

UNIVERSIDADE FEDERAL DA BAHIA. Política de Segurança da Informação e Comunicações – PoSIC. Salvador: UFBA, [s.d.]. Disponível em: https://sti.ufba.br/posic. Acesso em: 06 mai. 2025.

UNIVERSIDADE FEDERAL DO CEARÁ. Política de Segurança da Informação da UFC (em elaboração). Fortaleza: UFC, [s.d.]. Disponível em: https://seginfo.ufc.br/wp-content/uploads/2019/02/posic-rev.05-dseg.pdf. Acesso em: 06 mai. 2025.

UNIVERSIDADE FEDERAL DE JATAÍ. Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC. Portaria nº 320, de 24 de abril de 2025. Jataí: UFJ, 2025. Disponível em: https://ufj.edu.br/wp-content/uploads/2025/04/SEI_UFJ___0421521___PORTARIA.pdf . Acesso em: 29 set. 2025.