MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE RORAIMA
CONSELHO UNIVERSITÁRIO
Av. Capitão Ene Garcez nº 2413, Bairro Aeroporto, Boa Vista-RR, CEP: 69.304-000
E-mail: secretariadosconselhos@ufrr.br
Site: ufrr.br/conselhos

UFRR

RESOLUÇÃO CUNI/UFRR Nº 035, de 16 de abril de 2021.

Aprova a Política de Segurança da Informação e Comunicação (POSIC) da Universidade Federal de Roraima (UFRR) e dá outras providências.

O **PRESIDENTE DO CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DE RORAIMA**, no uso de suas atribuições legais e estatutárias, e tendo em vista o que deliberou o Conselho Universitário – CUNI, na reunião extraordinária realizada no dia 07 de abril de 2021, e considerando o que consta no processo nº 23129.002208/2020-75,

RESOLVE:

Art. 1° Aprovar a Política de Segurança da Informação e Comunicação (POSIC) da Universidade Federal de Roraima (UFRR), conforme Anexo I, o qual passa a fazer parte da presente Resolução como se nela estivesse escrito.

Art. 2º Esta Resolução entra em vigor na data de sua publicação, revogando a Resolução n° 013/2012-CUni e demais disposições em contrário.

Secretaria dos Conselhos Superiores, Boa Vista, 16 de abril de 2021.

Prof. Dr. José Geraldo Ticianeli
Presidente do Conselho Universitário/UFRR

Publicada no Mural e no sítio de internet oficial dos Conselhos Superiores da UFRR
Em: 16/04/2021

ANEXO I

CAPÍTULO I
DO ESCOPO

Art. 1° A Política de Segurança da Informação e Comunicação (POSIC) objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade e autenticidade das informações custodiadas e de propriedade da UFRR, de modo a preservar os seus ativos e sua imagem institucional.

Art. 2° A POSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito da UFRR, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e descarte, visando á continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 3º O Comitê de Gestão de Segurança da Informação e Comunicações (COSIC) é um grupo multidisciplinar que tem a responsabilidade da avaliar, monitorar e direcionar as ações que visem a proteção das informações no âmbito da UFRR.

Art. 4° Esta POSIC se aplica a todas as unidades da UFRR, e poderá ser complementada por normas, regulamentos e procedimentos técnicos.

Art. 5° Os recursos necessários para promover a cultura de segurança da informação e comunicação, por meio de atividades de conscientização, capacitação e especialização e o que houver, serão previstos no orçamento da UFRR, conforme o Plano de Desenvolvimento Institucional (PDI).

Parágrafo único. O COSIC deverá fomentar as ações para a composição do PDI.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 6° Para os efeitos desta Resolução, entende-se por:

I - ameaça: conjunto de fatores ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

II - ativo de informação: componente humano, tecnológico ou físico que sustenta um ou mais processos de negócio da organização e que tem valor para ela;

III - ativo: qualquer bem, tangível ou intangível, que possui valor para a organização;

IV - classificação da informação: atribuição, definida pela autoridade competente, do grau de

sigilo dado à informação, documento, material, área ou instalação;

V - confidencialidade: propriedade da informação que objetiva mantê-la acessível somente por pessoas ou sistemas devidamente autorizados;

VI - controle de segurança: qualquer ação ou medida que reduza a probabilidade de ocorrência ou o grau de impacto decorrentes de um incidente de segurança;

VII - disponibilidade: propriedade da informação que objetiva garantir que a informação esteja acessível e que possa ser utilizada sempre que necessário;

VIII - dispositivo móvel: Equipamentos com capacidade para acessar, armazenar e processar informações que podem ser movidos fisicamente ou cujas capacidades podem ser utilizadas enquanto estiverem em movimento, tais como, mas não se limitando à smartphone, telefone celular, tablet, laptop, relógios inteligentes;

IX - hardware: é a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

X - incidente de segurança: é qualquer evento adverso que comprometa a integridade, a disponibilidade ou a confidencialidade;

XI - integridade: propriedade da informação que objetiva mantê-la em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou não;

XII - recurso computacional: conjunto de recursos de hardware, software e rede de computadores;

XIII - software: são todos os programas existentes em um computador ou dispositivos móveis, como sistema operacional, aplicativos, entre outros;

XIV - usuário: todo aquele que, de alguma maneira, acesse ou faça uso das informações da organização, seja servidor, colaborador, estagiário, discente ou prestador de serviços terceirizado.

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 7° Esta POSIC observa a legislação e normas específicas, como nas referências.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 8° A segurança da informação na UFRR abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos seguintes princípios:

I - confidencialidade: garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

II - disponibilidade garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;

III - integridade: garante a não-violação das informações com intuito de protegê-las contra

alteração, gravação ou exclusão acidental ou proposital.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Seção I

Da Classificação da Informação

Art. 9° As informações produzidas ou custodiadas pela UFRR serão classificadas em função do seu grau de confidencialidade, criticidade, disponibilidade, integridade e prazo de retenção.

§ 1° O COSIC, com o apoio, no que couber, das demais unidades pertinentes submeterá proposta de regulamentação da classificação das informações.

§ 2° A autorização, o acesso e o uso das informações produzidas ou custodiadas pela UFRR devem ser controlados de acordo com a respectiva classificação.

Art. 10. O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.

Art. 11. A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Seção II

Da Segurança da Informação para com Terceiros

Art. 12. Nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para o MEC deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, bem como deverá ser exigida, da entidade contratada, a assinatura do termo de confidencialidade.

Parágrafo único. As particularidades das relações com terceiros deverão ser definidas em norma interna específica.

Seção III

Do Uso de Recursos Computacionais e Comunicações

Art. 13. Os recursos de tecnologia da informação e telecomunicações devem ser utilizados para a execução das atividades profissionais e acadêmicas dos usuários, exclusivamente, respondendo estes, em qualquer hipótese, pelas condições gerais do recurso e pelo seu eventual mau uso.

Art. 14. É responsabilidade da área de Tecnologia de Informação e Comunicação (TIC), em conjunto com o Gestor de Segurança da Informação e Comunicação, definir controles de segurança que propiciem um uso seguro dos recursos de TIC, tanto do ponto de vista de hardware e software, quanto de treinamentos de conscientização e orientações sobre seu uso.

Art. 15. Não é permitida a intervenção do usuário para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de qualquer natureza no equipamento, seja recurso de hardware ou software.

Parágrafo único. As exceções serão solicitadas e registradas na área de TIC da UFRR.

Seção IV

Da Segurança em Redes de Computadores

Art. 16. A rede de computadores da organização deve ser monitorada a fim de que se evite sua sobrecarga ou atividades indevidas e que possam causar a indisponibilidade dos sis-temas ou comprometer a integridade ou confidencialidade das informações.

Art. 17. Softwares de proteção como firewalls e de detecção e prevenção de intrusos devem ser implementados e terem suas regras revisadas periodicamente, levando em consideração o princípio do menor nível de acesso possível.

Seção V

Da Gestão de Acesso à Internet

Art. 18. O acesso à Internet deve restringir-se à execução de atividades profissionais e se dar exclusivamente por meio de softwares homologados pela área de TIC.

Art. 19. O uso da Internet para fins pessoais é permitido desde que não contrarie nenhuma regra contida nesta política de segurança da informação, em suas normas complementares ou legislação aplicável.

Art. 20. A área de TIC deve prover mecanismos para que os usuários acessem a Internet de maneira segura, incluindo o uso de softwares de monitoramento e registro das atividades dos usuários.

Parágrafo único. É obrigação do usuário não acessar conteúdo duvidoso, ilegal ou que possa representar um risco para a organização.

Seção VI

Do Uso de Correio Eletrônico

Art. 21. O correio eletrônico da organização é ferramenta de comunicação e apenas como tal deve ser utilizada, sendo permitida sua utilização para fins pessoais, desde que não infrinja as regras contidas nesta política, em suas normas complementares ou legislação aplicável.

Art. 22. Critérios para concessão de acesso ao correio eletrônico, espaço de caixa postal, padrões de nomenclatura das caixas postais, período de retenção de mensagens e demais características do serviço devem ser definidas pela área de TIC e serem comunicadas para a organização sempre que alguma mudança ocorrer e que possa afetar diretamente o usuário.

Seção VII

Da Segurança em Recursos Humanos

Art. 23. As responsabilidades em relação à segurança da informação devem ser comunicadas na fase de contratação dos colaboradores, que devem ser orientados a seguir as diretrizes desta política e de suas normas complementares, assinando um termo de compromisso que deverá ficar de posse da área de recursos humanos.

Art. 24. É responsabilidade do gestor do usuário ou do contrato, em conjunto com a área de recursos humanos, informar a área de TIC sobre o desligamento de um colaborador ou término de um contrato, para que as credenciais de acesso sejam devidamente revogadas.

Seção VIII

Da Gestão de Riscos

Art. 25. A gestão de riscos deverá ser prevista no Plano Estratégico Institucional, que deverá ser orientada pela Política de Gestão de Riscos da UFRR e pela Política de Governança de TIC, conforme estabelecido na Norma Complementar n° 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, ou documento correspondente que venha a substituí-lo.

Seção IX

Da Gestão de Continuidade

Art. 26. A gestão de continuidade deverá ser prevista no plano de continuidade de negócios da UFRR, com o objetivo de manter a disponibilidade dos serviços de tecnologia de informação e comunicações, incluindo o uso de redundância em sua implantação e a definição de planos de contingência para cada cenário de indisponibilidade de sistemas, informações e processos críticos,

conforme estabelecido na Norma Complementar n° 06/IN01/DSIC/GSI/PR, de 11 de fevereiro de 2009, ou documento correspondente que venha a substituí-lo.

Parágrafo único. A Diretoria de Tecnologia da Informação (DTI) tem a prerrogativa de definir as ações necessárias para garantir a continuidade do negócio dos sistemas institucionais.

Seção X

Da Auditoria e Conformidade

Art. 27. A UFRR deve criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna da UFRR.

Art. 28. A UFRR deve, periodicamente, promover verificação de conformidade às regulamentações de segurança e legislações em vigor.

CAPÍTULO VI

DAS PENALIDADES

Art. 29. A não observância dos dispositivos da POSIC/UFRR ou de quaisquer de suas normas e/ou procedimentos complementares pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VII

DAS COMPETÊNCIAS E RESPONSABILIDADES DOS ÓRGÃOS

Art. 30. A estrutura para a Gestão de Segurança da Informação e Comunicações na UFRR é composta pelo(a):

I - Comitê de Segurança da Informação e Comunicações (COSIC);

II - Gestor de Segurança da Informação e Comunicação;

III - Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Seção I

Do Comitê de Segurança da Informação e Comunicação

Art. 31. O COSIC será designado pelo Reitor e constituído pelos seguintes membros:

I – Gestor de Segurança da Informação e Comunicação;

II – Diretor da Diretoria de Tecnologia da Informação (DTI);

III – 1 (um) representante da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

IV – 1 (um) representante da Pró-Reitoria de Ensino e Graduação (PROEG);

V – 1 (um) representante da Pró-Reitoria de Pesquisa e Pós-Graduação (PRPPG);

VI – 1 (um) representante da Pró-Reitoria de Assuntos Estudantis e Extensão (PRAE).

§ 1º Os suplentes dos itens I e II serão seus respectivos substitutos imediatos.

§ 2º O suplente do Item III será indicado, juntamente com o seu titular, serão indicados pela ETIR.

§ 3º Os suplentes dos itens IV, V e VI, juntamente com os seus respectivos titulares, serão indicados pelos seus respectivos pró-reitores.

§ 4º O COSIC será presidido pelo Gestor de Segurança da Informação e Comunicação.

§ 5º O representante de que trata o inciso III não pode ser o Gestor de Segurança da Informação e Comunicação.

Art. 32. O COSIC possui as seguintes competências:

I - assessorar na implementação das ações de segurança da informação e comunicações;

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

III - propor projetos, normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;

IV - apoiar a POSIC;

V - garantir a revisão periódica desta Política e de suas normas e procedimentos relacionados;

VI - acompanhar as investigações dos incidentes de segurança quando solicitado, especialmente aqueles que resultarem na violação da POSIC e das normas e procedimentos relacionados;

VII - determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;

VIII - acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação,

IX - desenvolver ações conjuntas com o Comitê de Governança Digital (CGD), quando se tratar de assuntos relacionados com Segurança da Informação.

Seção II

Do Gestor de Segurança da Informação e Comunicação

Art. 33. O Gestor de Segurança da Informação e Comunicação é a pessoa responsável pelas ações de segurança da informação e comunicação e também pela administração de informações geradas em seu em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades.

Art. 34. Compete ao Gestor de Segurança da Informação e Comunicações:

I - promover a cultura de Segurança da Informação e Comunicações (SIC);

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor os recursos necessários às ações de SIC,

IV – coordenar a ETIR.

Seção III

Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

Art. 35. A ETIR será composta por no mínimo de 3 (três) integrantes, no qual será coordenado pelo Gestor de Segurança da Informação e Comunicação.

Parágrafo único. Os membros serão designados pelo reitor.

Art. 36. A ETIR possui as seguintes competências:

I - fomentar ações que fortaleçam a prevenção aos incidentes;

II - investigar, diagnosticar e registrar os incidentes de Segurança da Informação;

III - propor o tratamento dos incidentes de Segurança da Informação;

IV - reportar ao COSIC os incidentes de Segurança da Informação;

V - propor meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR;

VI - prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação de equipamentos direcionados a Segurança da Informação e Comunicação;

VII - responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

CAPÍTULO VIII

DA ATUALIZAÇÃO

Art. 37. Esta POSIC deverá ser revisada e atualizada quando identificada necessidade ou a cada 12 meses, a contar da data de sua publicação.

CAPÍTULO IX

DOS CASOS OMISSOS

Art. 38. Os casos omissos serão apreciados inicialmente pelo COSIC, cabendo recurso ao CGD.

REFERÊNCIAS[i]

ABNT NBR ISO/IEC 27001:2013 - Sistemas de gestão de segurança da informação — Requisitos;

ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;

Decreto nº 8.135/2013 - Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional;

Instrução Normativa n° 01/DSIC/GSIPR - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

Lei n° 12.527/2011 - Regula o acesso a informações previsto no inciso XXXIII do Art. 5°, no inciso II do § 3° do Art. 37 e no § 2° do Art. 216 da Constituição Federal (Lei de Acesso à Informação);

Lei n° 12.965/2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. MARCO CIVIL DA INTERNET;

Lei nº 13.709/2018 – Lei Geral e Proteção de Dados Pessoais (LGPD), atualizada pela Lei nº 13.853, de 08 de julho de 2019.
Norma Complementar n° 03/IN01/DSIC/GSIPR - Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

Norma Complementar n° 11/IN01/DSIC/GSIPR - Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta — APF;

Portaria Interministerial MP/MC/MD n° 141 - Das regras para comunicações de dados da Administração Pública Direta, Autárquica e Fundacional. REGULAMENTAÇÃO DO DECRETO 8135/2013;

Portaria Interministerial n° 14/CDN - Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR n°01/2008;

[i] Mencionadas no art. 7º do Anexo I.