MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE RORAIMA
GABINETE DA REITORIA
Av. Capitão Ene Garcez, 2413, Bairro Aeroporto – Boa Vista/RR - CEP: 69.310-000
Telefone: (95) 3621-3102
E-mail: reitoria@ufrr.br

UFRR

PORTARIA NORMATIVA Nº 007/2020-GR/UFRR

Institui a Política de Segurança da Informação e Comunicação da UFRR e dá outras providências.

O **REITOR DA UNIVERSIDADE FEDERAL DE RORAIMA,** nomeado pelo Decreto de 02 de março de 2020, publicado no Diário Oficial da União de 03 de março de 2020, no uso de suas atribuições legais e estatutárias, e considerando o que consta no Memorando Eletrônico nº 83/2020-PROPLAN,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação e Comunicação da UFRR, doravante POSIC, conforme anexo, a qual passa a fazer parte integrante desta Portaria Normativa, como se nela estivesse escrito.

Art. 2º Esta Portaria Normativa entra em vigor na data de sua publicação.

GABINETE DO REITOR DA UFRR, Boa Vista, 03 de julho de 2020.

Prof. Dr. José Geraldo Ticianeli
Reitor da UFRR

Publicada no Mural e no sítio de internet oficial dos Conselhos Superiores da UFRR
Em: 03/07/2020

Av. Capitão Ene Garcez, 2413, Bairro Aeroporto – Boa Vista/RR - CEP: 69.310-000
Telefone: (95) 3621-3102
E-mail: reitoria@ufrr.br

UFRR

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DA UNIVERSIDADE FEDERAL DE RORAIMA

CAPÍTULO I
DO ESCOPO

Art. 1º 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. 2º 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 à 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 Esta POSIC se aplica a todas as unidades da estrutura regimental da UFRR.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os efeitos desta portaria 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: qualquer bem, tangível ou intangível, que possui valor para a organização.

III - Ativo de Informação: componente humano, tecnológico ou físico que sustenta um ou mais processos de negócio da organização e que tem valor para ela.

IV - Disponibilidade: propriedade da informação que objetiva garantir que a informação esteja acessível e que possa ser utilizada sempre que necessário.

V - 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.

VI - Confidencialidade: propriedade da informação que objetiva mantê-la acessível somente por pessoas ou sistemas devidamente autorizados.

VII - Incidente de Segurança: é qualquer evento adverso que comprometa a integridade, a disponibilidade ou a confidencialidade.

VIII - Classificação da Informação: atribuição, definida pela autoridade competente, do grau de sigilo dado à informação, documento, material, área ou instalação.

IX - Controle de Segurança: qualquer ação ou medida que reduza a probabilidade de ocorrência ou o grau de impacto decorrentes de um incidente de segurança.

X - *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.

XI - 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.

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

XIII - Recurso Computacional: conjunto de recursos de hardware, software e rede de computadores.

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.

XV - Comitê de Segurança da Informação: grupo multidisciplinar que tem a responsabilidade de avaliar, monitorar e direcionar ações que visem a proteção das informações da organização.

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

XVII - Gestor de Segurança da Informação: pessoa responsável pelas ações de segurança da informação e comunicações no âmbito da UFRR.

XVIII – Encarregado do Tratamento dos Dados Pessoais: pessoa responsável em atuar como canal de comunicação entre os órgãos de controle interno e externo à UFRR, além de coordenar o tratamento de toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 5º Esta POSIC observa a legislação e normas específicas, destacando-se:

a) Instrução Normativa no 01/DSIC/GSIPR - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

b) Norma Complementar no 03/IN01/DSIC/GSIPR - Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

c) Norma Complementar no 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.

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

e) Portaria Interministerial no 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 no 01/2008.

f) Decreto 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.

g) Portaria Interministerial MP/MC/MD no 141 - Das regras para comunicações de dados da Administração Pública Direta, Autárquica e Fundacional. REGULAMENTAÇÃO DO DECRETO 8135/2013.

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

i) ABNT NBR ISO/IEC 27001:2013 – Sistemas de gestão de segurança da informação – Requisitos.

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

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 6º 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; e

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. 7º As informações produzidas ou custodiadas pela UFRR serão classificadas em função do seu grau de confidencialidade, criticidade, disponibilidade, integridade e prazo de retenção.

§ 1º A Unidade responsável pela Segurança da Informação da UFRR e o Comitê Gestor de Segurança da Informação, com o apoio, no que couber, das demais Unidades pertinentes submeterá proposta de regulamentação da classificação das informações.

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

Art. 8º 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. 9º 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. 10. 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.

Parágrafo único. As senhas ou credenciais de acesso aos recursos computacionais de tecnologia da informação e comunicações são de estrita responsabilidade do usuário, portanto intransferível, sendo impeditivo a sua disponibilização para terceiros.

Art. 11. É responsabilidade da área de TIC, em conjunto com o gestor de segurança da informação, 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. 12. 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.

Av. Capitão Ene Garcez, 2413, Bairro Aeroporto – Boa Vista/RR - CEP: 69.310-000
Telefone: (95) 3621-3102
E-mail: reitoria@ufrr.br

Seção IV

Da Segurança em Redes de Computadores

Art. 13. 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 sistemas ou comprometer a integridade ou confidencialidade das informações.

Art. 14. *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. 15. 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. 16. 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. 17. 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. 18. 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. 19. 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. 20. 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. 21. 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

Do Tratamento de Incidentes de Rede Computacional

Art. 22. A área de TIC da UFRR manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Parágrafo único. A regulamentação da ETIR deve ser realizada por meio de documento de constituição aprovado pelo gestor da área de TIC da UFRR.

Seção IX

Da Auditoria e Conformidade

Art. 23. 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. 24. A UFRR deve, periodicamente, promover verificação de conformidade às regulamentações de segurança e legislações em vigor.

CAPÍTULO VI

DAS PENALIDADES

Art. 25. A não observância dos dispositivos da PSI/UFRR 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

DA ATUALIZAÇÃO E VIGÊNCIA

Art. 26. Esta POSIC deverá ser revisada e atualizada quando identificada necessidade ou a cada 12 meses a contar da data de sua publicação.