RESOLUÇÃO CGAG/CONSUNI/UFOB Nº 018, DE 24 DE AGOSTO DE 2023.

Institui a Política de Segurança da Informação – PSI da Universidade Federal do Oeste da Bahia - UFOB.

A CÂMARA DE GESTÃO ADMINISTRATIVA E GOVERNANÇA, ASSESSORA AO CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA, no uso de suas atribuições legais, considerando a deliberação extraída da sua 24ª Reunião Ordinária, realizada no dia 24 de agosto de 2023, homologada na 42ª Reunião Ordinária do Conselho Universitário, realizada no dia 12 de setembro de 2023,

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, da Presidência da República, que institui a Política Nacional de Segurança da Informação, que dispõe sobre a governança da segurança da informação e dá outras providências; e

CONSIDERANDO as Normativas emitidas pelos Órgãos Federais de Segurança Institucional que dispõem sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução institui a Política de Segurança da Informação – PSI da Universidade Federal do Oeste da Bahia com o objetivo de promover a segurança da informação a seus ativos, sejam eles tangíveis ou intangíveis, observados os princípios, objetivos e diretrizes estabelecidos neste documento, além das disposições constitucionais, legais e regimentais vigentes.

Art. 2º Os termos e definições que seguem são adotadas na Política de Segurança da Informação:

I - auditoria: consiste na avaliação dos registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à **internet**;

II - contas de acesso: permissões de acesso a recursos ou ativos concedidos de forma legal, pessoal e intransferível aos servidores públicos da Instituição, estudantes, servidores terceirizados ou, quando aplicável, ao público externo, sob um ou mais métodos de autenticação;

III - Comitê Permanente de Segurança da Informação: órgão responsável por revisar e acompanhar a aplicação da Política de Segurança da Informação, entre outras competências cabíveis;

IV - incidente de segurança da informação: uma ocorrência identificada de um sistema, serviço ou componente da rede que indique violação desta política ou mesmo falha de controles de segurança e situações não conhecidas;

V - redes administrativas: redes de dados lógicos dentro do perímetro confiável limitadas ao acesso de agentes públicos da Universidade Federal do Oeste da Bahia para a execução de atividades institucionais;

VI - segurança cibernética: conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação;

VII - integridade: garantir que a informação não sofra qualquer tipo de alteração ou violação indevida, não podendo ser modificada por pessoa não autorizada;

VIII - método de autenticação: utilização de mecanismos de segurança para legitimar o acesso de usuários aos sistemas, arquivos ou a qualquer suporte informacional;

IX - risco: combinação das consequências de um evento e de sua probabilidade associada de ocorrência;

X - usuários: técnico-administrativos em educação, docentes, estudantes, prestadores de serviços e público externo que façam uso de sistemas ou ativos de Tecnologia da Informação e Comunicação - TIC dentro da Instituição; e

XI - vulnerabilidade: existência conhecida ou desconhecida de fragilidade ou fragilidades de segurança em ativos.

Art. 3º A Política de Segurança da Informação abrange:

I - a segurança cibernética;

II - a segurança física e a proteção dos dados organizacionais;

III - a proteção dos dados pessoais dos usuários públicos e privados que mantém relação com a Universidade Federal do Oeste da Bahia; e

IV - as ações destinadas a garantir a segurança, a confidencialidade, a integridade e a autenticidade das informações.

Art. 4º Todas as ações, programas e projetos desenvolvidos pela Universidade Federal do Oeste da Bahia, voltados para a segurança da informação e proteção de dados, fazem parte desta Política de Segurança da Informação.

Art. 5º A Política de Segurança da Informação abrange a proteção das informações acessadas, processadas ou armazenadas pela Instituição em qualquer ativo, independente do suporte.

Parágrafo único. Informações de propriedade pessoal de usuários somente poderão ser fornecidas em atendimento à demanda judicial ou previsão legal, incluindo as voltadas para o acesso à informação.

Art. 6º Os usuários que tratam com dados e informações abrangidos nesta política e nas demais normas e resoluções complementares são corresponsáveis pela segurança da informação, não podendo alegar desconhecimento.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 7º Os princípios abrangidos nesta Política de Segurança da Informação são:

I - autenticidade: princípio pelo qual assegura que a informação produzida na Universidade Federal do Oeste da Bahia seja produzida e publicada por quem realmente diz ser;

II - confidencialidade: assegura que as informações que se fazem necessárias sejam disponíveis apenas pelas pessoas físicas ou jurídicas, entidades, sistemas e órgãos autorizados pela Universidade Federal do Oeste da Bahia;

III - disponibilidade: garante que a informação esteja disponível, sempre que se fizer necessária, por pessoas autorizadas pela Universidade Federal do Oeste da Bahia;

IV - integridade: garante que as informações produzidas pelos usuários e sistemas da Universidade não sofram alterações não-autorizadas;

V - legalidade: observação das normas e resoluções no âmbito da Universidade Federal do Oeste da Bahia e das demais leis vigentes;

VI - segurança da informação e comunicação: consideram-se normas, legislações, disposições e procedimentos aplicáveis vigentes;

VII - não repúdio: assegura que o emissor de uma informação não possa negar a autoria ou transmissão de uma mensagem, permitindo a sua identificação;

VIII - privacidade: garante o direito, pessoal e coletivo, à intimidade e ao sigilo da comunicação individual; e

IX - responsabilidade: assegura a discriminação dos papéis e responsabilidades dos atores envolvidos na manutenção desta política.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Art. 8º Todas as informações deverão ter grau de classificação de segurança e critérios definidos desde a sua criação ao manuseio, custódia e descarte.

Art. 9º As contas de usuários autorizados são pessoais e intransferíveis. Cada usuário é responsável por suas credenciais.

Parágrafo único. As contas de unidades administrativas são de responsabilidade de seus respectivos gestores.

Art. 10. Deverá ser implementado controle de acesso dos usuários credenciados aos sistemas institucionais, buscando prevenir a realização de atividades que venham ocasionar algum incidente de segurança.

Art. 11. Os recursos e dispositivos de tecnologia da informação e comunicação da Universidade Federal do Oeste da Bahia devem ser destinados para os fins a que se propõem, conforme interesse da administração.

Parágrafo único. A ciência do descumprimento do **caput** deste artigo deverá ser comunicada ao Comitê Permanente de Segurança da Informação.

Art. 12. Ficam estabelecidas as plataformas institucionais como canais autorizados à tramitação e comunicação de informações sensíveis.

Art. 13. Qualquer alteração realizada na estrutura lógica ou física da rede da Universidade Federal do Oeste da Bahia deverá ser autorizada e encaminhada pela unidade responsável.

Art. 14. É vedada a utilização de programas portáveis ou executáveis, não homologados pela unidade responsável da Universidade Federal do Oeste da Bahia, conectados por meio de armazenamento externo ou compartilhamento de rede nos computadores institucionais.

Art.15. Redes abertas de **wi-fi** ou outras redes de acesso ao público não devem ser utilizadas indiscriminadamente, e se aplicam todas as legislações vigentes e itens desta Política de Segurança da Informação quanto a responsabilidade perante o uso.

Art. 16. O controle de acesso a documento(s) e/ou processo(s) e às informações a ele(s) inerente(s) é de responsabilidade do órgão ou unidade que mantém a sua guarda.

§1º Os documentos em suporte papel somente poderão ser removidos da Universidade Federal do Oeste da Bahia com autorização expressa do responsável pela unidade que mantém sua guarda, devendo a retirada ser justificada e protocolada.

§2º É vedado fotografar, fazer imagem e armazenar em equipamento pessoal informações pessoais e sensíveis de processos acessados em razão do cargo, assim como transferir arquivos semelhantes a terceiros.

Art. 17. Os órgãos ou unidades que detém a guarda de documentos com informações pessoais e sensíveis poderão compartilhá-los com terceiros nas condições previstas na legislação vigente.

Art. 18. A Universidade Federal do Oeste da Bahia garantirá condições adequadas de guarda e armazenamento das informações.

Art. 19. Os processos em suporte papel, com prazo de guarda superior a dez anos ou de guarda permanente, deverão ser convertidos para o meio digital.

§1º A digitalização dos processos será precedida da avaliação dos conjuntos documentais, conforme estabelecido nas tabelas de temporalidade e destinação de documentos relativos às atividades-meio e às atividades-fim, de modo a identificar previamente os que devem ser encaminhados para descarte.

§2º A digitalização dos processos, caso ocorra, deve ser realizada de acordo com os termos da legislação vigente.

§3º Será assegurado descarte adequado do documento de modo a garantir a segurança da informação, inclusive durante o processo de descarte, independentemente de seu meio.

Art. 20. Deve haver segregação de funções nas ações referentes à segurança de informação de forma que não haja sobrecarga de funções e perda, alcançando a eficiência, publicidade e eficácia pretendida por esta política.

Art. 21. Qualquer vulnerabilidade ou incidente de segurança da informação conhecido pelos usuários deve ser imediatamente informado ao Comitê Permanente de Segurança da Informação da Universidade Federal do Oeste da Bahia para os encaminhamentos cabíveis.

Art. 22. Deverá ser implementado pela Universidade Federal do Oeste da Bahia um processo de Gestão de Riscos de Segurança da Informação com vistas a minimizar possíveis impactos associados aos ativos, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

Art. 23. Os ativos de informação tangíveis e intangíveis no âmbito da Universidade Federal do Oeste da Bahia são passíveis de auditoria técnica pela unidade responsável, segundo plano a ser estabelecido em norma específica.

Parágrafo único. Caberá ao Comitê Gestor de Tecnologia da Informação da Universidade Federal do Oeste da Bahia aprovar o plano de Auditoria e Conformidade que deverá incluir métodos, técnicas, procedimentos, normas e responsabilidades para o efetivo cumprimento do estabelecido por esta Política de Segurança da Informação.

Art. 24. Esta Política de Segurança da Informação deve ser revisada com periodicidade máxima de 4 (quatro) anos.

Art. 25. A Política de Segurança da Informação deverá ser informada aos usuários internos quando ingressarem na Instituição e, sempre que houver necessidade, aos usuários externos quando da contratação e fornecimento de serviços de/para terceiros que envolvam utilização dos ativos da Universidade, devendo passar por treinamento adequado todos aqueles que utilizarem ou tiverem acesso às informações confidenciais ou pessoais.

CAPÍTULO IV
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 26. A estrutura para a gestão da segurança da informação será composta por:

I - Comitê Permanente de Segurança da Informação;

II - Gestor de Segurança da Informação;

III - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

IV - Usuários; e

V - Gestores de órgãos, núcleos e unidades.

Parágrafo único. A composição e o funcionamento do Comitê Permanente de Segurança da Informação deverão ser regulamentados por regimento próprio.

Art. 27. Compete ao Comitê Permanente de Segurança da Informação:

I - assessorar a 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; e

V - deliberar sobre normas internas de segurança da informação.

Art. 28. Compete ao Gestor de Segurança da Informação:

I - promover a cultura de segurança da informação;

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

III - coordenar o Comitê Permanente de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação; e

V - manter contato permanente e estreito com o órgão responsável pela Segurança da Informação e Comunicações do governo federal para o trato de assuntos relativos à segurança da informação.

Art. 29. Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais:

I - coordenar as atividades de tratamento e resposta a incidentes, tais como: recuperação de sistemas, análise de ataques e intrusões, análise e tratamento de interrupção do funcionamento de aplicações e serviços suportados por tecnologias de informação e comunicação; e

II - elaborar e atualizar periodicamente plano de contingência frente à incidentes, visando assegurar a continuidade dos serviços.

Art. 30. É de responsabilidade de todos os usuários:

I - cumprir políticas, normas e procedimentos de Segurança da Informação;

II - usar recursos tecnológicos apenas para fins profissionais e acadêmicos aprovados e de interesse da Instituição;

III - proteger informações pessoais ou confidenciais que tenha em posse contra acesso, modificação, divulgação ou destruição não autorizada; e

IV - comunicar imediatamente qualquer violação identificada aos responsáveis pelo tratamento e resposta de riscos.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 31. Os casos omissos surgidos na aplicação do disposto na Política de Segurança da Informação da Universidade Federal do Oeste da Bahia deverão ser tratados pelo Comitê Permanente de Segurança da Informação.

Art. 32. As normas complementares, referentes a temas como controle de acesso, gestão de contas, gestão de ativos, computação em nuvem, entre outros constantes na legislação vigente, deverão ser elaboradas e aprovadas em até 24 (vinte e quatro) meses após a publicação desta Resolução.

Art. 33. Esta Resolução entra em vigor em 1º de novembro de 2023.

gov.br Documento assinado digitalmente
LERIANE SILVA CARDOZO
Data: 27/09/2023 10:09:38-0300
Verifique em https://validar.iti.gov.br

LERIANE SILVA CARDOZO
Presidente da Câmara de Gestão Administrativa e Governança

gov.br Documento assinado digitalmente
JACQUES ANTONIO DE MIRANDA
Data: 24/10/2023 14:16:22-0300
Verifique em https://validar.iti.gov.br

JACQUES ANTONIO DE MIRANDA
Presidente do Conselho Universitário