Serviço Público Federal

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS

PROCESSO 23520.001280/2023-02

ELETRÔNICO

Cadastrado em 23/02/2023

Processo disponível para recebimento com código de barras/QR Code

Nome(s) do Interessado(s):	E-mail:	Identificador:
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	cgtic@ufob.edu.br	11011009
PRÓ-REITORIA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	protic@ufob.edu.br	110106

Tipo do Processo:
PROPOSTA DE RESOLUÇÃO

Assunto do Processo:
010.01 - ORGANIZAÇÃO E FUNCIONAMENTO - NORMATIZAÇÃO. REGULAMENTAÇÃO

Assunto Detalhado:
PROPOSTA DE RESOLUÇÃO PARA INSTITUIR A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA

Unidade de Origem:
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (11.01.10.09)

Criado Por:
VANESSA GODOY KINOSHITA

Observação:

MOVIMENTAÇÕES ASSOCIADAS

Data	Destino
23/02/2023	SECRETARIA DOS ÓRGÃOS DE DELIBERAÇÃO SUPERIOR (11.01.21)

Data	Destino

Para visualizar este processo, entre no **Portal Público** em https://sig.ufob.edu.br/public e acesse a Consulta de Processos.

Visualizar no Portal Público

RELATÓRIO DE PROPOSIÇÃO AO CONSUNI

Instrução do Processo: Comitê Gestor de Tecnologia da Informação e Comunicação
Processo: 23520.001280/2023-02
Assunto: Proposta de Política de Segurança da Informação da Universidade Federal do Oeste da Bahia
Interessado: Comitê Gestor de Tecnologia da Informação e Comunicação
Proponente: Comitê Gestor de Tecnologia da Informação e Comunicação
Documento de designação: Portaria CGTIC/UFOB nº 06, de 31 de março de 2021.

OBJETO DA PROPOSTA

Trata-se de proposta de Política de Segurança da Informação - PSI da Universidade Federal do Oeste da Bahia – UFOB.

CONSIDERAÇÕES

O Decreto nº 9.637, de 26 de dezembro de 2018, institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no país. Conforme art. 15, alínea II, cada órgão e entidade da administração pública federal deve "elaborar usa política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República".

Em atendimento ao disposto no Decreto nº 9.637, o Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC) instituiu uma comissão por meio da Portaria CGTIC/UFOB nº 06, de 31 de março de 2021, com o objetivo de elaborar a proposta da Política de Segurança da Informação da UFOB. A proposta foi apreciada e aprovada em reunião ordinária do CGTIC, do dia 14 de março de 2022, conforme ata em anexo.

DESCRIÇÃO

O objetivo da política é promover a segurança da informação aos ativos da universidade, sejam eles tangíveis ou intangíveis, observados os princípios, objetivos e diretrizes apresentados na proposta.

O documento é estruturado em 5 (cinco) capítulos, a saber:

I – Disposições Preliminares;

II – Dos Princípios;

III – Diretrizes Gerais;

IV – Competências e Responsabilidades; e

V – Disposições Finais.

CONSIDERAÇÕES FINAIS

Considerando as atribuições do CGTIC, apresento a Proposta de Resolução da Política de Segurança da Informação - PSI da UFOB para ser apreciada pela Câmara de Gestão Administrativa e Governança (CGAG).

Barreiras, 22 de fevereiro de 2023.

Vanessa Godoy Kinoshita

Presidente do Comitê Gestor de Tecnologia da Informação e Comunicação

Emitido em 2023

RELATÓRIO DE PROPOSIÇÃO À CGAG Nº 1/2023 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 23/02/2023 11:55)
VANESSA GODOY KINOSHITA
PROTIC (11.01.06)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1**, ano: **2023**, tipo: **RELATÓRIO DE PROPOSIÇÃO À CGAG**, data de emissão: **23/02/2023** e o código de verificação: **af23d5a0c7**

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Comitê Gestor de Tecnologia da Informação e Comunicação

PORTARIA CGTIC/UFOB Nº 06, DE 31 DE MARÇO DE 2021

Institui comissão para elaborar a Política de Segurança da Informação da Universidade Federal do Oeste da Bahia.

A PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGTIC), no uso das atribuições que lhe conferem a Portaria nº 214/2021 do Gabinete da Reitoria da UFOB, e

Considerando o disposto no Art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018;

Considerando a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), que dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, resolve:

Art. 1º INSTITUIR comissão para elaborar a Política de Segurança da Informação da Universidade Federal do Oeste da Bahia.

Art. 2º DESIGNAR Leila Oliveira dos Anjos, Cailon Franca de Castro, Uiliam Rangel Amorim Souza e Luiz Hilário Ferreira Damascena, sob presidência da primeira, para comporem a comissão.

Art. 3º ESTABELECER o prazo de 60 (sessenta) dias, a contar de 06/03/2021, para a conclusão dos trabalhos da referida comissão.

Publique-se, cumpra-se e registre-se.

VANESSA GODOY KINOSHITA

Presidente do Comitê Gestor de Tecnologia da Informação e Comunicação

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

Emitido em 04/04/2021

PORTARIA Nº 1504/2021 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 23/02/2023 11:55)
VANESSA GODOY KINOSHITA
PROTIC (11.01.06)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1504**, ano: **2021**, tipo: **PORTARIA**, data de emissão: **23/02/2023** e o código de verificação: **9bc0d6cf4b**

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Comitê Gestor de Tecnologia da Informação e Comunicação

PORTARIA CGTIC/UFOB Nº 08, DE 04 DE ABRIL DE 2021

Retifica a data de início dos trabalhos da comissão para elaborar a Política de Segurança da Informação da Universidade Federal do Oeste da Bahia.

A PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGTIC), no uso das atribuições que lhe conferem a Portaria nº 214/2021 do Gabinete da Reitoria da UFOB, resolve:

Art. 1º RETIFICAR a Portaria CGTIC/UFOB Nº 06/2021, de 31 de março de 2021, onde se lê:

> "Art. 3º ESTABELECER o prazo de 60 (sessenta) dias, a contar de 06/03/2021, para a conclusão dos trabalhos da referida comissão."

Leia-se:

> "Art. 3º ESTABELECER o prazo de 60 (sessenta) dias, a contar de **06/04/2021**, para a conclusão dos trabalhos da referida comissão."

VANESSA GODOY KINOSHITA
Presidente do Comitê Gestor de Tecnologia da Informação e Comunicação

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

Emitido em 04/04/2021

PORTARIA Nº 1505/2021 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 23/02/2023 11:55)
VANESSA GODOY KINOSHITA
PROTIC (11.01.06)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1505**, ano: **2021**, tipo: **PORTARIA**, data de emissão: **23/02/2023** e o código de verificação: **138dad956f**

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA

Conselho Superior

Câmara de Gestão Administrativa e Governança

RESOLUÇÃO CGAG/CONSUNI/UFOB nº XXX, DE XXXDE XXXXX DE XX

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

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 xxª Reunião Ordinária/Extraordinária, realizada no dia xx de x de xxxx,

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

CONSIDERANDO a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, resolve**:**

CAPÍTULO I

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 aos 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, discentes, servidores terceirizados ou, quando aplicável, ao público externo, sob um ou mais métodos de autenticação;

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

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 - evento 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 pessoal 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 da probabilidade de Risco x Consequências;

X - usuários: técnicos administrativos em educação, docentes, discentes, 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 os dados armazenados 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:

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

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 ao pessoal e coletivo, a intimidade e o sigilo da comunicação individual; e

IX - responsabilidade: os papéis e responsabilidades dos atores envolvidos na manutenção.

CAPÍTULO III

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.

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

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 documentos, avulso ou processo, e demais informações é de responsabilidade da unidade que mantém sua guarda.

§1º Os documentos em suporte papel somente poderão ser removidos da Universidade Federal do Oeste da Bahia com autorização do responsável pela unidade, 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 brasileira.

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 atividade-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.

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, incidente ou evento de segurança da informação, conhecido pelos seus usuários, deve ser imediatamente informado à unidade responsável pela segurança da informação da Universidade Federal do Oeste da Bahia para os encaminhamentos cabíveis.

Art. 22. Deverá ser construído 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,

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

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 periodicamente.

CAPÍTULO IV

COMPETÊNCIAS E RESPONSABILIDADES

Art. 25. 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); e
IV - Usuários.

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

Art. 26. 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. 27. 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.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 28. 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. 29. Esta resolução entra em vigor em xx de xxxx de xxxx.

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

LERIANE SILVA CARDOSO

Presidente da Câmara de Gestão Administrativa e Governança

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

Emitido em 2023

PROPOSTA DE RESOLUÇÃO Nº 1/2023 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 23/02/2023 11:55)
VANESSA GODOY KINOSHITA
PROTIC (11.01.06)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1**, ano: **2023**, tipo: **PROPOSTA DE RESOLUÇÃO**, data de emissão: **23/02/2023** e o código de verificação: **c4c3371691**

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA

ATA DO CGTIC Nº 3 / 2022 - CGTIC (11.01.10.09)

Nº do Protocolo: 23520.005313/2022-02

Barreiras-BA, 16 de Maio de 2022

Ata da 1ª Reunião Ordinária do Comitê Gestor de Tecnologia da Informação e Comunicação da Universidade Federal do Oeste da Bahia de 2022

Aos **quatorze dias do mês de março de dois mil e vinte e dois**, às quatorze horas e dez minutos, em uma sala de videoconferência da plataforma *Google Meet*, reuniram-se, em caráter ordinário, os membros do Comitê Gestor de Tecnologia da Informação e Comunicação - CGTIC, sob a presidência da Pró-Reitora de Tecnologia da Informação e Comunicação (PROTIC), **Vanessa Godoy Kinoshita**, com a presença da representante da Pró-Reitoria de Administração (PROAD), **Jaqueline Fritsch**, da representante da Pró-Reitoria de Extensão e Cultura (PROEC), **Daniela Cristina Calado**, da representante da Pró-Reitoria de Graduação (PROGRAD), **Adma Katia Lacerda Chaves**, da representante da Pró-Reitoria de Planejamento e Desenvolvimento Institucional (PROPLAN), **Leriane Silva Cardozo**, do representante da Pró-Reitoria de Gestão de Pessoas (PROGEP), **Clayton da Silva Barcelos**, do representante da Pró-Reitoria de Tecnologia da Informação e Comunicação (PROTIC), **David Dutkievicz**, do representante do Centro Multidisciplinar de Barra (CMBARRA), **Jairo Torres Magalhães Junior**, do representante do Centro das Ciências Biológicas e da Saúde (CCBS), **Rafael da Conceição Simões**, do representante do Centro das Ciências Exatas e das Tecnologias (CCET), **Valdeilson Souza Braga**, do representante do Centro Multidisciplinar de Bom Jesus da Lapa (CMLAPA), **Tony Silva Almeida**, do representante do Centro Multidisciplinar de Luís Eduardo Magalhães (CMLEM), **Bruno Motta Oliveira**, da representante do Centro Multidisciplinar de Santa Maria da Vitória (CMSAMAVI), **Vera Regiane Brescovici Nunes**, da representante da Superintendência Administrativa do Campus Reitor Edgard Santos (SACRES), **Adriana Migliorini Kieckhöfer**, e do representante da Superintendência de Inovação, Tecnologia e Desenvolvimento Regional (SITDR), **Erick Samuel Rojas Cajalvica**, para tratarem dos seguintes pontos de pauta: **1) Informes; 2) Apreciação das atas das reuniões do CGTIC dos dias 08/11/2021 e 14/02/2022; 3) Apreciação do Plano de Trabalho para a elaboração do PDTIC 2022-2024; 4) Apreciação de proposta de revisão do PDTIC 2020-2022; 5) Continuação da apreciação da Política de Segurança da Informação; 6) Apresentação dos Relatórios da Auditoria Interna; e 7) Apresentação da retomada da ação de inventário de TIC**. Havendo *quórum*, a Sra. presidente, Vanessa Godoy Kinoshita, cumprimentou e agradeceu a presença dos membros do Comitê e deu início à reunião perguntando se os membros teriam informes a fazer, não havendo manifestações. A Sra. presidente, então, informou que foi publicada a portaria nº 414, de 22 de fevereiro de 2022, que altera a composição do CGTIC. Passando ao segundo ponto de pauta, a Sra. presidente perguntou aos membros do Comitê se havia contribuições às atas. Como não houve manifestações, **a Sra. presidente submeteu as atas das reuniões do CGTIC dos dias 08/11/2021 e 14/02/2022 ao regime de votação, sendo aprovadas por unanimidade**. Dando seguimento ao terceiro ponto de pauta, a Sra. presidente passou a fala à coordenadora da equipe de elaboração do PDTIC 2022-2024, Sra. Leriane Silva Cardozo, que apresentou o Plano de Trabalho descrevendo cada um dos tópicos do documento e apresentou detalhadamente o cronograma das atividades definidas, com início em 03/03/2022 e publicação planejada para 14/06/2022. Em seguida, a Sra. presidente reforçou que a metodologia e a estrutura apresentadas no Plano de Trabalho seguiram o guia definido pelo SISP e então abriu o espaço para contribuições dos membros. Como não houve manifestações, **a Sra. presidente submeteu o Plano de Trabalho para a elaboração do PDTIC 2022-2024 ao regime de votação, sendo aprovado por unanimidade**. Para o quarto ponto de pauta, a Sra. presidente explicou que as demandas de TIC para 2022 foram recebidas e consolidadas e relembrou que as contratações serão feitas com base nessa consolidação, excluindo-se o que havia antes, e abriu o espaço para manifestações dos membros. A Sra.

Leriane atentou para os valores que podem ultrapassar o orçamento e perguntou se cada gestor fará análise dos valores do que foi colocado ou se isso será feito posteriormente. A Sra. Jaqueline Fritsch pediu a palavra para ressaltar, além da questão orçamentária levantada pela Sra. Leriane, que as estimativas devem refletir o que está na proposta orçamentária e que a lista dos itens de TIC é apenas uma parte do montante de itens que serão necessários adquirir. O Sr. Jairo Torres Magalhães Junior solicitou uma correção e suas demandas e perguntou como deve proceder. A Sra. presidente, considerando as colocações, sugeriu então prorrogar o prazo para que todos os setores reavaliem seus pedidos para readequação ao orçamento e posterior consolidação. Ressaltou, ainda, que, conforme orientação da Proad, o valor estimado das demandas pode ultrapassar até 30% (trinta por cento) do orçamento da unidade. Para esclarecer essa orientação, a Sra. Jaqueline explicitou que, nesse caso, a porcentagem deve ser contada sobre o valor que o setor pretende gastar com TIC, e não sobre o custeio total, reforçando, ainda, que se refere ao orçamento específico de cada unidade. O Sr. Rafael da Conceição Simões fez uma solicitação para que as reuniões do CGTIC sejam agendadas para às quintas-feiras, considerando que os Diretores dos centros também dão aulas. A Sra. Leriane perguntou à Sra. Jaqueline se o valor de custeio também pode ser considerado 30% a maior. A Sra. Jaqueline respondeu que, em tese, os 30% já são suficientes para os itens de TIC, mas que para os demais itens de custeio, pode ser aplicado até 50% a mais no valor, dependendo da especificidade e quantidade dos itens. Em seguida, a Sra. Adma Katia Lacerda Chaves explicou que foram solicitados itens para atender ao Núcleo de Tecnologias Educacionais que não foram considerados com base no orçamento da Prograd e perguntou se essas demandas seriam mantidas sob o custeio da unidade. A Sra. Leriane indicou que haverá informação sobre uma emenda parlamentar e que poderá responder à essa dúvida posteriormente. O Sr. Bruno Motta Oliveira perguntou, devido a problemas de conectividade, se a orientação era de que o valor dos pedidos de TIC seja 30% superior ao valor total do custeio. A Sra. Jaqueline explicou que a orientação considera o custeio como um todo, devido aos procedimentos licitatórios, e acrescentou que as unidades precisam considerar todas as suas demandas e, de forma que os itens de TIC não representam todas as necessidades, estes não podem corresponder ao valor total do custeio da unidade. O Sr. Bruno perguntou, em seguida, se as 500 baterias CR2032 solicitadas pela Protic seriam para suprir a demanda de toda UFOB. A Sra. presidente respondeu que seriam para uso na Reitoria e para emergências, de forma que cada unidade deve solicitar as suas. O Sr. David Dutkievicz atentou que a quantidade de pilhas solicitada para o CMLEM é pequena e sugeriu que os centros reavaliem esses itens considerando o retorno presencial às atividades na universidade. A Sra. Leriane perguntou o que deveria ser considerado em relação aos *softwares*. A Sra. presidente respondeu que deve ser considerada a cotação e a modalidade de contratação, que pode ser perpétua ou por locação por tempo determinado, de forma que deve ser levantada a questão da renovação para o ano seguinte. A Sra. Jaqueline complementou informando que os valores para aquisição dos *softwares* são provenientes dos custeios de cada unidade. Como não houve mais manifestações, **a Sra. presidente suspendeu o ponto de pauta para reavaliação das demandas pelas unidades**. Passando ao quinto ponto de pauta, a Sra. presidente explicou que foram feitas as inclusões das contribuições da reunião anterior e que o documento foi formatado conforme as normas de redação oficial da UFOB e acrescentou que, após aprovação do texto no CGTIC, o mesmo será encaminhado para parecer na Câmara de Gestão Administrativa e Governança (CGAG) e perguntou se os membros teriam contribuições ao documento. Como não houve manifestações, **a Sra. presidente submeteu a Política de Segurança da Informação ao regime de votação, sendo aprovada por unanimidade**. Dando seguimento ao sexto ponto de pauta, a Sra. presidente explanou sobre as duas ações da Auditoria Interna (nº 02/2022 e nº 03/2022) voltadas para TIC e apresentou o resumo dos achados e as recomendações feitas, direcionadas ao *datacenter* insuficiente e exposto a riscos diversos, à força de trabalho insuficiente, à ausência de Política de Segurança da Informação e Comunicação e de controle de acesso à informação, recursos e serviços de TIC, à ausência de Política de Gestão de Riscos, à carência de política e sistema de cópias de segurança (*backup*) e restauração de dados, à gestão do ciclo de vida dos ativos inoperantes, aos sistemas eletrônicos de registro patrimonial desatualizados, aos bens não localizados, ao não recolhimento dos *desktops* substituídos por *notebooks*, à fragilidade na preservação física dos ativos acessíveis ao público e à ausência de política de descarte ou desfazimento dos ativos inservíveis. Em seguida, abriu o espaço para discussão dos membros. A Sra. Jaqueline complementou que as ações são ligadas à TIC, mas que envolvem outros setores e esclareceu que a legislação referente ao desfazimento de bens tem sofrido alterações, mudando as regras do processo. Acrescentou que o inventário será retomado e que foi concluída a instalação da carga de dados para o SIADS e sugeriu que talvez este sistema seja suficiente para controle dos ativos, não sendo necessário alimentar o sistema Veredas. A Sra. presidente iniciou o sétimo ponto de pauta indicando que foram adquiridos *notebooks* a mais para uso de 20 novos docentes e salientou que vários docentes ainda não

solicitaram entrega do equipamento, acrescentou também que será solicitada manifestação dos docentes para manter o *notebook* ou o *desktop* e, em seguida, informou que será feito o recolhimento dos computadores substituídos, além de uma reorganização dos mesmos para que todos os usuários utilizem equipamentos na garantia e com *Windows* 10. Complementou que serão analisadas as necessidades de peças para *upgrade* de máquinas e de travas de segurança para os *desktops*, bem como serão mapeados os processos de inventário e desfazimento. A Sra. presidente explicou, ainda, que o uso do sistema Veredas deve ser continuado pois o mesmo possui um agente para atualização automática do inventário dos computadores, capaz de fazer uma varredura tanto de *hardware* como de *softwares* instalados nas máquinas. O Sr. Rafael perguntou como isso será comunicado à comunidade. A Sra. presidente sugeriu a composição de uma comissão com os técnicos de TIC dos *campi* para a realização dessas atividades, sob coordenação da gestora do Núcleo de Infraestrutura de TIC da Protic. O Sr. Jairo perguntou quantos dos 500 *notebooks* adquiridos já foram entregues, pois há cargos vagos de docentes no CMBARRA. A Sra. presidente explicou que os 500 foram adquiridos conforme o orçamento disponibilizado à época e que os primeiros 100 que foram recebidos pela universidade foram distribuídos com base em prioridade de uso, não havendo preferência para docentes. Já os demais 400 *notebooks* entregues foram reservados para os docentes, encaminhados conforme tabela da Progep. Os equipamentos que sobraram estão reservados para os docentes que ainda não solicitaram e para os novos docentes que devem chegar à universidade. Para confirmar a informação, o Sr. Jairo perguntou se a reserva dos 20 *notebooks* mencionada anteriormente considera as vagas não preenchidas do *campus* de Barra. A Sra. presidente passou a fala para o Sr. Clayton da Silva Barcelos, que respondeu que sim, estavam previstos na quantidade já reservada. A Sra. presidente relembrou que solicitará às chefias imediatas dos técnicos de TI autorização da participação dos mesmos na comissão para realização do inventário. O Sr. Bruno apontou para a dificuldade de realização dos *backups* para os *notebooks*, indicando que alguns docentes estão sem espaço em nuvem e perguntou se já houve limitação do espaço e qual é delimitação atual do mesmo. A Sra. presidente respondeu que a limitação não foi feita, pois a proposta ainda será apreciada pela CGAG, e sugeriu que os *backups* sejam feitos utilizando o espaço em nuvem da Microsoft. Reforçou, por fim, que deve ser feita a avaliação dos tipos de licença dos *softwares* conforme a destinação do uso (acadêmico ou administrativo). Como não houve outras manifestações, a Sra. presidente agradeceu a presença dos participantes e encerrou a reunião. Nada mais havendo a tratar, eu Beatriz dos Santos Seidel, lavrei a presente ata que, após lida e achada conforme, segue assinada por mim e todos os presentes. Barreiras, 14 de março de 2022.

(Assinado digitalmente em 17/05/2022 10:44)
ADMA KATIA LACERDA CHAVES
PRO-REITOR(A)
Matrícula: 1860243

(Assinado digitalmente em 16/05/2022 18:44)
ADRIANA MIGLIORINI KIECKHOFER
SUPERINTENDENTE
Matrícula: 1907442

(Assinado digitalmente em 16/05/2022 16:39)
BEATRIZ DOS SANTOS SEIDEL
SECRETARIO
Matrícula: 2993352

(Assinado digitalmente em 17/05/2022 15:59)
BRUNO MOTTA OLIVEIRA
DIRETOR
Matrícula: 1218313

(Assinado digitalmente em 16/05/2022 22:45)
CLAUDIO REICHERT DO NASCIMENTO
PRO-REITOR(A)
Matrícula: 1146719

(Assinado digitalmente em 17/05/2022 16:59)
CLAYTON DA SILVA BARCELOS
PRO-REITOR(A)
Matrícula: 1494568

(Assinado digitalmente em 16/05/2022 16:50)
DAVID DUTKIEVICZ
COORDENADOR
Matrícula: 1870822

(Assinado digitalmente em 16/05/2022 18:36)
ERICK SAMUEL ROJAS CAJAVILCA
SUPERINTENDENTE
Matrícula: 1683056

(Assinado digitalmente em 20/05/2022 08:52)
JAQUELINE FRITSCH
PRO-REITOR(A)
Matrícula: 1583761

(Assinado digitalmente em 17/05/2022 10:45)
LERIANE SILVA CARDOZO
PRO-REITOR(A)
Matrícula: 2265035

(Assinado digitalmente em 21/05/2022 22:33)
MARILIA CONCEICAO DE SOUZA CACERES
PROFESSOR DO MAGISTERIO SUPERIOR
Matrícula: 1554371

(Assinado digitalmente em 17/05/2022 09:37)
RAFAEL DA CONCEICAO SIMOES
DIRETOR
Matrícula: 1207764

(Assinado digitalmente em 17/05/2022 10:12)
TONY SILVA ALMEIDA
DIRETOR
Matrícula: 1073305

(Assinado digitalmente em 19/05/2022 14:59)
VANESSA GODOY KINOSHITA
PRO-REITOR(A)
Matrícula: 1575718

(Assinado digitalmente em 17/05/2022 10:06)
VERA REGIANE BRESCOVICI NUNES
DIRETOR
Matrícula: 1034382

Para verificar a autenticidade deste documento entre em https://sig.ufob.edu.br/documentos/ informando seu número: **3**, ano: **2022**, tipo: **ATA DO CGTIC**, data de emissão: **16/05/2022** e o código de verificação: **82e44cbf2f**

Emitido em 16/05/2022

ATA Nº 1/2022 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 23/02/2023 11:55)
VANESSA GODOY KINOSHITA
PROTIC (11.01.06)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1**, ano: **2022**, tipo: **ATA**, data de emissão: **23/02/2023** e o código de verificação: **5898f3bd99**

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

DESPACHO Nº 2/2023 - CGTIC (11.01.10.09)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 23 de fevereiro de 2023.

Prezada Sra Gleicianne Dourado,
Secretária dos Órgãos de Deliberação Superior

Ao cumprimentá-la cordialmente, encaminho o processo nº 23520.001280/2023-02 de solicitação de apreciação da Proposta de Política de Segurança da Informação da Universidade Federal do Oeste da Bahia pela Câmara de Gestão Administrativa e Governança.
Coloco-me à disposição para esclarecimentos.

Respeitosamente,

(Assinado digitalmente em 23/02/2023 11:55)
VANESSA GODOY KINOSHITA
PROTIC (11.01.06)
Matrícula: ###757#8

Processo Associado: 23520.001280/2023-02

Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018

Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

O PRESIDENTE DA REPÚBLICA , no uso da atribuição que lhe confere o art. 84, **caput** , inciso VI, alínea “a”, da Constituição,

DECRETA :

CAPÍTULO I

DISPOSIÇÕES GERAIS

~~Art. 1º Fica instituída a Política Nacional de Segurança da Informação - PNSI, 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.~~

Art. 1º Fica instituída a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional. (Redação dada pelo Decreto nº 10.641, de 2021)

Art. 2º Para os fins do disposto neste Decreto, a segurança da informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física e a proteção de dados organizacionais; e

IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º São princípios da PNSI:

I - soberania nacional;

II - respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

III - visão abrangente e sistêmica da segurança da informação;

IV - responsabilidade do País na coordenação de esforços e no estabelecimento de políticas, estratégias e diretrizes relacionadas à segurança da informação;

V - intercâmbio científico e tecnológico relacionado à segurança da informação entre os órgãos e as entidades da administração pública federal;

VI - preservação do acervo histórico nacional;

VII - educação como alicerce fundamental para o fomento da cultura em segurança da informação;

VIII - orientação à gestão de riscos e à gestão da segurança da informação;

IX - prevenção e tratamento de incidentes de segurança da informação;

X - articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação;

XI - dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

XII - **need to know** para o acesso à informação sigilosa, nos termos da legislação;

XIII - consentimento do proprietário da informação sigilosa recebida de outros países, nos casos dos acordos internacionais;

XIV - cooperação entre os órgãos de investigação e os órgãos e as entidades públicos no processo de credenciamento de pessoas para acesso às informações sigilosas;

XV - integração e cooperação entre o Poder Público, o setor empresarial, a sociedade e as instituições acadêmicas; e

XVI - cooperação internacional, no campo da segurança da informação.

CAPÍTULO III

DOS OBJETIVOS

Art. 4º São objetivos da PNSI:

I - contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais;

II - fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação;

III - aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação;

IV - fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação;

V - fortalecer a cultura da segurança da informação na sociedade;

VI - orientar ações relacionadas a:

a) segurança dos dados custodiados por entidades públicas;

b) segurança da informação das infraestruturas críticas;

c) proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica; e

d) tratamento das informações com restrição de acesso; e

VII - contribuir para a preservação da memória cultural brasileira.

CAPÍTULO IV

DOS INSTRUMENTOS

Art. 5º São instrumentos da PNSI:

I - a Estratégia Nacional de Segurança da Informação; e

II - os planos nacionais.

Art. 6º A Estratégia Nacional de Segurança da Informação conterá as ações estratégicas e os objetivos relacionados à segurança da informação, em consonância com as políticas públicas e os programas do Governo federal, e será dividida nos seguintes módulos, entre outros, a serem definidos no momento de sua publicação:

I - segurança cibernética;

II - defesa cibernética;

III - segurança das infraestruturas críticas;

IV - segurança da informação sigilosa; e

V - proteção contra vazamento de dados.

Parágrafo único. A construção da Estratégia Nacional de Segurança da Informação terá a ampla participação da sociedade e dos órgãos e das entidades do Poder Público.

Art. 7º Os planos nacionais de que trata o inciso II do **caput** do art. 5º conterão:

I - o detalhamento da execução das ações estratégicas e dos objetivos da Estratégia Nacional de Segurança da Informação;

II - o planejamento, a organização, a coordenação das atividades e do uso de recursos para a execução das ações estratégicas e o alcance dos objetivos da Estratégia Nacional de Segurança da Informação; e

III - a atribuição de responsabilidades, a definição de cronogramas e a apresentação da análise de riscos e das ações de contingência que garantam o atingimento dos resultados esperados.

Parágrafo único. Os planos nacionais serão divididos em temas e designados a um órgão responsável, conforme estabelecido na Estratégia Nacional de Segurança da Informação.

CAPÍTULO V

DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO

Art. 8º Fica instituído o Comitê Gestor da Segurança da Informação, com atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República nas atividades relacionadas à segurança da informação.

Art. 9º O Comitê será composto por um representante titular e respectivo suplente indicados pelos seguintes órgãos:

I - Gabinete de Segurança Institucional da Presidência da República, que o coordenará;

II - Casa Civil da Presidência da República;

~~III - Ministério da Justiça;~~

III - Ministério da Justiça e Segurança Pública; (Redação dada pelo Decreto nº 9.832, de 2019)

~~IV - Ministério da Segurança Pública;~~

IV - Ministério da Defesa; (Redação dada pelo Decreto nº 9.832, de 2019)

~~V - Ministério da Defesa;~~

V - Ministério das Relações Exteriores; (Redação dada pelo Decreto nº 9.832, de 2019)

~~VI - Ministério das Relações Exteriores;~~

VI - Ministério da Economia; (Redação dada pelo Decreto nº 9.832, de 2019)

~~VII - Ministério da Fazenda;~~

VII - Ministério da Infraestrutura; (Redação dada pelo Decreto nº 9.832, de 2019)

~~VIII - Ministério dos Transportes, Portos e Aviação Civil;~~

VIII - Ministério da Agricultura, Pecuária e Abastecimento; (Redação dada pelo Decreto nº 9.832, de 2019)

~~IX - Ministério da Agricultura, Pecuária e Abastecimento;~~

IX - Ministério da Educação; (Redação dada pelo Decreto nº 9.832, de 2019)

~~X - Ministério da Educação;~~

X - Ministério da Cidadania; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XI - Ministério da Cultura;~~

XI - Ministério da Saúde; (Redação dada pelo Decreto nº 9.832, de 2019)

XI-A - Ministério do Trabalho e Previdência; (Incluído pelo Decreto nº 10.849, de 2021)

~~XII - Ministério do Trabalho;~~

XII - Ministério de Minas e Energia; (Redação dada pelo Decreto nº 9.832, de 2019)

XII-A - Ministério das Comunicações; (Incluído pelo Decreto nº 10.641, de 2021)

~~XIII - Ministério do Desenvolvimento Social;~~

~~XIII - Ministério da Ciência, Tecnologia, Inovações e Comunicações; (Redação dada pelo Decreto nº 9.832, de 2019)~~

XIII - Ministério da Ciência, Tecnologia e Inovações; (Redação dada pelo Decreto nº 10.641, de 2021)

~~XIV - Ministério da Saúde;~~

XIV - Ministério do Meio Ambiente; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XV - Ministério da Indústria, Comércio Exterior e Serviços;~~

XV - Ministério do Turismo; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XVI - Ministério de Minas e Energia;~~

XVI - Ministério do Desenvolvimento Regional; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XVII - Ministério do Planejamento, Desenvolvimento e Gestão;~~

XVII - Controladoria-Geral da União; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XVIII - Ministério da Ciência, Tecnologia, Inovações e Comunicações;~~

XVIII - Ministério da Mulher, da Família e dos Direitos Humanos; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XIX - Ministério do Meio Ambiente;~~

XIX - Secretaria-Geral da Presidência da República; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XX - Ministério do Esporte;~~

XX - Secretaria de Governo da Presidência da República; (Redação dada pelo Decreto nº 9.832, de 2019)

~~XXI - Ministério do Turismo;~~
~~XXI - Advocacia-Geral da União; e~~ (Redação dada pelo Decreto nº 9.832, de 2019)

XXI - Advocacia-Geral da União; (Redação dada pelo Decreto nº 10.849, de 2021)

~~XXII - Ministério da Integração Nacional;~~
~~XXII - Banco Central do Brasil.~~ (Redação dada pelo Decreto nº 9.832, de 2019)

XXII - Banco Central do Brasil; e (Redação dada pelo Decreto nº 10.849, de 2021)

XXII-A - Autoridade Nacional de Proteção de Dados. (Incluído pelo Decreto nº 10.849, de 2021)

~~XXIII - Ministério das Cidades;~~ (Revogado pelo Decreto nº 9.832, de 2019)
~~XXIV - Ministério da Transparência e Controladoria-Geral da União;~~ (Revogado pelo Decreto nº 9.832, de 2019)
~~XXV - Ministério dos Direitos Humanos;~~ (Revogado pelo Decreto nº 9.832, de 2019)
~~XXVI - Secretaria-Geral da Presidência da República;~~ (Revogado pelo Decreto nº 9.832, de 2019)
~~XXVII - Secretaria de Governo da Presidência da República;~~ (Revogado pelo Decreto nº 9.832, de 2019)
~~XXVIII - Advocacia-Geral da União; e~~ (Revogado pelo Decreto nº 9.832, de 2019)
~~XXIX - Banco Central do Brasil.~~ (Revogado pelo Decreto nº 9.832, de 2019)

~~§ 1º Os membros do Comitê serão indicados pelos titulares dos órgãos mencionados no **caput** , no prazo de dez dias, contado da data de publicação deste Decreto, e serão designados em ato do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, no prazo de vinte dias, contado da data de publicação deste Decreto.~~

§ 1º Os membros do Comitê Gestor da Segurança da Informação e os respectivos suplentes serão indicados pelos titulares dos órgãos que representam e designados em ato do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República. (Redação dada pelo Decreto nº 10.641, de 2021)

~~§ 2º A indicação do membro titular dos órgãos mencionados no **caput** recairá no gestor de segurança da informação de que trata o inciso III do **caput** do art. 15, e o respectivo suplente deverá ocupar cargo em comissão do Grupo-Direção e Assessoramento Superiores, de nível 4 ou superior, ou equivalente.~~
~~§ 2º O membro titular do Comitê Gestor da Segurança da Informação deverá ser o gestor de segurança da informação de que trata o inciso III do **caput** do art. 15, e seu suplente deverá ser ocupante de cargo em comissão ou função de confiança equivalente ou superior ao nível 4 do Grupo-Direção e Assessoramento Superiores.~~
~~(Redação dada pelo Decreto nº 9.832, de 2019)~~

§ 2º Os membros de que trata o § 1º deverão ser indicados dentre os agentes públicos que possuam atribuição para definir políticas ou normas relacionadas à tecnologia da informação ou à segurança da informação nos respectivos órgãos. (Redação dada pelo Decreto nº 10.641, de 2021)

§ 3º Os membros titulares do Comitê serão substituídos pelos respectivos suplentes, em suas ausências ou impedimentos.

~~§ 4º A participação no Comitê será considerada prestação de serviço público relevante, não remunerada.~~

§ 4º A participação no Comitê Gestor da Segurança da Informação e nos subcolegiados será considerada prestação de serviço público relevante, não remunerada. (Redação dada pelo Decreto nº 9.832, de 2019)

~~§ 5º No prazo de noventa dias, contado da data de publicação deste Decreto, será aprovado regimento interno para dispor sobre a organização e o funcionamento do Comitê.~~

§ 5º O Coordenador do Comitê Gestor da Segurança da Informação aprovará o regimento interno, que disporá sobre a organização e o funcionamento do Comitê, no prazo de noventa dias, contado da data de publicação do Decreto nº 9.832, de 12 de junho de 2019. (Redação dada pelo Decreto nº 9.832, de 2019)

Art. 10. O Comitê se reunirá, em caráter ordinário, semestralmente e, em caráter extraordinário, por convocação de seu Coordenador.

§ 1º As reuniões do Comitê ocorrerão, em primeira convocação, com a presença da maioria simples de seus membros ou, quinze minutos após a hora estabelecida, em segunda convocação, com a presença de, no mínimo, um terço de seus membros.

~~§ 2º O Comitê poderá instituir grupos de trabalho ou câmaras técnicas para tratar de temas específicos relacionados à segurança da informação e poderá convidar representantes do setor público ou privado e especialistas com notório saber.~~ (Revogado pelo Decreto nº 9.832, de 2019)

~~§ 3º A composição, o funcionamento e as competências dos grupos de trabalho ou câmaras técnicas serão estabelecidos pelo Comitê.~~ (Revogado pelo Decreto nº 9.832, de 2019)

§ 4º As deliberações do Comitê serão aprovadas pela maioria simples dos membros presentes e o Coordenador, além do voto regular, terá o voto de desempate.

~~§ 5º Os membros do Comitê Gestor da Segurança da Informação que se encontrarem no Distrito Federal se reunirão presencialmente e os membros que se encontrem em outros entes federativos participarão da reunião por meio de videoconferência.~~ (Incluído pelo Decreto nº 9.832, de 2019)

§ 5º Os membros do Comitê Gestor da Segurança da Informação que se encontrarem no Distrito Federal se reunirão presencialmente ou por videoconferência, nos termos do disposto no Decreto nº 10.416, de 7 de julho de 2020, e os membros que se encontrarem em outros entes federativos participarão da reunião por meio de videoconferência. (Redação dada pelo Decreto nº 10.641, de 2021)

Art. 10-A. O Comitê Gestor da Segurança da Informação poderá instituir subcolegiados com o objetivo de tratar de temáticas específicas relacionadas à segurança da informação. (Incluído pelo Decreto nº 9.832, de 2019)

Art. 10-B. Os subcolegiados a que se refere o art. 10-A: (Incluído pelo Decreto nº 9.832, de 2019)

I - serão compostos na forma de ato do Comitê Gestor da Segurança da Informação; (Incluído pelo Decreto nº 9.832, de 2019)

II - não poderão ter mais de sete membros; (Incluído pelo Decreto nº 9.832, de 2019)

III - terão caráter temporário e duração não superior a um ano; e (Incluído pelo Decreto nº 9.832, de 2019)

IV - estão limitados a quatro operando simultaneamente. (Incluído pelo Decreto nº 9.832, de 2019)

~~Art. 11. O Gabinete de Segurança Institucional da Presidência da República prestará o apoio técnico e administrativo necessário ao Comitê.~~

~~Art. 11. A Secretaria-Executiva do Comitê Gestor da Segurança da Informação será exercida pelo Departamento de Segurança da Informação da Secretaria de Coordenação de Sistemas do Gabinete de Segurança Institucional da Presidência da República.~~ (Redação dada pelo Decreto nº 9.832, de 2019)

Art. 11. A Secretaria-Executiva do Comitê Gestor da Segurança da Informação será exercida pelo Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República. (Redação dada pelo Decreto nº 10.641, de 2021)

CAPÍTULO VI

DAS COMPETÊNCIAS

Seção I

Do Gabinete de Segurança Institucional da Presidência da República

~~Art. 12. Compete ao Gabinete de Segurança Institucional da Presidência da República, nos temas relacionados à segurança da informação, assessorado pelo Comitê Gestor da Segurança da Informação:~~

Art. 12. Compete ao Gabinete de Segurança Institucional da Presidência da República, nos temas relacionados à segurança da informação: (Redação dada pelo Decreto nº 10.641, de 2021)

I - estabelecer norma sobre a definição dos requisitos metodológicos para a implementação da gestão de risco dos ativos da informação pelos órgãos e pelas entidades da administração pública federal;

II - aprovar diretrizes, estratégias, normas e recomendações;

III - elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação dos servidores públicos federais e da sociedade;

IV - acompanhar a evolução doutrinária e tecnológica, em âmbito nacional e internacional;

V - elaborar e publicar a Estratégia Nacional de Segurança da Informação, em articulação com o Comitê Interministerial para a Transformação Digital, criado pelo Decreto nº 9.319, de 21 de março de 2018 ;

VI - apoiar a elaboração dos planos nacionais vinculados à Estratégia Nacional de Segurança da Informação;

VII - estabelecer critérios que permitam o monitoramento e a avaliação da execução da PNSI e de seus instrumentos;

~~VIII - propor a edição dos atos normativos necessários à execução da PNSI; e~~

VIII - propor a edição dos atos normativos necessários à execução da PNSI; (Redação dada pelo Decreto nº 10.641, de 2021)

~~IX - estabelecer os requisitos mínimos de segurança para o uso dos produtos que incorporem recursos de segurança da informação, de modo a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação e garantir a interoperabilidade entre os sistemas de segurança da informação, ressalvadas as competências específicas de outros órgãos.~~

IX - estabelecer os requisitos mínimos de segurança para o uso dos produtos que incorporem recursos de segurança da informação, de modo a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação e garantir a interoperabilidade entre os sistemas de segurança da informação, ressalvadas as competências específicas de outros órgãos; e (Redação dada pelo Decreto nº 10.641, de 2021)

X - articular-se com centros nacionais de prevenção, tratamento e resposta a incidentes cibernéticos pertencentes a outros países. (Incluído pelo Decreto nº 10.641, de 2021)

Parágrafo único. Nas hipóteses de que trata o inciso IX do **caput** , quando se tratar de competência de outro órgão, caberá ao Gabinete de Segurança Institucional da Presidência da República propor as atualizações referentes à segurança da informação.

Seção II

Do Ministério da Defesa

Art. 13. Ao Ministério da Defesa compete:

I - apoiar o Gabinete de Segurança Institucional da Presidência da República nas atividades relacionadas à segurança cibernética; e

II - elaborar as diretrizes, os dispositivos e os procedimentos de defesa que atuem nos sistemas relacionados à defesa nacional contra ataques cibernéticos.

~~**Seção III**~~
~~**Do Ministério da Transparência e Controladoria-Geral da União**~~

Seção III

Da Controladoria-Geral da União
(Redação dada pelo Decreto nº 10.641, de 2021)

~~Art. 14. Ao Ministério da Transparência e Controladoria-Geral da União compete auditar a execução das ações da Política Nacional de Segurança da Informação de responsabilidade dos órgãos e das entidades da administração pública federal.~~

Art. 14. Compete à Controladoria-Geral da União auditar a execução das ações da PNSI de responsabilidade dos órgãos e das entidades da administração pública federal. (Redação dada pelo Decreto nº 10.641, de 2021)

Seção IV

Dos órgãos e das entidades da administração pública federal

Art. 15. Aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete:

I - implementar a PNSI;

II - elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República;

III - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;

IV - instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI;

V - destinar recursos orçamentários para ações de segurança da informação;

VI - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

~~VII - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais, que comporá a rede de equipes formada pelos órgãos e entidades da administração pública federal, coordenada pelo Centro de Tratamento de Incidentes de Redes do Governo do Gabinete de Segurança Institucional da Presidência da República;~~

VII - instituir e implementar equipe de prevenção, tratamento e resposta a incidentes cibernéticos, que comporá a rede de equipes dos órgãos e das entidades da administração pública federal, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República; (Redação dada pelo Decreto nº 10.641, de 2021)

VIII - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

IX - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação; e

X - aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação.

§ 1º O comitê de segurança da informação interno de que trata o inciso IV do **caput** será composto por:

I - o gestor da segurança da informação do órgão ou da entidade, de que trata o inciso III do **caput** , que o coordenará;

II - um representante da Secretaria-Executiva ou da unidade equivalente do órgão ou da entidade;

III - um representante de cada unidade finalística do órgão ou da entidade; e

IV - o titular da unidade de tecnologia da informação e comunicação do órgão ou da entidade.

~~§ 2º Os membros do comitê de segurança da informação interno de que tratam os incisos II e III do § 1º deverão ocupar cargo em comissão do Grupo-Direção e Assessoramento Superiores, de nível 5 ou superior, ou equivalente.~~

~~§ 2º Os membros do comitê de segurança da informação interno de que tratam os incisos I a III do § 1º deverão ocupar cargo em comissão ou função de confiança de nível 5 ou superior do Grupo-Direção e Assessoramento Superiores ou equivalente.~~ ~~(Redação dada pelo Decreto nº 9.832, de 2019)~~ (Revogado pelo Decreto nº 10.641, de 2021)

§ 3º O comitê de segurança da informação interno dos órgãos e das entidades da administração pública federal tem as seguintes atribuições:

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 - propor alterações na política de segurança da informação interna; e

IV - propor normas internas relativas à segurança da informação.

§ 4º O gestor de segurança da informação será designado dentre os servidores públicos ocupantes de cargo efetivo, empregados públicos e militares do órgão ou da entidade, com formação ou capacitação técnica compatível com as normas estabelecidas por este Decreto. (Incluído pelo Decreto nº 10.641, de 2021)

Art. 16. Os órgãos e as entidades da administração pública federal editarão atos para definir a forma de funcionamento dos respectivos comitês de segurança da informação, observado o disposto neste Decreto e na legislação.

Art. 17. Compete à alta administração dos órgãos e das entidades da administração pública federal a governança da segurança da informação, e especialmente:

I - promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;

II - monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;

III - incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades;

IV - planejar a execução de programas, de projetos e de processos relativos à segurança da informação;

V - estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;

VI - observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

VII - implementar controles internos fundamentados na gestão de riscos da segurança da informação;

VIII - instituir um sistema de gestão de segurança da informação;

IX - implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados pelos órgãos da administração pública federal; e

X - observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidos neste Decreto e na legislação.

§ 1º O planejamento e a execução de programas, de projetos e de processos relativos à segurança da informação de que trata o inciso IV do **caput** serão orientados para:

I - a utilização de recursos criptográficos adequados aos graus de sigilo exigidos no tratamento das informações e as restrições de acesso estabelecidas para o compartilhamento das informações, observada a legislação;

II - o aumento da resiliência dos ativos de tecnologia da informação e comunicação e dos serviços definidos como estratégicos pelo Governo federal;

~~III - a contínua cooperação entre as equipes de resposta e de tratamento de incidentes de segurança na administração pública federal direta, autárquica e fundacional e o Centro de Tratamento de Incidentes de Redes do Governo do Gabinete de Segurança Institucional da Presidência da República; e~~

III - a contínua cooperação entre as equipes de prevenção, tratamento e resposta a incidentes cibernéticos na administração pública federal direta, autárquica e fundacional e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República; e (Redação dada pelo Decreto nº 10.641, de 2021)

IV - a priorização da interoperabilidade de tecnologias, processos, informações e dados, com a promoção:

a) da integração e do compartilhamento dos ativos de informação do Governo federal ou daqueles sob sua custódia;

b) da uniformização e da redução da fragmentação das bases de informação de interesse do Governo federal e da sociedade;

c) da integração e do compartilhamento das redes de telecomunicações da administração pública federal direta, autárquica e fundacional; e

d) da padronização da comunicação entre sistemas.

§ 2º O sistema de gestão de segurança da informação de que trata o inciso VIII do **caput** identificará as necessidades da organização quanto aos requisitos de segurança da informação e implementará o processo de gestão de riscos de segurança da informação.

~~Art. 18. Os órgãos e as entidades da administração pública federal direta, autárquica e fundacional, nos atos administrativos que envolvam ativos de tecnologia da informação, sem prejuízo dos demais dispositivos legais, incorporarão as normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República e os normativos de gestão de tecnologia da informação e comunicação e de segurança da informação do Ministério do Planejamento, Desenvolvimento e Gestão.~~

Art. 18. Os órgãos e as entidades da administração pública federal direta, autárquica e fundacional, nos atos administrativos que envolvam ativos de tecnologia da informação, sem prejuízo dos demais dispositivos legais, incorporarão as normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República. (Redação dada pelo Decreto nº 10.641, de 2021)

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 19. O Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República editará, no prazo de noventa dias, contado da data de publicação deste Decreto, glossário com a definição dos termos técnicos e operacionais relativos à segurança da informação, que será utilizado como referência conceitual para as normas e os regulamentos relacionados à segurança da informação.

Art. 20. O Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República poderá expedir atos complementares necessários à aplicação deste Decreto.

~~Art. 21. O Decreto nº 2.295, de 4 de agosto de 1997 , passa a vigorar com as seguintes alterações:~~ (Revogado pelo Decreto nº 10.631, de 2021)

~~"Art. 1º .....~~

~~.....~~

~~III - aquisição de equipamentos e contratação de serviços técnicos especializados para as áreas de inteligência, de segurança da informação, de segurança cibernética, de segurança das comunicações e de defesa cibernética.~~

~~....." (NR)~~

Art. 22. Ficam revogados:

I - o Decreto nº 3.505, de 13 de junho de 2000 ; e

II - o Decreto nº 8.135, de 4 de novembro de 2013 .

Art. 23. Este Decreto entra em vigor na data de sua publicação.

Brasília, 26 de dezembro de 2018; 197º da Independência e 130º da República.

MICHEL TEMER
Sergio Westphalen Etchegoyen

Este texto não substitui o publicado no DOU de 27.12.2018

*

Emitido em 26/12/2018

DECRETO Nº 1/2018 - SODS (11.01.21)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 24/02/2023 15:54)
GLEICIANNE DOURADO COSTA
SODS (11.01.21)
Matrícula: ###525#0

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1**, ano: **2018**, tipo: **DECRETO**, data de emissão: **24/02/2023** e o código de verificação: **e52061c8c6**

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 28/05/2020 | Edição: 101 | Seção: 1 | Página: 13

Órgão: Presidência da República/Gabinete de Segurança Institucional

INSTRUÇÃO NORMATIVA Nº 1, DE 27 DE MAIO DE 2020

Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA , no uso das atribuições que lhe conferem o art. 87 da Constituição, a Lei nº 13.844, de 18 de junho de 2019, e o Decreto nº 9.668, de 2 de janeiro de 2019, considerando o disposto no art. 12 do Decreto nº 9.637, de 26 de dezembro de 2018, e em cumprimento ao Decreto nº 10.139, de 28 de novembro de 2019 resolve:

Art. 1º Aprovar a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 2º A Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal dispõe sobre as orientações para gestão de segurança da informação que deverão ser observadas e implementadas pelos órgãos e pelas entidades da administração pública federal, direta e indireta, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional.

Art. 3º Para os fins do disposto nesta Instrução Normativa, a segurança da informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física;

IV - a proteção de dados organizacionais; e

V - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO II

DAS REFERÊNCIAS NORMATIVAS DE SEGURANÇA DA INFORMAÇÃO

Art. 4º Para o planejamento da gestão da segurança da informação, cabe aos órgãos e às entidades da administração pública federal observar, sem prejuízo das demais normas em vigor:

I - o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

II - a Resolução SE/GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação;

III - a Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

IV - o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; e

V - as instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

Seção I

Da Política Nacional de Segurança da Informação

Art. 5º Devem ser considerados no planejamento da gestão da segurança da informação os seguintes aspectos da Política Nacional de Segurança da Informação, instituída por meio do Decreto nº 9.637, de 2018:

I - a abrangência da segurança da informação;

II - os objetivos;

III - os instrumentos;

IV - a instituição e as competências do Comitê Gestor de Segurança da Informação;

V - as competências do Gabinete de Segurança Institucional da Presidência da República;

VI - as competências do Ministério da Defesa;

VII - as competências da Controladoria-Geral da União; e

VIII - as competências dos demais órgãos e das entidades da administração pública federal.

Seção II

Do Glossário de Segurança da Informação

Art. 6º Os órgãos e as entidades da administração pública federal deverão utilizar o Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI/PR nº 93, de 26 de setembro de 2019, como referência na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos.

Art. 7º O Glossário de Segurança da Informação, sempre que possível, será atualizado pelo Gabinete de Segurança Institucional da Presidência da República, devendo os órgãos e as entidades da administração pública federal enviar, a qualquer tempo, contribuições e sugestões para seu aperfeiçoamento.

Seção III

Da Estratégia Nacional de Segurança Cibernética

Art. 8º Devem ser considerados no planejamento da gestão da segurança da informação, em especial, os seguintes aspectos da Estratégia Nacional de Segurança Cibernética, aprovada pelo Decreto nº 10.222, de 2020:

I - os objetivos estratégicos; e

II - as ações estratégicas.

CAPÍTULO III

DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 9º É obrigatório a todos os órgãos e as entidades da administração pública federal possuir uma Política de Segurança da Informação, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

Parágrafo único. A autoridade máxima do órgão ou da entidade é responsável por garantir os recursos necessários para a execução da Política de Segurança da Informação no âmbito de sua organização.

Art. 10. A Política de Segurança da Informação deve ser elaborada sob a coordenação do Gestor de Segurança da Informação do órgão ou entidade, com a participação do Comitê de Segurança da Informação interno ou estrutura equivalente.

Parágrafo único. Cabe ao Gestor de Segurança da Informação promover, com apoio da alta administração, a ampla divulgação da Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, aos usuários e aos prestadores de serviço, a fim de que esses tomem conhecimento de tais instrumentos.

Art. 11. A elaboração da Política de Segurança da Informação deve levar em consideração a natureza e a finalidade do órgão ou da entidade e estar alinhada ao seu planejamento estratégico.

Art. 12. A Política de Segurança da Informação deverá ser composta, no mínimo, pelos seguintes itens:

I - escopo: descreve o objetivo e a abrangência da Política, definindo o limite dentro do qual as ações de segurança da informação serão desenvolvidas no órgão ou na entidade;

II - conceitos e definições: relaciona e descreve os conceitos e definições a serem utilizados na Política do órgão ou da entidade que possam gerar dificuldade de interpretação ou ambiguidade, devendo ser utilizadas as definições contidas no Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República;

III - princípios: relaciona os princípios que regem a segurança da informação no órgão ou na entidade;

IV - diretrizes gerais: estabelece diretrizes sobre a implementação, no mínimo, dos seguintes temas:

a) Tratamento da Informação;

b) Segurança Física e do Ambiente;

c) Gestão de Incidentes em Segurança da Informação;

d) Gestão de Ativos;

e) Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;

f) Controles de Acesso;

g) Gestão de Riscos;

h) Gestão de Continuidade; e

i) Auditoria e Conformidade.

V - competências: define as atribuições e as responsabilidades dos envolvidos na estrutura de gestão de segurança da informação;

VI - penalidades: estabelece as consequências e as penalidades para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre penalidades ao servidor público federal relativas ao assunto; e

VII - política de atualização: estabelece a periodicidade máxima para a revisão da Política de Segurança da Informação e dos respectivos instrumentos normativos.

§ 1º A periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos.

§ 2º A Política de Segurança da Informação, quando necessário, deve ser complementada por normas, metodologias e procedimentos.

Art. 13. A elaboração e a adoção de uma Política de Segurança da Informação interna evidenciam o comprometimento da alta administração com vistas a prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação em sua organização.

CAPÍTULO IV

DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA

Art. 14. Ao Gabinete de Segurança Institucional da Presidência da República compete a publicação de atos normativos sobre Segurança da Informação, que devem abordar os principais aspectos a serem observados no planejamento de ações relacionadas a esse tema no âmbito dos órgãos e das entidades da administração pública federal.

Parágrafo único. A adoção dos controles gerais de segurança da informação estabelecidos pelo Gabinete de Segurança Institucional da Presidência da República é de cumprimento obrigatório para a alta administração dos órgãos e das entidades da administração pública federal.

CAPÍTULO V

DOS ÓRGÃOS E DAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Art. 15. Além das obrigações já dispostas nesta Instrução Normativa, compete aos órgãos e às entidades da administração pública federal, direta e indireta, em seu âmbito de atuação:

I - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;

II - instituir Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação;

III - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

IV - instituir e implementar Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República;

V - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

VI - consolidar e analisar os resultados dos trabalhos de auditoria sobre gestão de segurança da informação; e

VII - aplicar as ações corretivas e administrativas cabíveis, nos casos de violação da segurança da informação.

CAPÍTULO VI

DA ESTRUTURA PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 16. De forma a estruturar a gestão da segurança da informação, os órgãos e entidades da administração pública federal deverão designar ou instituir, ao menos:

I - o Gestor de Segurança da Informação;

II - o Comitê de Segurança da Informação ou estrutura equivalente; e

III - uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente.

Art. 17. Os órgãos e as entidades da administração pública federal deverão utilizar os guias metodológicos que serão disponibilizados pelo Gabinete de Segurança Institucional da Presidência da República em seu sítio eletrônico, para fins de implementação de ações relacionadas à gestão da segurança da informação.

Seção I

Do Gestor de Segurança da Informação

Art. 18. O gestor de segurança da informação será designado dentre os servidores públicos civis ocupantes de cargo efetivo e militares de carreira do órgão ou entidade, com formação ou capacitação técnica compatível às suas atribuições.

Art. 19. Compete ao gestor de segurança da informação:

I - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a alta administração na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

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 ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de 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 Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Seção II

Do Comitê de Segurança da Informação

Art. 20. O Comitê de Segurança da Informação interno dos órgãos e das entidades da administração pública federal possui as seguintes atribuições:

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. 21. O Comitê de Segurança da Informação disposto no art. 20 terá a seguinte composição:

I - o gestor de segurança da informação do órgão ou da entidade, que o coordenará;

II - um representante da Secretaria-Executiva ou da unidade equivalente do órgão ou da entidade;

III - um representante de cada unidade finalística do órgão ou da entidade; e

IV - o titular da unidade de tecnologia da informação do órgão ou da entidade.

Seção III

Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Art. 22. Todos os órgãos e entidades que possuem a competência de administrar a infraestrutura de rede de sua organização deverão criar uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

§ 1º Deverá ser elaborado documento de constituição da Equipe de Tratamento e Resposta a Incidentes Cibernéticos, o qual designará suas atribuições e seu escopo de atuação.

§ 2º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe.

§ 3º A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo, sem prejuízo das demais metodologias e padrões conhecidos.

§ 4º As notificações enviadas pela Equipe ao Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo, bem como a troca de informações entre as Equipes existentes, devem seguir os formatos e os procedimentos que serão estabelecidos pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo.

CAPÍTULO VII

DOS ATOS DE DISPOSIÇÕES TRANSITÓRIAS

Art. 23. Ficam revogados os seguintes atos normativos:

I - a Instrução Normativa GSI Nº 1, de 13 de junho de 2008;

II - a Norma Complementar nº 01, de 13 de outubro de 2008;

III - a Norma Complementar nº 02, de 13 de outubro de 2008; e

IV - a Norma Complementar nº 03, de 30 de junho de 2009.

Parágrafo único. As referidas normas preservarão seus efeitos até a entrada em vigor desta Instrução Normativa.

Art. 24. Esta Instrução Normativa entra em vigor no dia 1º de julho de 2020.

AUGUSTO HELENO RIBEIRO PEREIRA

Emitido em 27/05/2020

INSTRUÇÃO NORMATIVA SODS/REITORIA Nº 10, DE 24 DE FEVEREIRO DE 2023

(Assinado digitalmente em 24/02/2023 15:54)
GLEICIANNE DOURADO COSTA
SODS (11.01.21)
Matrícula: ###525#0

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **10**, ano: **2020**, tipo: **INSTRUÇÃO NORMATIVA**, data de emissão: **24/02/2023** e o código de verificação: **cdd499b28f**

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
SECRETARIA DOS ÓRGÃOS DE DELIBERAÇÃO SUPERIOR

DESPACHO Nº 272/2023 - SODS (11.01.21)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 24 de fevereiro de 2023.

DESPACHO CGAG/CONSUNI/UFOB Nº 015/2023.

Processo 23520.001280/2023-02.

Prezado Professor Thiago Ribeiro Rafagnin,

Assessor

Cumprimentando-o cordialmente, encaminho processo referente à Proposta de Resolução que institui a Política de Segurança da Informação – PSI da Universidade Federal do Oeste da Bahia - UFOB, **para realização de Análise Técnica Legislativa e de Compatibilidade da proposta com o Estatuto, o Regimento Geral e demais normativas da UFOB, e com a legislação superior vigente, no prazo de 10 (dez) dias corridos, a contar de 27/02/2023**.

Após esse prazo, solicito a gentileza de encaminhar o documento de Análise Técnica Legislativa à Secretaria dos Órgãos de Deliberação Superior para os encaminhamentos pertinentes.

GLEICIANNE DOURADO COSTA

Secretária dos Órgãos de Deliberação Superior

(Assinado digitalmente em 24/02/2023 15:54)
GLEICIANNE DOURADO COSTA
SODS (11.01.21)
Matrícula: ###525#0

Processo Associado: 23520.001280/2023-02

, ano: **2023**, tipo: **DESPACHO**, data de emissão: **24/02/2023** e o código de verificação: **219a5a5c97**

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
SECRETARIA DOS ÓRGÃOS DE DELIBERAÇÃO SUPERIOR

DESPACHO FAVORÁVEL/DESFAVORÁVEL Nº 52/2023 - SODS (11.01.21)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 08 de março de 2023.

Em **08/03/2023**, solicito o Desentranhamento da(s) peça(s) listada(s) abaixo, do processo 23520.001280/2023-02, por motivo de **ajustes.**

Ordem: 10
Número: 321
Ano: 2023
Número de Protocolo: NÃO PROTOCOLADO
Tipo de Documento: DESPACHO

Documento não acessível publicamente

(Assinado digitalmente em 08/03/2023 10:04)
GLEICIANNE DOURADO COSTA
SODS (11.01.21)
Matrícula: ###525#0

Processo Associado: 23520.001280/2023-02

Visualize o documento original em https://sig.ufob.edu.br/public/documentos/index.jsp informando seu número: **52**, ano: **2023**, tipo: **DESPACHO FAVORÁVEL/DESFAVORÁVEL**, data de emissão: **08/03/2023** e o código de verificação: **5c17ee878b**

UFOB

Secretaria dos Órgãos de Deliberação Superior da UFOB <orgaossuperiores@ufob.edu.br>

Solicitação de prorrogação

Thiago Ribeiro Rafagnin <thiago.rafagnin@ufob.edu.br> 7 de março de 2023 às 14:39
Para: Secretaria dos Órgãos de Deliberação Superior da UFOB <orgaossuperiores@ufob.edu.br>

Estimada Secretária,

em tempo, solicito que a dilação de prazo seja de 15 dias.

Cordialmente,

Prof. Dr. Thiago R. Rafagnin
Universidade Federal do Oeste da Bahia

---------- Forwarded message ---------
De: **Thiago Ribeiro Rafagnin** <thiago.rafagnin@ufob.edu.br>
Date: seg., 6 de mar. de 2023 às 16:37
Subject: Solicitação de prorrogação
To: Secretaria dos Órgãos de Deliberação Superior da UFOB <orgaossuperiores@ufob.edu.br>

Estimada Secretária,

Por meio do presente, solicito a prorrogação, pelo período de 05 dias, para que possamos concluir as etapas finais relativas às candidaturas da sociedade civil para o CONSUNI.

Cordialmente,

Prof. Dr. Thiago R. Rafagnin
Universidade Federal do Oeste da Bahia

Emitido em 07/03/2023

SOLICITAÇÃO DE PRORROGAÇÃO DE PRAZO Nº 4/2023 - SODS (11.01.21)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 08/03/2023 10:07)
GLEICIANNE DOURADO COSTA
SODS (11.01.21)
Matrícula: ###525#0

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **4**, ano: **2023**, tipo: **SOLICITAÇÃO DE PRORROGAÇÃO DE PRAZO**, data de emissão: **08/03/2023** e o código de verificação: **20bb36b5f4**

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
SECRETARIA DOS ÓRGÃOS DE DELIBERAÇÃO SUPERIOR

DESPACHO FAVORÁVEL/DESFAVORÁVEL Nº 54/2023 - SODS (11.01.21)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 15 de março de 2023.

Em **15/03/2023**, solicito o Desentranhamento da(s) peça(s) listada(s) abaixo, do processo 23520.001280/2023-02, por motivo de **ajustes.**

Ordem: 13
Número: 322
Ano: 2023
Número de Protocolo: NÃO PROTOCOLADO
Tipo de Documento: DESPACHO

Documento não acessível publicamente

(Assinado digitalmente em 15/03/2023 11:56)
GLEICIANNE DOURADO COSTA
SODS (11.01.21)
Matrícula: ###525#0

Processo Associado: 23520.001280/2023-02

Visualize o documento original em https://sig.ufob.edu.br/public/documentos/index.jsp informando seu número: **54**, ano: **2023**, tipo: **DESPACHO FAVORÁVEL/DESFAVORÁVEL**, data de emissão: **15/03/2023** e o código de verificação: **e2bac464ff**

DESPACHO CGAG/CONSUNI/UFOB Nº 023/2023.

Processo 23520.001280/2023-02.

Prezado Professor Thiago Ribeiro Rafagnin,
Assessor

Atendendo à solicitação encaminhada através de e-mail enviado à Secretaria dos Órgãos de Deliberação Superior em 07/03/23, anexa, **prorrogo, por 10 (dez) dias, a contar de 09/03/23, o prazo** para que emita a **Análise Técnica Legislativa e de Compatibilidade** da Proposta de Resolução que institui a Política de Segurança da Informação – PSI da Universidade Federal do Oeste da Bahia – UFOB.

Após esse prazo, solicito a gentileza de encaminhar o documento de Análise Técnica Legislativa à Secretaria dos Órgãos de Deliberação Superior para os encaminhamentos pertinentes.

Barreiras, 08 de março de 2023.

GLEICIANNE DOURADO COSTA
Secretária dos Órgãos de Deliberação Superior
(despacho anexado ao processo e assinado digitalmente)

Emitido em 08/03/2023

DESPACHO Nº 328/2023 - SODS (11.01.21)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 15/03/2023 12:02)
GLEICIANNE DOURADO COSTA
SODS (11.01.21)
Matrícula: ###525#0

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **328**, ano: **2023**, tipo: **DESPACHO**, data de emissão: **15/03/2023** e o código de verificação: **3a52243ae2**

ANÁLISE TÉCNICA LEGISLATIVA

Instrução do Processo: COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Processo: 23520.001280/2023-02
Assunto: PROPOSTA DE RESOLUÇÃO PARA INSTITUIR A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Interessado: COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO / PRÓ-REITORIA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Responsável pela análise: THIAGO RIBEIRO RAFAGNIN

OBJETO DE APRECIAÇÃO

Trata-se de Análise Técnica Legislativa e de Compatibilidade de proposta de Resolução para dispor sobre a proposta de resolução para instituir a política de segurança da informação - PSI da Universidade Federal do Oeste da Bahia, com o Estatuto, o Regimento Geral e demais normativas da Universidade, e com a legislação superior vigente.

CONSIDERAÇÕES

Inicialmente há de se destacar que o objeto da presente análise está adstrito, tão somente, à técnica legislativa e compatibilidade normativa da proposta em face da legislação que trata da redação legislativa, sobretudo dos atos normativos inferiores a decreto, assim como Estatuto e Regimento Geral da UFOB, portanto, as considerações aqui emanadas não estão relacionadas ao mérito da proposta.

Nessa toada, salvo melhor juízo, verifico que há compatibilidade entre a proposição e as normas institucionais desta Universidade.

Passo, agora, à análise relacionada à técnica legislativa.

Na Lei Complementar nº 95/1998 encontra-se o conjunto de preceitos relacionados à técnica legislativa. Apesar desta nomenclatura remeter aos atos do Poder Legislativo, é fundamental ter-se em vista que o conjunto de técnicas (e princípios) legislativas aplicam-se a quaisquer atos normativos, sejam eles emanados de órgãos de quaisquer dos Poderes, assim como da administração direta, indireta, autárquica e fundacional.

É imprescindível que toda norma jurídica atenda, a priori, a cinco princípios: a) Integralidade; b) Irredutibilidade; c) Coerência; d) Correspondência; e) Realidade.

a) Integralidade: a norma não pode apresentar lacunas que possam trazer antinomias em relação à sua aplicação interna ou externa ao órgão;

b) Irredutibilidade: a norma tem de expressar apenas aquilo que se relaciona aos seus próprios fins;

c) Coerência: a norma deve ser coerente com os objetivos a que propõe;

d) Correspondência: a norma deve se coadunar com o ordenamento jurídico e, claro, que fazem parte do arcabouço jurídico do órgão, a fim de que haja harmonia;

e) Realidade: a norma deve levar em conta a realidade do órgão, inclusive econômica, jurídica e social.

Além disso, a estrutura, articulação, redação e formatação dos atos normativos inferiores a decreto deverão observar o estabelecido no Decreto nº 9.191 de 1º de novembro de 2017. Não obstante, é necessária observância do Decreto nº 10.139 de 28 de novembro de 2019 que dispõe sobre a revisão e a consolidação dos atos normativos inferiores a decreto.

No âmbito dos órgãos da administração pública federal, serão admitidas apenas "Portarias", "Resoluções" e "Instruções Normativas", sendo que tais atos deverão observar o disposto no art. 3º da Lei Complementar nº 95/98, sendo estruturados em três partes básicas:

a) parte preliminar, compreendendo a epígrafe, a ementa, o preâmbulo, o enunciado do objeto e a indicação do âmbito de aplicação das disposições normativas;

b) parte normativa, compreendendo o texto das normas de conteúdo substantivo relacionadas com a matéria regulada;

c) parte final, compreendendo as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo, às disposições transitórias, se for o caso, a cláusula de vigência e a cláusula de revogação, quando couber.

Diante disso, considerando o arcabouço legal mencionado, verifico que não há necessidade de ajuste formal na proposta como forma de se atender à técnica legislativa.

RESULTADO DA ANÁLISE

Diante das considerações apresentadas, encaminho a presente análise para a Secretaria dos Órgãos de Deliberação Superior, a fim de que se dê conhecimento ao conteúdo do presente, seguindo os devidos trâmites processuais para posterior deliberação do mérito da matéria.

Barreiras, 20 de março de 2023.

Thiago Ribeiro Rafagnin
Assessor da Reitoria
Responsável pela análise técnica legislativa

Emitido em 20/03/2023

ANÁLISE TÉCNICA LEGISLATIVA Nº 1/2023 - SODS (11.01.21)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 28/03/2023 12:14)
GLEICIANNE DOURADO COSTA
COORD.DE SECRETARIA SUPERIOR - TITULAR
SODS (11.01.21)
Matrícula: ###525#0

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1**, ano: **2023**, tipo: **ANÁLISE TÉCNICA LEGISLATIVA**, data de emissão: **28/03/2023** e o código de verificação: **9d45dd9769**