Serviço Público Federal

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

PROCESSO 23520.012816/2023-15

ELETRÔNICO

Cadastrado em 06/12/2023

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

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 BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS 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
07/12/2023	SECRETARIA DOS ÓRGÃOS DE DELIBERAÇÃO SUPERIOR (11.01.21)
19/12/2023	PRÓ-REITORIA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (11.01.06)
20/12/2023	COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (11.01.10.09)
01/02/2024	SECRETARIA DOS ÓRGÃOS DE DELIBERAÇÃO SUPERIOR (11.01.21)

Data	Destino

SIPAC | Pró-Reitoria de Tecnologia da Informação e Comunicação - (77) 3614-3560 @ | Copyright © 2005-2024 - UFRN - sipac.ufob.edu.br

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 À CGAG

Instrução do Processo: Comitê Gestor de Tecnologia da Informação e Comunicação
Processo: 23520.012816/2023-15
Assunto: Proposta de Política de Backup e Restauração de Dados Digitais 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 03, de 5 de abril de 2022

OBJETO DA PROPOSTA

Trata-se de proposta de Política de Backup e Restauração de Dados Digitais da Universidade Federal do Oeste da Bahia.

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, a universidade instituiu a Política de Segurança da Informação - PSI da UFOB, por meio da Resolução CGAG/CONSUNI/UFOB nº 018, de 24 de agosto de 2023. O art. 18 da Resolução dispõe que "a Universidade Federal do Oeste da Bahia garantirá condições adequadas de guarda e armazenamento das informações". Além disso, o art. 32 diz que as normas complementares deverão ser elaboradas em 24 (vinte e quatro) meses após a publicação da Resolução.

Neste contexto, o Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC) encaminha proposta de Política de Backup e Restauração de Dados Digitais, uma norma complementar ao PSI com o objetivo de instituir diretrizes e responsabilidades em relação à segurança, proteção e disponibilidade dos dados digitais custodiados pela UFOB.

JUSTIFICATIVAS

Considerando a necessidade de elaborar normas complementares que permitam auxiliar a implantação da Política de Segurança da Informação na universidade, o CGTIC instituiu Comissão, por meio da Portaria CGTIC/UFOB nº 03, de 5 de abril de 2022, para a elaboração da proposta da Política de Backup e Restauração de Dados Digitais. O documento foi apreciado em reunião ordinária do Comitê, em 25 de setembro de 2023, e aprovado por unanimidade.

DESCRIÇÃO

O objetivo da política é definir as diretrizes básicas para o gerenciamento de backups e restaurações de dados digitais, além de atribuir responsabilidades aos setores e/ou pessoas competentes.

O documento é estruturado em 8 (oito) capítulos, a saber:

I – Disposições Preliminares;

II – Do Backup;

III – Do Transporte e Armazenamento;

IV– Da Restauração;

V – Dos Testes de Backup;

VI – Do Descarte de Mídia;

VII – Das Responsabilidades;

VIII – Das Disposições Finais.

CONSIDERAÇÕES FINAIS

Considerando as atribuições do CGTIC, encaminho a Proposta de Política de Backup e Restauração de Dados Digitais da Universidade Federal do Oeste da Bahia para ser apreciada pela Câmara de Gestão Administrativa e Governança (CGAG).

Barreiras, 6 de dezembro de 2023.

Vanessa Godoy Kinoshita

Presidente do Comitê Gestor de Tecnologia da Informação e Comunicação

RELATÓRIO DE PROPOSIÇÃO À CGAG Nº 2/2023 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 07/12/2023 09:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***2****, ano:* ***2023****, tipo:* ***RELATÓRIO DE PROPOSIÇÃO À CGAG****, data de emissão:* ***07/12/2023*** *e o código de verificação:* ***6c3b3b48ce***

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

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

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

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

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

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I - a segurança cibernética;

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

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

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

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

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

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

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

CAPÍTULO II
DOS PRINCÍPIOS

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

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

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

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

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

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

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

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

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

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

CAPÍTULO III
DAS DIRETRIZES GERAIS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO IV
DAS COMPETÊNCIAS E RESPONSABILIDADES

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

I - Comitê Permanente de Segurança da Informação;

II - Gestor de Segurança da Informação;

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

IV - Usuários; e

V - Gestores de órgãos, núcleos e unidades.

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

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

I - assessorar a implementação das ações de segurança da informação;

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

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

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

V - deliberar sobre normas internas de segurança da informação.

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

I - promover a cultura de segurança da informação;

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

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

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

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

LERIANE SILVA CARDOZO
Presidente da Câmara de Gestão Administrativa e Governança

JACQUES ANTONIO DE MIRANDA
Presidente do Conselho Universitário

RESOLUÇÃO CGAG Nº 1/2023 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 07/12/2023 09:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2023****, tipo:* ***RESOLUÇÃO CGAG****, data de emissão:* ***07/12/2023*** *e o código de verificação:* ***3ba09b4043***

PORTARIA CGTIC/UFOB Nº 03, DE 05 DE ABRIL DE 2022

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 INSTITUIR comissão para elaborar a Política de Backup e Restauração de Dados Digitais da Universidade Federal do Oeste da Bahia.

Art. 2º DESIGNAR Luiz Hilário Ferreira Damascena (SIAPE 1880542), Cleyton Martins Sena (SIAPE 2280515) e Elivelton de Oliveira Santos (SIAPE 3216178), sob presidência do primeiro, para comporem a comissão.

Art. 3º ESTABELECER o prazo de 60 (sessenta) dias, a contar de 11/04/2022, para a conclusão dos trabalhos da referida comissão.

Art. 4º Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviços da UFOB.

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

PORTARIA Nº 1/2023 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 07/12/2023 09:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2023****, tipo:* ***PORTARIA****, data de emissão:* ***07/12/2023*** *e o código de verificação:* ***6803119b88***

RESOLUÇÃO CGAG/CONSUNI/UFOB Nº xxx, DE xx DE xxxx DE 2022.

Estabelece a Política de Backup e Restauração de Dados Digitais 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 Resolução Consuni nº 007/2018, de 9 de novembro de 2018, que estabelece as normas de uso de recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito da Universidade Federal do Oeste da Bahia,

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, e suas alterações, que institui a Política Nacional de Segurança da Informação e toma outras providências,

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD),

CONSIDERANDO a Norma Técnica ABNT NBR ISO/IEC 27001:2013, que provê um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI),

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27002:2013, utilizada como referência na seleção de controles dentro do processo de implementação de um Sistema de Gestão da Segurança da Informação (SGSI),

CONSIDERANDO a deliberação extraída da sua xxª Reunião xxxxrdinária, realizada em xx de xxxx de 2022, RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução institui a Política de **Backup** e Restauração de Dados Digitais no âmbito da Universidade Federal do Oeste da Bahia - UFOB, que compreende as diretrizes e responsabilidades visando a segurança, proteção e disponibilidade dos dados digitais custodiados pela universidade.

Art. 2º Para os fins previstos nesta Resolução, entende-se por:

I – arquivos em nuvem – método de armazenamento que permite aos serviços e aplicativos acessarem os dados por meio de sistemas de arquivos compartilhados pela **internet**;

II – **backup** – conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

III - **backup** completo - procedimento que faz uma cópia integral de dados dos sistemas de informação;

IV - **backup** diferencial - procedimento que compara o conteúdo armazenado no último **backup** completo e copia todas as alterações realizadas.

V - **backup** incremental - procedimento que salva os dados modificados ou criados desde o último **backup** (seja completo, diferencial ou incremental).

VI - mídia - mecanismo em que dados podem ser armazenados, podendo ser discos ópticos, magnéticos, CDs, fitas e papel, entre outros.

VII - serviços em nuvem - infraestrutura, plataformas ou sistemas hospedados por fornecedores terceirizados fora das dependências da contratante e disponibilizados aos usuários via **internet**.

Art. 3º Não serão salvaguardados nem restaurados dados armazenados em sistemas de armazenamento individuais de arquivos em nuvem, tais como **Google Drive**, **Microsoft OneDrive** ou qualquer tipo da mesma natureza, bem como dados armazenados localmente nos microcomputadores ou em quaisquer outros dispositivos utilizados por usuários.

Art. 4º A salvaguarda dos dados digitais pertencentes a serviços de tecnologia da informação e comunicação (TIC) da UFOB mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deverá estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Art. 5º Os **backups** e as restaurações deverão utilizar soluções próprias e especializadas preferencialmente realizadas de forma automatizada.

CAPÍTULO II

DO BACKUP

Art. 6º Os **backups** dos serviços de TIC deverão ser realizados utilizando-se as seguintes frequências temporais: diária, semanal e mensal.

Art. 7º Os tipos de **backups** que poderão ser realizados são: completo, incremental ou diferencial.

Art. 8º Os procedimentos e os instrumentos necessários aos **backup** deverão ser descritos detalhadamente no Plano de **Backup** e Restauração de Dados Digitais, que conterá, no mínimo, os seguintes itens:

I – abrangência/escopo dos **backups** (ou seja, aquilo que deve ser copiado, incluindo indicações de datas e períodos);

II – documentação e registro das tarefas de **backup**, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança;

III – documentação sobre os procedimentos para realizar a restauração;

IV - frequência de realização dos **backups;**

V - os tipos de **backups** a serem realizados;

VI - o tempo de retenção;

VII - requisitos específicos de segurança informação;

VIII - unidades de armazenamento; e

IX - locais de armazenamento.

CAPÍTULO III

DO TRANSPORTE E ARMAZENAMENTO

Art. 9º As unidades de armazenamento e salvaguarda dos dados digitais deverão considerar as seguintes características:

I – a criticidade do dado salvaguardado;

II – o tempo de retenção do dado;

III – a probabilidade de necessidade de restauração;

IV – o tempo esperado para restauração;
V – o custo de aquisição da unidade de armazenamento de **backup**; e

VI – a vida útil da unidade de armazenamento de **backup**.

Art. 10. As unidades de armazenamento de **backups** deverão ser devidamente identificadas e acondicionadas em locais apropriados, tendo como critério mínimo o controle de fatores ambientais sensíveis tais como umidade e temperatura.

Art. 11. Os locais de armazenamento dos **backups** deverão possuir acesso restrito às pessoas autorizadas somente pelos administradores de **backup**.

CAPÍTULO IV

DA RESTAURAÇÃO

Art. 12. A restauração de dados não será realizada em caso de perdas posteriores à conclusão do último **backup** válido.

Art. 13. As solicitações de restauração de dados deverão ser realizadas pelos responsáveis diretos dos arquivos ou sistemas e encaminhados via abertura de chamados.

Parágrafo único. Caso a restauração de dados possa ser realizada, o local para acesso dos arquivos ou sistemas deverá ser indicado pelo responsável pelo procedimento.

CAPÍTULO V

DOS TESTES DE BACKUP

Art. 14. Os **backups** serão verificados periodicamente a fim de garantir a integridade dos dados salvaguardados.

Art. 15. Quando problemas de **backup** são identificados durante os testes, ações corretivas devem ser tomadas para reduzir os riscos associados a **backups** com falha.

Art. 16. Os testes deverão ser realizados em todos os **backups** produzidos dos sistemas computacionais.

Art. 17. Os registros dos testes realizados deverão ser documentados para demonstrar conformidade com esta Política e para fins de auditoria.

Parágrafo único. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do **backup** e se o procedimento foi concluído com sucesso.

CAPÍTULO VI

DO DESCARTE DE MÍDIA

Art. 18. O descarte de mídias de **backup** deverá garantir que:

I – a mídia não contenha mais imagens de **backups** ativas e que o seu conteúdo não possa ser lido ou recuperado por terceiros não autorizados; e

II – as mídias sejam destruídas previamente.

CAPÍTULO VII

DAS RESPONSABILIDADES

Art. 19. O gerenciamento do **backup** e restauração dos sistemas e respectivas bases de dados custodiados pela universidade ficam a cargo dos administradores de **backup**.

Parágrafo único. Os administradores de **backup** serão designados entre os servidores do Órgão Gestor de Tecnologia da Informação e Comunicação.

Art. 20. Compete aos administradores de **backup:**

I – elaborar e revisar o Plano de **Backup** e Restauração de Dados Digitais;

II – propor soluções de **backup** dos dados digitais produzidas ou custodiadas pela organização;

III – providenciar a criação e manutenção dos **backups**;

IV – configurar as soluções de **backup**;

V – zelar pelo funcionamento das unidades de armazenamento, equipamentos e soluções que executem as tarefas de **backup** e restauração;

VI – coordenar os testes de **backup**, sempre que necessário;

VII – realizar procedimentos de restauração;

VIII – atender às solicitações de restauração de dados que estão sob sua responsabilidade;

IX – zelar pelo cumprimento dos procedimentos estabelecidos no Plano de **Backup** e Restauração de Dados Digitais; e

X - realizar a comunicação sobre o Plano de **Backup** e Restauração de Dados Digitais às partes interessadas.

Art. 21. Administração Central ficará responsável por:

I – fornecer meios tecnológicos adequados para o funcionamento das soluções de **backup** e restauração definidas pelos administradores; e

II – promover formas de capacitação aos administradores nas tecnologias e recursos envolvidos.

Art. 22. O Órgão Gestor de Tecnologia da Informação e Comunicação, em conjunto com o Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC), deverá zelar pelo cumprimento das diretrizes, bem como notificar o usuário e/ou sua chefia imediata ou conforme o caso, de eventuais infrações provenientes do descumprimento desta Política.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 23. Os casos omissos serão resolvidos pelo CGTIC.

Art. 24. Esta Resolução entrará em vigor em XX de XXXX de 2022.

LERIANE SILVA CARDOZO

Presidente da Câmara de Gestão Administrativa e Governança

PROPOSTA DE RESOLUÇÃO Nº 2/2023 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 07/12/2023 09:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***2****, ano:* ***2023****, tipo:* ***PROPOSTA DE RESOLUÇÃO****, data de emissão:* ***07/12/2023*** *e o código de verificação:* ***c753e80541***

ATO DECISÓRIO CGTIC/UFOB Nº 01, DE 25 DE SETEMBRO DE 2023

O COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – CGTIC, no uso das atribuições legais, e

Considerando a deliberação extraída da **1ª Reunião Ordinária de 2023, realizada em 25 de setembro de 2023**, decide:

Art. 1º Aprovar a Política de Backup e Restauração de Dados da UFOB.

Art. 2º Este Ato Decisório entra em vigor a contar de 25 de setembro de 2023, justificado pela necessidade de atendimento ao princípio da continuidade do serviço público.

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

ATO DECISÓRIO Nº 1/2023 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 07/12/2023 09:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2023****, tipo:* ***ATO DECISÓRIO****, data de emissão:* ***07/12/2023*** *e o código de verificação:* ***2ccb56549f***

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

DESPACHO Nº 3/2023 - CGTIC (11.01.10.09)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 07 de dezembro de 2023.

Encaminha-se Proposta de Resolução para ser apreciada pela CGAG.
Coloco-me à disposição para esclarecimentos.

Atenciosamente,

(Assinado digitalmente em 07/12/2023 09:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Processo Associado: 23520.012816/2023-15

Visualize o documento original em https://sig.ufob.edu.br/public/documentos/index.jsp informando seu número: **3**, ano: **2023**, tipo: **DESPACHO**, data de emissão: **07/12/2023** e o código de verificação: **e3308e2034**

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

DESPACHO Nº 614/2023 - SODS (11.01.21)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 19 de dezembro de 2023.

DESPACHO CGAG/CONSUNI/UFOB Nº 056/2023.

Processo 23520.012816/2023-15.

Prezada Sra. Vanessa Godoy Kinoshita,

Presidente do CGTIC

Cumprimentando-a cordialmente, após análise do referido processo, que trata da Avaliação da Proposta de Resolução que Estabelece a Política de Backup e Restauração de Dados Digitais da Universidade Federal do Oeste da Bahia – UFOB, encaminhada pelo Comitê Gestor de Tecnologia da Informação e Comunicação – CGTIC, foi identificada a necessidade de inclusão de documentos para sanar pendências e dar melhor suporte à avaliação pela Câmara de Gestão Administrativa e Governança - CGAG: Inserir no processo a legislação (interna e externa) que dá amparo à proposição (Leis, Decretos, Resoluções e outros atos normativos inferiores aos citados).

Após atendimento à indicação, solicito a gentileza de encaminhar o processo à Secretaria dos Órgãos de Deliberação Superior para as providências quanto à apreciação pela Câmara de Gestão Administrativa e Governança - CGAG.

GLEICIANNE DOURADO COSTA

Secretária dos Órgãos de Deliberação Superior

(Assinado digitalmente em 19/12/2023 18:36)
GLEICIANNE DOURADO COSTA
COORD.DE SECRETARIA SUPERIOR - TITULAR
SODS (11.01.21)
Matrícula: ###525#0

Processo Associado: 23520.012816/2023-15

, ano: **2023**, tipo: **DESPACHO**, data de emissão: **19/12/2023** e o código de verificação: **4391f35c1c**

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;~~ (Revogado pelo Decreto nº 11.856, de 2023)

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;~~ (Revogado pelo Decreto nº 11.856, de 2023)

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

*

DECRETO Nº 1/2024 - CGTIC (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 01/02/2024 10:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2024****, tipo:* ***DECRETO****, data de emissão:* ***01/02/2024*** *e o código de verificação:* ***af6f9f5e73***

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

DESPACHO Nº 1/2024 - CGTIC (11.01.10.09)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 01 de fevereiro de 2024.

Sra. Gleicianne Dourado Costa

Secretária dos Órgãos de Deliberação Superior

Cumprimentando-a cordialmente, encaminho a Proposta de Resolução para ser apreciada pela CGAG, com a legislação anexada.
Coloco-me à disposição para esclarecimentos.

Atenciosamente,

(Assinado digitalmente em 01/02/2024 10:49)
VANESSA GODOY KINOSHITA
ANALISTA DE TEC DA INFORMACAO
NPTIC (11.01.06.02.01)
Matrícula: ###757#8

Processo Associado: 23520.012816/2023-15

Visualize o documento original em https://sig.ufob.edu.br/public/documentos/index.jsp informando seu número: **1**, ano: **2024**, tipo: **DESPACHO**, data de emissão: **01/02/2024** e o código de verificação: **fb5044c369**