Serviço Público Federal

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

PROCESSO 23520.011101/2024-18

ELETRÔNICO

Cadastrado em 12/11/2024

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		11011009
COMITÊ PERMANENTE DE SEGURANÇA DA INFORMAÇÃO		11011014
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 QUE INSTITUI POLÍTICA DE GESTÃO DE ATIVOS DE INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA UFOB.

Unidade de Origem:
PRÓ-REITORIA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (11.01.06)

Criado Por:
UILIAM RANGEL AMORIM SOUZA

Observação:

MOVIMENTAÇÕES ASSOCIADAS

Data	Destino
12/11/2024	PRÓ-REITORIA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (11.01.06)
12/11/2024	COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (11.01.10.09)
12/11/2024	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 À CGAG

Instrução do Processo: Comitê Gestor de Tecnologia da Informação e Comunicação
Processo: 23520.011101/2024-18
Assunto: Proposta de Política de Gestão de Ativos de Informação da Universidade Federal do Oeste da Bahia
Interessado: Comitê Gestor de Tecnologia da Informação e Comunicação; Comitê Permanente de Segurança da Informação; e Pró-Reitoria de Tecnologia da Informação e Comunicação.
Proponente: Comitê Gestor de Tecnologia da Informação;
Documento de designação: PORTARIA CGTIC/UFOB Nº 02, DE 05 DE ABRIL DE 2022

OBJETO DA PROPOSTA

Trata-se de proposta de Política de Gestão de Ativos de Informação da Universidade Federal do Oeste da Bahia.

CONSIDERAÇÕES

A Universidade Federal do Oeste da Bahia (UFOB), em conformidade com o Decreto nº 9.637/2018, que estabelece a Política Nacional de Segurança da Informação e impõe a necessidade de governança e normas internas de segurança da informação, criou sua própria Política de Segurança da Informação (PSI) pela Resolução CGAG/CONSUNI/UFOB nº 018, de 24 de agosto de 2023.

O art. 32 da PSI destaca a gestão de ativos como uma norma complementar obrigatória, determinando que as normas associadas à gestão de ativos sejam desenvolvidas e aprovadas no prazo de até 24 meses a partir da publicação da Resolução. Atendendo a essa exigência, o Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC) propõe a Política de Gestão de Ativos de Informação, que visa estabelecer diretrizes e responsabilidades para todo o processo do Ciclo de vida desses ativos no âmbito da UFOB, desde a aquisição, a identificação, o rastreamento, a manutenção e o descarte adequados. Essa norma complementar reforça o compromisso da universidade em assegurar a segurança da

informação e a proteção de dados pessoais, por meio de um controle efetivo de seus ativos de informação, em alinhamento com as exigências governamentais.

JUSTIFICATIVAS

Considerando a necessidade de inventariar os ativos de tecnologia da informação e comunicação (TIC) da Universidade Federal do Oeste da Bahia, o CGTIC instituiu Comissão, por meio da Portaria CGTIC/UFOB nº 02, de 5 de abril de 2022, para a execução desta atividade e complementarmente, foi também produto do trabalho desta comissão as estregas do processo e o normativo, objeto da proposta da Política de Ativos de Informação. O documento foi apreciado em reunião ordinária do Comitê, em 21 de maio de 2024, e aprovado por unanimidade.

DESCRIÇÃO

O objetivo da política é definir os princípios, objetivos, diretrizes e responsabilidades inerentes aos procedimentos durante o ciclo de vida dos ativos de informação.

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

I – DISPOSIÇÕES PRELIMINARES;

II – DOS PRINCÍPIOS, OBJETIVOS E DIRETRIZES;

III – DA GESTÃO DE ATIVOS DE INFORMAÇÃO;

IV– DAS RESPONSABILIDADES E OBRIGAÇÕES; e

V – DAS DISPOSIÇÕES FINAIS;

CONSIDERAÇÕES FINAIS

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

Barreiras, 12 de novembro de 2024.

Uiliam Rangel Amorim Souza

Presidente do Comitê Gestor de Tecnologia da Informação e Comunicação

RELATÓRIO DE PROPOSIÇÃO À CGAG Nº 1/2024 - null (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/11/2024 18:47)
UILIAM RANGEL AMORIM SOUZA
PRO-REITOR(A)
PROTIC (11.01.06)
Matrícula: ###746#9

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2024****, tipo:* ***RELATÓRIO DE PROPOSIÇÃO À CGAG****, data de emissão:* ***12/11/2024*** *e o código de verificação:* ***731e3de9c2***

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA

Conselho Superior

Câmara de Gestão Administrativa e Governança

RESOLUÇÃO CGAG/CONSUNI/UFOB nº 0XX, DE XX DE XXXX DE 2024

Institui a Política de Gestão de Ativos de Informação 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 xxª Reunião Ordinária/Extraordinária, realizada no dia xx de xxxx de xxxx,

CONSIDERANDO a Resolução CONSUNI/UFOB nº 07, de 09 de novembro de 2018, que dispõe sobre as normas de uso de recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito da Universidade Federal do Oeste da Bahia, e

CONSIDERANDO a Resolução CGAG/CONSUNI/UFOB nº 018, de 24 de agosto de 2023, que institui a Política de Segurança da Informação – PSI da Universidade Federal do Oeste da Bahia – UFOB, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução institui a Política de Gestão de Ativos de Informaçãoda Universidade Federal do Oeste da Bahia (UFOB), que compreende princípios, objetivos, diretrizes e responsabilidades dos procedimentos de inventário de bens, mapeamento de processos, monitoramento, descarte e desfazimento dos ativos de informação.

Art. 2º Esta política se estende a todas as unidades administrativas e acadêmicas, em todos os níveis de gestão (estratégico, tático e operacional), nos processos e projetos organizacionais, no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e nos normativos da instituição.

SEÇÃO I

Dos termos e definições

Art. 3º Para os efeitos desta política, considera-se:

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

I. Ativos de Informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

II. *Backup*: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.

III. Ciclo de vida de ativo de informação: período compreendido entre o planejamento, a aquisição/contratação e a disponibilização do ativo e o seu descarte ou desfazimento.

IV. Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

V. *Datacenter* (Centro de dados): consiste em uma estrutura, ou grupo de estruturas, dedicada à acomodação centralizada, interconexão e operação dos equipamentos de tecnologia da informação e redes de telecomunicações que fornecem serviços de armazenamento, processamento e transporte de dados.

VI. Disponibilidade: capacidade de um sistema, serviço ou recurso estar acessível e operacional quando necessário.

VII. Gestão de riscos de segurança da informação e comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos.

VIII. *Hardware*: equipamentos que compõem os recursos físicos de tecnologia e de informática, como computadores, mídias removíveis, equipamentos de conectividade, entre outros, conforme a legislação vigente;

IX. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

X. Inventário: coleção de ativos nomeados e classificados, com informações que permitam identificar de forma inequívoca cada item.

XI. Mapeamento de processos: técnica usada para mapear visualmente os fluxos de trabalho e os processos. Ela envolve a criação de um mapa de processo, também chamado de fluxograma, fluxograma de processo ou diagrama do fluxo de trabalho.

XII. Nível de criticidade: indica o impacto que o comprometimento de um componente, sistema ou serviço pode ter nos dados, finanças e atividades da instituição.

XIII. Nuvem: é um modelo para permitir que o provisionamento de recursos e serviços possam ser realizados de qualquer lugar e a qualquer momento, com acesso por meio de rede a recursos computacionais.

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

XIV. Órgão Gestor de TIC: unidade organizacional responsável por gerenciar e orientar o bom uso dos ativos de informação durante seu ciclo de vida.

XV. Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

XVI. *Software*: programas, sistemas, ferramentas e utilitários que realizam processamento, armazenamento, comunicação e outras operações em computadores e permitem a interação com o usuário.

XVII. Usuário: qualquer pessoa física, devidamente autorizada, que utiliza os sistemas de informação ou a infraestrutura de TIC da UFOB.

CAPÍTULO II

DOS PRINCÍPIOS, OBJETIVOS E DIRETRIZES

Seção I

Dos princípios

Art. 4º A gestão de ativos de informação da UFOB tem como princípios:

I. alinhamento estratégico, devendo ser considerados, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da instituição;

II. alinhamento com a Política de Segurança da Informação (PSI) da UFOB;

III. utilização do mapeamento de processos para apoio à tomada de decisão e à elaboração do planejamento estratégico;

IV. utilização da gestão de ativos de informação para apoio à melhoria contínua dos processos organizacionais;

V. atuação resiliente, devendo ser assegurada a otimização dos ativos de informação e uso dos recursos de forma equilibrada, mantendo a operação dos sistemas e tecnologias da informação e comunicação críticos de forma ininterrupta; e

VI. atuação com eficiência, devendo subsidiar a instituição a conhecer, valorizar, proteger e manter seus ativos de informação, em conformidade com os requisitos legais e do negócio.

Parágrafo único. Serão observados ainda, sem prejuízo dos demais, outros princípios constitucionais que regem a Administração Pública Federal.

Seção II

Dos objetivos

Art. 5º A gestão de ativos de informação da UFOB tem como objetivos:

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

I. manter a segurança de continuidade de negócios da UFOB;

II. prover o órgão de um entendimento comum, consistente e inequívoco de seus ativos de informação, da identificação clara de seus responsáveis e de um conjunto de informações básicas de segurança da informação e comunicação;

III. orientar e fornecer as diretrizes básicas para o planejamento, desenvolvimento, gestão e uso dos ativos de informação, em conformidade com as boas práticas recomendadas pelos órgãos de planejamento e de controle da Administração Pública Federal;

IV. fornecer orientações para o gerenciamento do ciclo de vida dos ativos de informação;

V. definir as responsabilidades nos processos relativos à gestão de ativos de informação;

VI. assegurar a utilização e execução de ativos estritamente autorizados; e

VII. garantir a disponibilidade e a integridade da informação gerada ou mantida pelos ativos de informação em uso.

Seção III

Das diretrizes

Art. 6º A gestão de ativos de informação da UFOB tem como diretrizes:

I. os equipamentos que vierem a ser adquiridos devem ser de fácil utilização, reduzindo a necessidade de capacitação dos usuários e da equipe de suporte, aumentando a efetividade do uso dos ativos de informação;

II. as rotinas de inventário de ativos de informação devem ser orientadas para a identificação dos ativos da organização, a fim de manter seu escopo devidamente identificado e documentado; e

III. processo dinâmico, periódico e estruturado de gestão de ativos de informação, para manter sua base de registros atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de gestão.

CAPÍTULO III

DA GESTÃO DE ATIVOS DE INFORMAÇÃO

Seção I

Do ciclo de vida dos ativos de informação

Art. 7º Os ativos de informação devem ser identificados, inventariados e monitorados durante todo o seu ciclo de vida.

Art. 8º O ciclo de vida dos ativos de informação compreende as seguintes etapas:

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

I. planejamento: fase que compreende a revisão dos ativos de informação que já estão em uso e a análise da necessidade e do custo de novas aquisições, alinhada ao planejamento estratégico institucional;

II. contratação: é a definição do padrão técnico que será utilizado, seleção de fornecedores, contratações e estabelecimento de acordos contratuais;

III. implantação: fase do cadastramento no sistema de controle aplicável, configuração/instalação e disponibilização dos ativos de informação para os usuários, conforme padrões estabelecidos;

IV. gerenciamento: é a fase de controle ou inventário automatizado, com manutenção, atualização, monitoramento e suporte técnico dos ativos de informação e manutenção dos registros dos ativos e fornecimento de informações de acompanhamento, controle e auditoria, sob demanda;

V. descarte: é o processo realizado quando um ativo torna-se antieconômico e perde sua utilidade, ou seja, material inservível, obsoleto ou excedente; e

VI. desfazimento: é o processo de exclusão de um bem do acervo patrimonial da instituição.

Seção II

Do planejamento e contratação dos ativos de informação

Art. 9º A contratação de ativos de informação só poderá ser realizada mediante planejamento prévio por meio do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) vigente e do Plano Anual de Contratações.

Parágrafo único. A estratégia de sustentação e provimento da infraestrutura computacional deverá ser definida pelo Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC) da instituição.

Art. 10. A padronização dos ativos de informação deve ser estabelecida pelo Órgão Gestor de TIC, visando a contratação e distribuição alinhadas aos interesses da instituição, observando-se o princípio da economicidade.

Seção III

Da implantação dos ativos de informação

Art. 11. Para cada ativo físico identificado, deve ser designado o respectivo responsável antes da implantação definitiva.

Art. 12. Os ativos físicos adquiridos só poderão ser disponibilizados ao responsável após realização dos procedimentos de homologação e configuração pré-estabelecidos pelo Órgão Gestor de TIC.

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

Seção IV

Do gerenciamento dos ativos de informação

Art. 13. Os ativos de informação devem ser utilizados estritamente para fins institucionais, no contexto de um processo de gestão estabelecido e documentado, a fim de garantir que sejam gerenciados e monitorados.

Art. 14. Os ativos de informação devem ser monitorados para garantir seu funcionamento adequado e fornecer informações para o gerenciamento de capacidade e demanda, para remanejamento e descarte.

Art. 15. A atualização de equipamentos e de soluções de infraestrutura observará a garantia contratada, conforme legislação vigente, a vida útil do equipamento, a projeção da evolução da demanda, os custos e os benefícios envolvidos.

Art. 16. O registro dos ativos de informação deve compreender as seguintes informações, quando aplicáveis:

I. tipo de ativo;

II. nome/número do modelo;

III. nome da marca;

IV. número do tombo;

V. número de série;

VI. data de instalação;

VII. número da versão;

VIII. nome do(a) servidor(a) responsável pelo ativo;

IX. localização (*campus*, prédio e sala);

X. as interdependências/conexões entre ativos, quando houver;

XI. endereço físico (controle de acesso à mídia (MAC));

XII. endereço de protocolo de internet (IP);

XIII. data de aquisição e de recebimento; e

XIV. prazo de garantia e/ou suporte contratado.

Parágrafo único. A coleta de dados dos ativos de informação, quando couber, deve ser realizada de forma automatizada.

Subseção I

Do inventário de ativos de informação

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

Art. 17. O processo de inventário dos ativos de informação deve conter, no mínimo, as seguintes ações:

I. informar aos usuários antecipadamente, indicando as datas e locais onde o inventário será realizado;

II. coletar as informações dos ativos, conforme descrito no Art. 16;

III. padronizar equipamentos que possuam configurações divergentes da orientação dada pelo Órgão Gestor de TIC;

IV. atualizar os equipamentos que estejam com o sistema operacional defasado;

V. inserir/atualizar as informações dos equipamentos inventariados em sistema informatizado adotado pelo Órgão Gestor de TIC; e

VI. classificar os ativos de informação conforme o nível de criticidade.

Art. 18. O processo de inventário deve coletar periodicamente informações de todos os *softwares* existentes na rede, realizando o registro, rastreamento e correção para que apenas *softwares* autorizados sejam instalados e executados, enquanto qualquer *software* não autorizado ou que viole direitos autorais, propriedade intelectual ou legislações vigentes seja identificado e removido.

Art. 19. O inventário dos ativos de informação deve ser realizado conforme frequência definida pela legislação vigente.

Subseção II

Do mapeamento dos processos da gestão de ativos de informação

Art. 20. Os processos relacionados à gestão de ativos de informação devem ser mapeados e compreender, no mínimo, os seguintes itens:

I. recebimento de materiais e equipamentos de TIC;

II. empréstimo de equipamentos de TIC;

III. devolução de equipamentos de TIC;

IV. inventário de TIC;

V. monitoramento dos ativos de informação; e

VI. desfazimento dos ativos de informação.

Parágrafo único. O mapeamento de processos deve estar alinhado à metodologia vigente na instituição.

Subseção II

Da manutenção dos ativos de informação

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

Art. 21. A manutenção dos ativos físicos deverá ser realizada pelos técnicos de TIC dos *campi* e da Reitoria, seguindo orientações estabelecidas pelo Órgão Gestor de TIC, ou, se houver garantia, pelo fornecedor contratado, mediante abertura de chamado.

Art. 22. Os técnicos de TIC dos *campi* e da Reitoria podem recompor ativos físicos utilizando peças de equipamentos obsoletos ou irrecuperáveis.

Parágrafo único. É vedada a alteração de peças de ativos físicos durante o período de garantia, salvo quando autorizado pelo fornecedor/fabricante.

Art. 23. A abertura de solicitações de garantia dos ativos físicos deve ser feita exclusivamente pelos os técnicos de TIC dos *campi* e da Reitoria.

Subseção III

Do monitoramento dos ativos de informação

Art. 24. O monitoramento dos ativos de informação deve conter, no mínimo, as seguintes etapas:

I. identificar e registrar os ativos de informação, padronizando o registro do parque tecnológico em sistema informatizado padronizado;

II. gerenciar o ciclo de vida dos ativos de informação;

III. gerenciar licenças de *software* adquiridas ou contratadas;

IV. gerenciar a capacidade e desempenho dos ativos de informação relacionados ao hardware; e

V. selecionar e priorizar de ativos para o monitoramento proativo contínuo com vistas a produzir relatórios, gráficos, ou alertas para detecção de problemas em *hardware* e *software*, especialmente aqueles que hospedam sistemas de informação ou forneçam conectividade à rede para diversos usuários, conforme capacidade tecnológica do ativo de informação.

Art. 25. Os ativos que sofrem degradação com o tempo devem ser monitorados para prevenir problemas e assegurar o seu funcionamento adequado.

§1º Os ativos de informação que compõem o *Data Center* e a infraestrutura de rede local e em nuvem devem ser monitorados e os seguintes indicadores devem ser observados, quando aplicável:

I. consumo de CPU, memória e disco;

II. atualizações de segurança de sistema operacional;

III. validade das licenças dos *softwares* instalados;

IV. atualizações de antivírus, se instalado;

V. taxas de utilização;

VI. taxas de erros;

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

VII. atraso dos pacotes;

VIII. período de disponibilidade dos *links*; e

IX. tempo ativo do sistema (Uptime).

§2º É recomendado que a coleta dos indicadores para o monitoramento dos ativos de informação seja feita de forma automatizada, mas poderá ser feita por amostragem quando a automatização não estiver disponível.

Art. 26. Os ativos de informação que compõem o *Data Center* e a infraestrutura de rede local e em nuvem que possuam indicadores que apontem ociosidade dos recursos computacionais poderão ser realocados para outras atividades.

Seção V

Do descarte e desfazimento dos ativos de informação

Art. 27. Os processos de descarte e desfazimento dos ativos de informação e do lixo eletrônico deve ser aderente à legislação pertinente, respeitando-se os critérios de sustentabilidade.

Art. 28. O remanejamento de ativos de informação deve ser priorizado em detrimento do descarte.

Parágrafo único. A metodologia de rodízio e reuso interno dos equipamentos, visando alocar os equipamentos mais modernos aos usuários cujas atividades cotidianas demandam maior capacidade computacional, cascateando os demais equipamentos aos demais usuários, deve ser definida de acordo com as prioridades de realocação com base nas atividades internas e sua necessidade de uso da tecnologia e capacidade computacional.

Art. 29. Os ativos de dados poderão ser descartados ou destruídos durante o processo de manutenção, que inclui formatação para devolução ou realocação do ativo, sendo o *backup* um procedimento de responsabilidade do usuário proprietário ou responsável pelos dados em questão.

Art. 30. Todos os dispositivos que armazenam dados serão formatados pelos técnicos da área de TIC antes do repasse e descarte.

Art. 31. As licenças de aplicações obtidas pela universidade e armazenadas em CDs e DVDs das fabricantes poderão ser descartadas por inservibilidade mediante Relatório de Bem Inservível emitido por técnico da área de TIC.

Art. 32. Os ativos de *hardware* devem ser descartados mediante avaliação do estado do bem e emissão do Relatório de Bem Inservível, ambos feitos por técnico da área TIC.

CAPÍTULO IV

DAS RESPONSABILIDADES E OBRIGAÇÕES

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

Art. 33. É de competência dos técnicos de TIC dos *campi*:

I. conferir os ativos de informação a serem recebidos no *campus*, oriundos de processos de aquisição ou doação, e assinar o termo de recebimento provisório do bem;

II. realizar o inventário dos ativos de informação localizados no respectivo *campus*;

III. atualizar os sistemas e padronizar as configurações dos equipamentos disponíveis no *campus*;

IV. fazer manutenções, dar suporte ou acionar a garantia dos ativos de *hardware* e *software* nos *campi*, quando necessário;

V. garantir a segurança de informações contidas em discos de armazenamento em casos de descartes, baixas patrimoniais, ou envios para consertos em empresas externas;

VI. implantar *softwares* em equipamentos dos *campi*, quando necessário; e

VII. registrar e manter atualizadas as informações coletadas dos ativos de informação no sistema informatizado indicado pelo Órgão Gestor de TIC.

Art. 34. É de competência do Órgão Gestor de TIC:

I. definir a padronização das configurações de *hardware* e *software* para os equipamentos da UFOB;

II. preparar a configuração necessária dos ativos TIC para plena utilização dos equipamentos e execução das atividades pelos usuários finais;

III. conferir os ativos de informação a serem recebidos na Reitoria, oriundos de processos de aquisição ou doação, e assinar o termo de recebimento provisório do bem;

IV. remanejar os ativos de informação mais antigos de acordo com suas especificações técnicas considerando as demandas setoriais para utilização das máquinas;

V. fazer manutenções, dar suporte ou acionar a garantia dos ativos de *hardware* e *software* na Reitoria, quando necessário;

VI. orientar sobre a proteção os ativos de *hardware* contra violação por meio do uso de lacres e/ou etiquetas;

VII. garantir a segurança de informações contidas em discos de armazenamento em casos de descartes, baixas patrimoniais, ou envios para consertos em empresas externas;

VIII. implantar *softwares* nos equipamentos da Reitoria, quando necessário.

IX. revisar periodicamente os processos da gestão de ativos de informação mapeados; e

X. elaborar as diretrizes para aquisição de novos equipamentos.

Art. 35. São obrigações dos usuários:

I. respeitar e seguir as diretrizes presentes nesta política;

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

II. fazer o *backup* de dados em máquinas de sua utilização de forma periódica ou quando houver necessidade de suporte técnico, considerando que o *backup* de arquivos pessoais salvos no sistema é de sua total responsabilidade;

III. não repassar, emprestar, ou entregar ativos de informação, ou componentes de ativos de informação, a pessoas sem autorização;

IV. não realizar, por conta própria, nenhum tipo de manutenção, formatação, atualização, instalação ou conserto em ativos de *hardware*;

V. não realizar por conta própria nenhum tipo de instalação ou atualização de *softwares*, com exceção da biblioteca de instaladores disponibilizada pelo Órgão Gestor de TIC em seu sistema informatizado; e

VI. acionar o *Helpdesk* por meio de chamado diante da necessidade de requisição e/ou suporte de TIC.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 36. Os casos omissos serão resolvidos pelo Órgão Gestor de TIC da UFOB.

Art. 37. Esta Resolução entra em vigor na data de sua publicação.

SIGNATÁRIO

Presidente da Câmara de Gestão Administrativa e Governança

MINUTA

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

PROPOSTA DE RESOLUÇÃO Nº 2/2024 - null (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/11/2024 21:22)
UILIAM RANGEL AMORIM SOUZA
PRO-REITOR(A)
PROTIC (11.01.06)
Matrícula: ###746#9

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***2****, ano:* ***2024****, tipo:* ***PROPOSTA DE RESOLUÇÃO****, data de emissão:* ***12/11/2024*** *e o código de verificação:* ***cdcb9c60a4***

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 CONSUNI Nº 3/2024 - null (11.01.21)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/11/2024 21:22)
UILIAM RANGEL AMORIM SOUZA
PRO-REITOR(A)
PROTIC (11.01.06)
Matrícula: ###746#9

*Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **3**, ano: **2024**, tipo: **RESOLUÇÃO CONSUNI**, data de emissão: **12/11/2024** e o código de verificação: **3e22e6729f***

Resolução Consuni nº 007/2018

Estabelece as normas de uso de recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito da Universidade Federal do Oeste da Bahia.

O Conselho Universitário da Universidade Federal do Oeste da Bahia, no uso de suas atribuições legais, e considerando a deliberação extraída da sessão ordinária realizada nos dias 08 e 09 de novembro de 2018,

RESOLVE:

Art. 1º Estabelecer as normas de uso de recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito da Universidade Federal do Oeste da Bahia (UFOB), nos termos estabelecidos no documento anexo.

CAPÍTULO I
DA OPERACIONALIZAÇÃO

Art. 2º Os recursos de TIC devem ser utilizados de maneira, ética e legal, consistente com os objetivos de ensino, pesquisa, extensão e administrativos da UFOB, definidos por meio de seu Estatuto, planos institucionais e outras normas internas, bem como nos termos da legislação vigente.

Art. 3º Usuário é qualquer pessoa física, devidamente autorizada, que utiliza os sistemas de informação ou a infraestrutura de TIC da UFOB.

Art. 4º São usuários de TIC da UFOB:

I - servidores;

II - discentes;

III - terceirizados;

IV - visitantes.

Art. 5º Incumbe aos usuários de TIC:

I - respeitar todas as normas e procedimentos de uso dos recursos de TIC;

II - usar os recursos de TIC de forma a não interferir ou comprometer a utilização destes por outros usuários;

III - respeitar os direitos de propriedade intelectual, as obrigações contratuais da UFOB e as licenças de uso específico;

IV - não permitir ou colaborar com o acesso aos recursos de TIC por parte de pessoas não autorizadas, sob pena de ser co-responsabilizado por eventuais problemas que esses acessos vierem a causar;

V - preservar as credencias de acesso à rede mantendo seu caráter pessoal e intransferível;

VI - zelar pelo uso consciente e racional dos recursos de TIC, não sobrepondo os interesses pessoais sobre os institucionais.

CAPÍTULO II
DO USO DE SOFTWARE

Art. 6º Os equipamentos de TIC da UFOB devem possuir licenciamento do sistema operacional e de todos os demais *softwares* instalados.

§1 º Caso seja verificado a ocorrência de *software* não licenciado, o mesmo será removido pelo Órgão de Gestão de TIC da UFOB.

§2 º Qualquer aquisição de equipamentos de TIC deve prever e garantir a compra de *software* legalizado para sua utilização, seja sistema operacional ou *software* de uso específico.

CAPÍTULO III
DO ACESSO ADMINISTRATIVO À EQUIPAMENTOS

Art. 7º Os equipamentos de TIC serão fornecidos aos usuários somente após o bloqueio das configurações da BIOS (*Basic Input/Output System*) e da conta administrativa, que serão acessíveis apenas pelo Órgão de Gestão de TIC da UFOB.

I - os usuários terão acesso aos equipamentos de TIC da instituição através da utilização de uma conta com perfil "Usuário Comum", sem privilégios administrativos;

II - equipamentos cuja área de atuação demande acesso administrativo, ou para fins de computação de alto desempenho, serão entregues com acesso à conta de administrador e às configurações da BIOS, mediante solicitação com justificativa, por parte do chefe do setor, que será analisada pelo Órgão de Gestão de TIC da UFOB.

Art. 8º São competências exclusivas do Órgão de Gestão de TIC da UFOB:

I - alterar as configurações da BIOS;

II - abrir equipamentos de TIC;

III - realizar qualquer alteração no *hardware*;

IV - remover componentes;

V - formatar e alterar sistemas operacionais ou outros *softwares*.

CAPÍTULO IV
DO USO DE EQUIPAMENTOS PESSOAIS

Art. 9º Qualquer utilização de dispositivos pessoais estará sujeita ao conjunto de normas e procedimentos que regem a área de TIC da UFOB.

Art. 10. A UFOB não se responsabiliza por acessos indevidos ao dispositivo pessoal, dano de *hardware* e/ou *software* que possam ocorrer ao equipamento. A responsabilidade de proteção física e lógica de equipamentos pessoais é exclusiva do proprietário.
Art. 11. A UFOB não fornecerá material de consumo, *software* ou manutenção em equipamentos pessoais.

Art. 12. A UFOB não se responsabiliza por *software* utilizado nos dispositivos pessoais que não possuírem as devidas licenças de uso.

CAPÍTULO V
DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 13. Em caso de descumprimento dos termos estabelecidos por esta norma, serão aplicadas sanções administrativas nos termos da legislação vigente.

Art. 14. As situações não previstas nesta resolução ou em instruções normativas correlatas serão apreciadas pelo Comitê Gestor de Tecnologia da Informação e Comunicação.

Art. 15. Esta Resolução entra em vigor na data de sua aprovação, revogadas quaisquer disposições em contrário.

Barreiras, 09 de novembro de 2018.

Iracema Santos Veloso
Presidente do Conselho Universitário

RESOLUÇÃO CONSUNI Nº 4/2024 - null (11.01.21)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/11/2024 21:22)
UILIAM RANGEL AMORIM SOUZA
PRO-REITOR(A)
PROTIC (11.01.06)
Matrícula: ###746#9

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***4****, ano:* ***2024****, tipo:* ***RESOLUÇÃO CONSUNI****, data de emissão:* ***12/11/2024*** *e o código de verificação:* ***a9256358fa***

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 2/2024 - null (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/11/2024 21:22)
UILIAM RANGEL AMORIM SOUZA
PRO-REITOR(A)
PROTIC (11.01.06)
Matrícula: ###746#9

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***2****, ano:* ***2024****, tipo:* ***DECRETO****, data de emissão:* ***12/11/2024*** *e o código de verificação:* ***eb19ae8ccd***

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
PRÓ-REITORIA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

DESPACHO Nº 25/2024 - PROTIC (11.01.06)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 12 de novembro de 2024.

Ao Sr. Presidente da Câmara de Gestão Administrativa e Governança, Clayton Barcelos.

Com os cordiais cumprimentos, considerando o que está posto no Relatório anexo a este processo, encaminho a solicitação de apreciação por esta câmara da Proposta da Resolução de Ativos de Informação no âmbito da UFOB.

(Assinado digitalmente em 12/11/2024 21:22)
UILIAM RANGEL AMORIM SOUZA
PRO-REITOR(A)
PROTIC (11.01.06)
Matrícula: ###746#9

Processo Associado: 23520.011101/2024-18

Visualize o documento original em https://sig.ufob.edu.br/public/documentos/index.jsp informando seu número: **25**, ano: **2024**, tipo: **DESPACHO**, data de emissão: **12/11/2024** e o código de verificação: **5f128aba93**

ATO DECISÓRIO CGTIC/UFOB Nº 01, DE 11 DE NOVEMBRO DE 2024

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 2024, realizada em 21 de maio de 2024**, decide:

Art. 1º Aprovar a minuta da Política de Gestão de Ativos de Informação da UFOB.

Art. 2º Este Ato Decisório entra em vigor a contar de 11 de novembro de 2024, justificado pela necessidade de atendimento ao princípio da continuidade do serviço público.

UILIAM RANGEL AMORIM SOUZA

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

EXTRATO DE DECISÃO Nº 2/2024 - null (11.01.10.09)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/11/2024 21:22)
UILIAM RANGEL AMORIM SOUZA
PRO-REITOR(A)
PROTIC (11.01.06)
Matrícula: ###746#9

*Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **2**, ano: **2024**, tipo: **EXTRATO DE DECISÃO**, data de emissão: **12/11/2024** e o código de verificação: **7ddfade770***