Serviço Público Federal

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

PROCESSO 23520.003869/2024-18

ELETRÔNICO

Cadastrado em 10/04/2024

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	cgtic@ufob.edu.br	11011009

Tipo do Processo:
PROPOSTA DE RESOLUÇÃO

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

Assunto Detalhado:
TRATA-SE DE PROPOSTA DE REGIMENTO INTERNO DO COMITÊ PERMANENTE DE SEGURANÇA DA INFORMAÇÃO CPSI DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA.

Unidade de Origem:
COMITÊ PERMANENTE DE SEGURANÇA DA INFORMAÇÃO (11.01.10.14)

Criado Por:
LUIZ HILARIO FERREIRA DAMASCENA

Observação:

MOVIMENTAÇÕES ASSOCIADAS

Data	Destino
12/04/2024	GABINETE REITORIA (11.01.10)
03/05/2024	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

TERMO DE ABERTURA DE PROCESSO

Aos **dez dias do mês de abril do ano de dois mil e vinte e quatro** procedi à abertura do Processo nº 23520.003869/2024-18, que se inicia com a folha nº 01 e trata da Solicitação de apreciação da Proposta de Regimento que regulamenta o funcionamento do Comitê Permanente de Segurança da Informação da Universidade Federal do Oeste da Bahia - UFOB.

Para constar eu subscrevo e assino.

LUIZ HILÁRIO FERREIRA DAMASCENA
Coordenador do Comitê Permanente de Segurança da Informação

TERMO DE ABERTURA DE PROCESSO Nº 1/2024 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 10/04/2024 17:59)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2024****, tipo:* ***TERMO DE ABERTURA DE PROCESSO****, data de emissão:* ***10/04/2024*** *e o código de verificação:* ***20a18edccb***

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 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 10/04/2024 17:59)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

*Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: **1**, ano: **2023**, tipo: **RESOLUÇÃO CGAG**, data de emissão: **10/04/2024** e o código de verificação: **977b4bba6e***

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Gabinete da Reitoria

PORTARIA UFOB N° 009, DE 01 DE FEVEREIRO DE 2024

O REITOR DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA, nomeado pelo Decreto de 11 de setembro de 2023, publicado no Diário Oficial da União em 12 de setembro de 2023, seção 2, pág. 1, tendo em vista o disposto no art. 8º da Lei nº 12.825, de 5 de junho de 2013, no uso das atribuições que lhe conferem no art. 51 do Regimento Geral da UFOB,

Considerando o disposto na RESOLUÇÃO CGAG/CONSUNI/UFOB Nº 018, de 24 de agosto de 2023, resolve:

Art. 1º Designar o servidor Luiz Hilário Ferreira Damascena, Analista de Tecnologia da Informação, matrícula Siape nº 1880542, para exercer a função de Gestor de Segurança da Informação, cujas competências estão elencadas no Art. 28 da resolução supracitada.

Art. 2º Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviços da UFOB.

JACQUES ANTONIO DE MIRANDA

Reitor

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

PORTARIA Nº 1/2024 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 10/04/2024 17:59)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2024****, tipo:* ***PORTARIA****, data de emissão:* ***10/04/2024*** *e o código de verificação:* ***e6b7d59891***

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Gabinete da Reitoria

PORTARIA UFOB N° 011, DE 01 DE FEVEREIRO DE 2024

O REITOR DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA, nomeado pelo Decreto de 11 de setembro de 2023, publicado no Diário Oficial da União em 12 de setembro de 2023, seção 2, pág. 1, tendo em vista o disposto no art. 8º da Lei nº 12.825, de 5 de junho de 2013, no uso das atribuições que lhe conferem no art. 51 do Regimento Geral da UFOB,

Considerando o disposto na RESOLUÇÃO CGAG/CONSUNI/UFOB Nº 018, de 24 de agosto de 2023, resolve:

Art. 1º Instituir o Comitê Permanente de Segurança da Informação, composto por:

I- Gestor de Segurança da Informação: Luiz Hilário Ferreira Damascena (Coordenador);
II- Representante da unidade gestora de Tecnologia da Informação e Comunicação: Cleyton Martins Sena;
III- Autoridade pelo monitoramento da Lei de Acesso à Informação: Andrea Santana Leone;
IV- Representante do Comitê Gestor de Tecnologia da Informação: Uiliam Rangel Amorim Souza;
V- Representante das áreas finalísticas (Pesquisa, Ensino e Extensão): Darlan do Nascimento Gomes;
VI- Encarregado pelo tratamento de dados pessoais: Reinilton da Silva Juvenal;

Art. 2º Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviços da UFOB.

JACQUES ANTONIO DE MIRANDA

Reitor

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

PORTARIA Nº 2/2024 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 10/04/2024 17:59)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***2****, ano:* ***2024****, tipo:* ***PORTARIA****, data de emissão:* ***10/04/2024*** *e o código de verificação:* ***23ea452aa8***

pedido, a Administração Aduaneira Requerente informará à Administração Aduaneira Requerida o uso que fez dos dados fornecidos e os resultados alcançados;

c) a Administração Aduaneira Requerente pode transmitir o dado pessoal apenas às Autoridades Policiais e, nos casos em que seja necessário para instauração de processo, à promotoria pública e às autoridades judiciais. Tal informação não será comunicada a outras autoridades a não ser que a Administração Aduaneira Requerida concorde expressamente, e que a legislação que reja as autoridades que receberam os dados permita tal comunicação;

d) a Administração Aduaneira Requerida terá de determinar a validade e a precisão dos dados pessoais a serem fornecidos. No caso de a Administração Aduaneira Requerida constatar que dados incorretos ou dados pessoais de conteúdo reservado tenham sido cedidos, ela terá de informar a Administração Aduaneira Requerente desse fato, sem demora. A Administração Aduaneira Requerente, ou possivelmente outra Administração que tenha recebido aquele dado pessoal, o corrigirá, destruirá ou eliminará esse dado pessoal sem demora;

e) a Administração Aduaneira Requerida fornecerá juntamente com os dados pessoais, o prazo final para a eliminação deles, de acordo com a legislação de sua Parte Contratante. A Administração Aduaneira Requerente eliminará a informação pessoal assim que a finalidade para a qual os dados pessoais possam ter ser usados em conformidade com este Acordo deixe de existir;

f) mediante pedido à autoridade competente de uma Parte Contratante e com o consentimento prévio escrito da outra Parte Contratante, a pessoa cujos dados tenham sido transferidos será notificada sobre o dado transferido e o uso pretendido, desde que os requisitos legais nacionais da Parte Contratante requerida a fornecer a informação não o vede. Entretanto, essa informação não será fornecida caso o interesse público prevaleça sobre os interesses da pessoa envolvida.

g) as Autoridades Aduaneiras manterão os registros de dados pessoais fornecidos ou recebidos;

h) as Autoridades Aduaneiras têm de adotar medidas que assegurem que os dados pessoais não estarão expostos a acesso não autorizado ou incidental, modificação, destruição, dano ou transmissão não autorizada, bem como a outros procedimentos não autorizados ou a mal uso; e

i) o manuseio de dados pessoais fornecidos, nos termos deste Acordo, será supervisionado em conformidade com a legislação em vigor no território das Partes Contratantes.

Artigo 16
Derrogação

1. Quando qualquer assistência solicitada nos termos deste Acordo puder violar a soberania, as leis e os compromissos internacionais, a segurança estatal, a saúde pública, a ordem pública, as atividades de combate ao crime, ou a qualquer outro interesse nacional fundamental da Parte Contratante requerida, ou prejudique qualquer interesse comercial ou profissional legítimos, tal assistência pode ser recusada por esta Parte Contratante ou ser fornecida mediante quaisquer termos ou condições que as circunstâncias venha a exigir.

2. Se uma Administração Aduaneira solicitar assistência em que ela própria não esteja apta a cumprir, caso essa assistência lhe seja solicitada pela Administração Aduaneira da outra Parte Contratante, ela destacará tal fato em seu pedido. O atendimento de tal pedido ficará a critério da Administração Aduaneira Requerida.

3. A assistência poderá ser postergada caso existam razões para se acreditar que a mesma interferirá em investigação, demanda judicial ou procedimentos em curso. Em tal caso, a Administração Aduaneira Requerida consultará a Administração Aduaneira Requerente, para avaliar se a assistência possa ser prestada sob termos ou condições que a Administração Aduaneira Requerida venha a especificar.

4. No caso em que a Administração Aduaneira Requerida conclua que os esforços necessários para o cumprimento de um pedido são claramente desproporcionais ao benefício esperado pela Administração Aduaneira Requerente, ela notificará a Administração Aduaneira Requerente dessa conclusão. A assistência requerida poderá ser recusada, se a Administração Aduaneira Requerente não fornecer informação que contradiga essa conclusão.

5. Quando a assistência for negada ou adiada, as razões para a recusa ou o adiamento serão fornecidas.

Artigo 17
Custos

1. As Partes Contratantes não reivindicarão o reembolso de despesas resultantes da execução desse Acordo. Entretanto, mediante pedido, as despesas com peritos, testemunhas, intérpretes e tradutores que não sejam funcionários do Estado serão reembolsadas pela Parte Contratante Requerente.

2. Caso despesas de natureza substancial e extraordinária sejam exigidas a fim de se executar um pedido, as Partes Contratantes se consultarão para determinar os termos e as condições sob as quais o pedido será atendido, bem como o modo pelo qual custos serão suportados.

Artigo 18
Implementação do Acordo

1. As Administrações Aduaneiras:

a) comunicar-se-ão diretamente para os fins de negociar as questões que surgirem no âmbito desse Acordo;

b) após consulta, estabelecerão as diretrizes administrativas necessárias para a implementação deste Acordo; e

c) envidarão esforços, por mútuo acordo, para solucionar os problemas ou questionamentos que decorrerem da interpretação ou aplicação deste Acordo.

2. As Administrações Aduaneiras podem acordar em disposições de implementação detalhadas com vistas a implementar adequadamente este Acordo.

3. Conflitos para os quais nenhuma solução puder ser encontrada serão resolvidos por via diplomática.

Artigo 19
Aplicação

Este Acordo será aplicável nos territórios de ambas as Partes Contratantes, conforme definido pelas suas disposições legais e administrativas nacionais.

Artigo 20
Entrada em vigor

Este Acordo entrará em vigor três meses depois que as Partes Contratantes tiverem notificado uma à outra, por escrito, por via diplomática, que os requisitos legais nacionais para entrada em vigor deste Acordo foram cumpridos.

Artigo 21
Denúncia

1. É intenção das Partes Contratante que este Acordo tenha duração indeterminada, mas ambas podem denunciá-lo, a qualquer tempo, mediante notificação escrita, por via diplomática. A denúncia surtirá efeito três meses a partir da data de notificação da denúncia à outra Parte Contratante.

2. Os procedimentos em andamento no momento da denúncia serão concluídos, de acordo com as disposições deste Acordo.

3. A denúncia deste Acordo não revoga a obrigação de sigilo conforme previsto no Artigo 14, parágrafo 2º.

Artigo 22
Revisão

As Administrações Aduaneiras realizarão reuniões a fim de rever este Acordo, quando necessário ou após cinco anos de sua entrada em vigor, a não ser que elas notifiquem uma à outra, por escrito, que nenhuma revisão é necessária.

EM TESTEMUNHO DO QUE, os abaixo assinados, devidamente autorizados por seus respectivos Governos, assinaram o presente Acordo.

FEITO em Praga, em 1º de novembro de 2012, em dois originais, nos idiomas português, tcheco e inglês, sendo todos os textos igualmente autênticos. No caso de divergência de interpretação do Acordo, o inglês prevalecerá.

PELA REPÚBLICA FEDERATIVA DO BRASIL

George Monteiro Prata
Embaixador em Praga

PELA REPÚBLICA TCHECA

Pavel Novotny
Diretor-Geral de Alfândega

DECRETO Nº 9.636, DE 26 DE DEZEMBRO DE 2018

Revoga o Decreto nº 38.893, de 14 de março de 1956, que aprova o Regulamento do Museu Histórico e Diplomático do Itamaraty.

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

D E C R E T A :

Art. 1º Fica revogado o Decreto nº 38.893, de 14 de março de 1956.

Art. 2º O Ministro de Estado das Relações Exteriores deverá editar o regulamento do Museu Histórico e Diplomático do Itamaraty.

Art. 3º Este Decreto entra em vigor em 1º de fevereiro de 2019.

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

MICHEL TEMER
Aloysio Nunes Ferreira Filho
Esteves Pedro Colnago Junior

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,

D E C R E T A :

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

I - a segurança cibernética;

II - a defesa cibernética;

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

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

CAPÍTULO II
DOS PRINCÍPIOS

Art. 3º São princípios da PNSI:

I - soberania nacional;

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

III - visão abrangente e sistêmica da segurança da informação;

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

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

VI - preservação do acervo histórico nacional;

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

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

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

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

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

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

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

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

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

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

CAPÍTULO III
DOS OBJETIVOS

Art. 4º São objetivos da PNSI:

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

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

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

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

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

VI - orientar ações relacionadas a:

a) segurança dos dados custodiados por entidades públicas;

b) segurança da informação das infraestruturas críticas;

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

d) tratamento das informações com restrição de acesso; e

VII - contribuir para a preservação da memória cultural brasileira.

CAPÍTULO IV
DOS INSTRUMENTOS

Art. 5º São instrumentos da PNSI:

I - a Estratégia Nacional de Segurança da Informação; e

II - os planos nacionais.

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

I - segurança cibernética;

II - defesa cibernética;

III - segurança das infraestruturas críticas;

IV - segurança da informação sigilosa; e

V - proteção contra vazamento de dados.

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

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

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

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

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

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

CAPÍTULO V
DO COMITÊ GESTOR DA SEGURANÇA DA INFORMAÇÃO

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

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

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

II - Casa Civil da Presidência da República;

III - Ministério da Justiça;

IV - Ministério da Segurança Pública;

V - Ministério da Defesa;

VI - Ministério das Relações Exteriores;

VII - Ministério da Fazenda;

VIII - Ministério dos Transportes, Portos e Aviação Civil;

IX - Ministério da Agricultura, Pecuária e Abastecimento;

X - Ministério da Educação;

XI - Ministério da Cultura;

XII - Ministério do Trabalho;

XIII - Ministério do Desenvolvimento Social;

XIV - Ministério da Saúde;

XV - Ministério da Indústria, Comércio Exterior e Serviços;

XVI - Ministério de Minas e Energia;

XVII - Ministério do Planejamento, Desenvolvimento e Gestão;

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

XIX - Ministério do Meio Ambiente;

XX - Ministério do Esporte;

XXI - Ministério do Turismo;

XXII - Ministério da Integração Nacional;

XXIII - Ministério das Cidades;

XXIV - Ministério da Transparência e Controladoria-Geral da União;

XXV - Ministério dos Direitos Humanos;

XXVI - Secretaria-Geral da Presidência da República;

XXVII - Secretaria de Governo da Presidência da República;

XXVIII - Advocacia-Geral da União; e

XXIX - Banco Central do Brasil.

§ 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.

§ 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.

§ 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.

§ 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.

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.

§ 3º A composição, o funcionamento e as competências dos grupos de trabalho ou câmaras técnicas serão estabelecidos pelo Comitê.

§ 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.

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

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:

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

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.

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

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.

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;

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.

§ 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.

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

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.

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:

"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

DECRETO Nº 1/2018 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 10/04/2024 17:59)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2018****, tipo:* ***DECRETO****, data de emissão:* ***10/04/2024*** *e o código de verificação:* ***bf226037f5***

RELATÓRIO DE PROPOSIÇÃO À CNR

Instrução do Processo: Comitê Permanente de Segurança da Informação
Processo: 23520.003869/2024-18
Assunto: Proposta de Regimento Interno do Comitê Permanente de Segurança da Informação da Universidade Federal do Oeste da Bahia
Interessados: Comitê Permanente de Segurança da Informação - CPSI Comitê Gestor de Tecnologia da Informação e Comunicação - CGTIC
Proponente: Comitê Permanente de Segurança da Informação
Documento de designação: PORTARIA UFOB Nº 011, de 01 de fevereiro de 2024.

OBJETO DA PROPOSTA

Trata-se da Proposta de Resolução para o Regimento Interno do Comitê Permanente de Segurança da Informação – CPSI 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 - PNSI e dispõe sobre a governança da segurança da informação no país.

Conforme art. 15, em sua alínea III, apresenta que cada órgão e entidade da administração pública federal deve "instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI".

O art. 16 da PNSI institui que "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".

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. 26 da Resolução dispõe no parágrafo único que "A composição e o funcionamento do Comitê Permanente de Segurança da Informação deverão ser regulamentados por regimento próprio". Adicionalmente, o art. 28 elenca que entre as competências do Gestor de Segurança da Informação está "coordenar o Comitê Permanente de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais".

A Universidade designou através da PORTARIA UFOB Nº 009, de 01 de fevereiro de 2024, o Gestor de Segurança da Informação e pela PORTARIA UFOB Nº 011, de 01 de fevereiro de 2024, a composição do Comitê Permanente de Segurança da Informação.

LEGISLAÇÃO

- 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

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm

- 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.

https://ufob.edu.br/a-ufob/instrumentos-normativos/resolucoes/2023/cgag/resolucao-cgag-018-2023-institui-a-politica-de-seguranca-da-informacao-2013-psi-da-ufob.pdf

PÚBLICO ALVO

A proposta alcança primordialmente aos membros do Comitê Permanente de Segurança da Informação da UFOB, frente ao seu funcionamento em pautas e ações nos temas relacionados as suas competências, perante solicitações da Universidade, do próprio comitê ou externas.

JUSTIFICATIVAS

Considerando a importância da existência do regimento para o funcionamento inicial do CPSI, foi elaborada a Proposta pelo Gestor de Segurança da Informação, que ocupa o cargo de Coordenador. O documento foi apreciado na 1ª Reunião Ordinária do Comitê Permanente de Segurança da Informação, em 08 de março de 2024, que com o acolhimento das sugestões do demais membros do CPSI foi aprovado por unanimidade.

DIMENSÕES

O objetivo do regimento é definir as diretrizes de funcionamento do CPSI, além delimitar as atribuições das pessoas competentes.

O documento é estruturado em 6 (seis) capítulos, a saber:

I – DA NATUREZA;

II – DA COMPOSIÇÃO;

III – DAS ATRIBUIÇÕES;

IV– DOS GRUPOS DE TRABALHO;

V – DO FUNCIONAMENTO DO CPSI;

VI – DAS DISPOSIÇÕES FINAIS.

CONSIDERAÇÕES FINAIS

Considerando os normativos vigentes relacionados e portarias de designação da Universidade, a proposta de Resolução que trata do funcionamento do Comitê Permanente de Segurança da Informação da UFOB apresenta em linhas gerais proposta para o seu modo de funcionamento, a fim de apoiar instâncias superiores na discussão de temas relativos à segurança da informação.

Barreiras, 10 de abril de 2024.

LUIZ HILÁRIO FERREIRA DAMASCENA

Comitê designado pela PORTARIA UFOB Nº 011, DE 01 DE FEVEREIRO DE 2024.

RELATÓRIO DE PROPOSIÇÃO À CNR Nº 1/2024 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 11/04/2024 18:42)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2024****, tipo:* ***RELATÓRIO DE PROPOSIÇÃO À CNR****, data de emissão:* ***11/04/2024*** *e o código de verificação:* ***eb713551cc***

Regimento Interno do Comitê Permanente de Segurança da Informação da UFOB

CAPÍTULO I
DA NATUREZA

Art. 1º O presente Regimento disciplina a organização, as competências e o funcionamento do Comitê Permanente de Segurança da Informação (CPSI) da Universidade Federal do Oeste da Bahia.

CAPÍTULO II
DA COMPOSIÇÃO

Art. 2º O Comitê Permanente de Segurança da Informação é constituído pelos seguintes membros:

I – Gestor de Segurança da Informação e Comunicações, que será o(a) coordenador(a);

II – Dirigente do órgão de Tecnologia da Informação e Comunicação;

III – Autoridade de monitoramento da LAI (Lei de Acesso à Informação);

IV – Encarregado pelo tratamento de dados pessoais;

V – Representante do Comitê Gestor de Tecnologia da Informação e Comunicação;

VI – Representante das áreas finalísticas de Ensino, Pesquisa e Extensão.

CAPÍTULO III
DAS ATRIBUIÇÕES

SEÇÃO I
DAS ATRIBUIÇÕES DOS MEMBROS DO CPSI

Art. 3º Considerando o Art. 27 da Resolução CGAG/CONSUNI/UFOB Nº 018, de 24 de agosto de 2023, compete ao CPSI:

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 complementares;

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

IV – propor alterações à Política de Segurança da Informação e às normas complementares; e

V – deliberar sobre normas complementares de segurança da informação.

SEÇÃO II
DAS ATRIBUIÇÕES DO COORDENADOR DO CPSI

Art. 4º Compete ao Gestor de Segurança da Informação que irá coordenar o CPSI:

I – elaborar as pautas e redigir as atas das reuniões;

II – convocar e presidir reuniões ordinárias e extraordinárias;

III – resolver as questões de ordem;

IV – exercer o voto de qualidade;

V – baixar atos necessários à organização interna;

VI – criar Grupos de Trabalho sobre assuntos técnicos ou operacionais para aprofundar debates e discussões.

CAPÍTULO IV
DOS GRUPOS DE TRABALHO

Art. 5º O(A) Coordenador(a) do Comitê poderá indicar membros para compor Grupos de Trabalho para a participação em tarefas específicas, permanentes ou temporárias, com competências, composições e meios adequados a cada caso.

§ 1º Cada Grupo de Trabalho terá um coordenador designado pelo CPSI.

§ 2º Poderão participar dos Grupos de Trabalho, sem direito a voto, pessoas externas ao Comitê, a convite do CPSI ou do coordenador do Grupo de Trabalho.

§ 3º As atividades dos Grupos de Trabalho serão objeto de relatório circunstanciado para encaminhamentos que se fizerem necessários.

CAPÍTULO V
DO FUNCIONAMENTO DO CPSI

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

Art. 6° Os recursos tecnológicos e apoio administrativo necessário ao funcionamento do Comitê Permanente de Segurança da Informação deverão ser garantidos pela Administração Superior.

Art. 7º O CPSI deverá reunir-se semestralmente ou quando convocado de forma extraordinária pelo(a) Coordenador(a) ou pela solicitação de mais da metade de seus membros.

§ 1º As reuniões ordinárias deverão ser agendadas com o mínimo de 10 (dez) dias úteis, ou se em ambiente virtual, 5 (dias) úteis de antecedência.

§ 2º As ausências devem ser previamente justificadas e encaminhadas ao(à) Coordenador(a).

§ 3º Reuniões extraordinárias deverão observar o prazo mínimo de 48 (quarenta e oito) horas entre a convocação e a realização da reunião.

§ 4º As sessões ocorrerão apenas com a presença da maioria simples dos seus membros.

Art. 8º Em reuniões ordinárias, todos os membros poderão propor itens de pauta, podendo ser encaminhados para o(a) Coordenador(a) com o mínimo de 15 (quinze) dias.

§ 1º A critério do(a) Coordenador(a) ou da maioria dos membros presentes, poderão ser propostas matérias relevantes, não expressamente consignadas na pauta da reunião, cabendo ao proponente relatá-la.

§ 2º As matérias referentes ao parágrafo anterior deverão ser propostas no início das sessões.

Art. 9º Em matérias deliberativas deverá haver a presença de 50% (cinquenta por cento) dos membros mais 01 (um) de seus membros.

Parágrafo Único. Todos os membros terão direito a voto simples.

Art. 10 As propostas de alterações em políticas e normas internas da universidade relativas à segurança da informação deverão ser encaminhadas ao Comitê Gestor de Tecnologia da Informação (CGTIC) da UFOB.

Art. 11 Os atos do Comitê serão registrados em atas e formalizados de acordo com a natureza da matéria.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 12 Os atos do CPSI serão publicados eletronicamente.

Art. 13 A participação no CPSI não enseja remuneração de qualquer espécie.

Art. 14 Os casos omissos a este regimento serão resolvidos pelo próprio CPSI em reunião ordinária.

Art. 15 Esta Resolução entra em vigor na data de sua publicação.

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

PROPOSTAS Nº 1/2024 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 11/04/2024 18:42)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2024****, tipo:* ***PROPOSTAS****, data de emissão:* ***11/04/2024*** *e o código de verificação:* ***af7f9fdbf0***

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Comitê Permanente de Segurança da Informação

OFICIO Nº 001/2024 - CPSI (11.01.10.14)

Barreias, 12 de abril de 2024.

A Vossa Magnificência o Senhor
Profª Dr. Jacques Antonio de Miranda
Reitor
Universidade Federal do Oeste da Bahia
Rua Profº José Seabra de Lemos, 316, Recantos dos Pássaros
Barreiras - BA

Assunto: Proposta de Regimento Interno do CPSI.

Magnífico Reitor,

Cumprimentando-o cordialmente, encaminhamos a Vossa Magnificência para conhecimento a proposta de Regimento Interno do Comitê Permanente de Segurança da Informação da Universidade Federal do Oeste da Bahia, em que havendo admissibilidade do conteúdo seja submetida para apreciação da Câmara de Normas e Recursos.

Respeitosamente,

LUIZ HILÁRIO FERREIRA DAMASCENA
Coordenador do Comitê Permanente de Segurança da Informação

OFICIO Nº 1/2024 - null (11.01.10.14)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 12/04/2024 19:19)
LUIZ HILARIO FERREIRA DAMASCENA
ANALISTA DE TEC DA INFORMACAO
PROTIC (11.01.06)
Matrícula: ###805#2

Visualize o documento original em https://sig.ufob.edu.br/documentos/ informando seu número: ***1****, ano:* ***2024****, tipo:* ***OFICIO****, data de emissão:* ***12/04/2024*** *e o código de verificação:* ***f78a111bdc***

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
GABINETE REITORIA

DESPACHO Nº 262/2024 - GAB.REITORIA (11.01.10)

Nº do Protocolo: NÃO PROTOCOLADO

Barreiras-BA, 03 de maio de 2024.

Prezada Gleiciane Dourado Costa,

Ao cumprimentá-la, após ciência do Magnífico Reitor, prof. Dr. Jacques Antonio de Miranda, encaminho a proposta de Regimento Interno do Comitê Permanente de Segurança da Informação da Universidade Federal do Oeste da Bahia, para apreciação da Câmara de Normas e Recursos.

Atenciosamente.

(Assinado digitalmente em 03/05/2024 19:56)
MARINA MEIRELLES PAES
CHEFE
GAB.REITORIA (11.01.10)
Matrícula: ###378#3

Processo Associado: 23520.003869/2024-18