Política Corporativa de Segurança da Informação e Proteção de Dados

PORTARIA MEC N° 495, DE 18 DE JULHO DE 2022 (DOU 136 SECÃO 1 PG. 95

Ministério da Educação
Comitê de Governança Digital
Subcomitê de Segurança da Informação e Privacidade de Dados

Brasília/DF, julho de 2022.

MINISTÉRIO DA EDUCAÇÃO

Victor Godoy Veiga
Ministro

COMITÊ DE GOVERNANÇA DIGITAL

José de Castro Barreto Júnior
Secretário Executivo

Carlos Francisco de Paula Nadalim
Secretário de Alfabetização

Mauro Luiz Rabelo
Secretário de Educação Básica

Tomás Dias Sant´Ana
Secretário de Educação Profissional e Tecnológica

Wagner Vilas Boas de Souza
Secretário de Educação Superior

Karine Silva dos Santos
Secretária de Modalidades Especializadas de Educação

Diana Guimarães Azin
Secretária de Regulação e Supervisão da Educação Superior

André Henrique dos Santos Castro
Subsecretário de Tecnologia da Informação e Comunicação

Jose Dos Reis De Oliveira
Encarregado pelo Tratamento de Dados Pessoais

SUBCOMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

Álvaro da Costa Rondon Neto
Gestor de Segurança da Informação

Jose Dos Reis De Oliveira
Encarregado pelo Tratamento de Dados Pessoais

Estêvão Perpétuo Martins
Representante da Secretaria Executiva

Daniel Prado Machado
Representante da Secretaria de Alfabetização

Felipe Campos de Oliveira
Representante da Secretaria de Educação Básica

Marina Ramos Vasconcelos Rada
Secretaria de Educação Profissional e Tecnológica

Rafael Richer Barbosa Moura
Secretaria de Educação Superior

Luciana Santana Leão
Representante da Secretaria de Modalidades Especializadas de Educação

Lucas Garcia Ferreira
Representante da Secretaria de Regulação e Supervisão da Educação Superior

APOIO TÉCNICO PARA ELABORAÇÃO E REVISÃO

Delson Pereira da Silva
Gerente de Governança, Projetos e Aquisições de TIC

Edgard Carvalho Ribeiro Neto
Coordenador-Geral de Infraestrutura e Segurança da Informação

DIÁRIO OFICIAL DA UNIÃO
Publicado em: 20/07/2022 | Edição: 136 | Seção: 1 | Página: 95
Órgão: Ministério da Educação/Gabinete do Ministro

PORTARIA Nº 495, DE 18 DE JULHO DE 2022

Institui a Política Corporativa de Segurança da Informação e Proteção de Dados - PSI.

O MINISTRO DE ESTADO DA EDUCAÇÃO, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II, da Constituição, resolve:

Art. 1º Instituir, na forma do Anexo I, a Política Corporativa de Segurança da Informação e Proteção de Dados do Ministério da Educação - PSI/MEC constituída pelo conjunto de objetivos, princípios, diretrizes, políticas, normas, práticas, estruturas organizacionais e competências para orientar o uso e o compartilhamento de ativos de informação durante todo o seu ciclo de vida, sob a ótica da segurança física e virtual, da defesa cibernética e da proteção de dados organizacionais, com a finalidade de garantir a disponibilidade, integridade, confidencialidade e autenticidade de dados e informações bem como a proteção de dados pessoais e a privacidade de indivíduos.

Art. 2º As diretrizes e orientações previstas na referida Política, nas normas complementares associadas, nos procedimentos, manuais e documentos correlatos são aplicáveis a todos os servidores, demais colaboradores e terceiros que tenham acesso a dados, informações e recursos de Tecnologia da Informação e Comunicação do Ministério da Educação.

Art. 3º A PSI/MEC poderá ser revista, sempre que necessário, a fim de assegurar seu alinhamento às prioridades e estratégias institucionais e às mudanças na legislação vigente.

Art. 4º Fica revogada a Portaria MEC nº 1.054, de 2 de agosto de 2011, e suas alterações (Portaria nº 996, de 6 de agosto de 2012).

Art. 5º Esta Portaria entra em vigor em 1º de agosto de 2022.

VICTOR GODOY VEIGA

Índice

Apêndices

Classificação

Origem	Aplicação
Comitê de Governança Digital	A PSI-MEC se aplica no âmbito do Ministério da Educação (exceto entidades vinculadas)

Classificação
Acesso Público I Informação não classificada (DECRETO Nº 7.724, DE 16 DE MAIO DE 2012)

Controle de versões

Versão	Descrição	Data de aprovação
Draft	Primeira versão submetida ao Subcomitê de Segurança da Informação e Proteção de Dados	18.05.2022
V0	Versão submetida ao Subcomitê de Segurança da Informação e Proteção de Dados	29.06.2022
V1	Versão publicada no Diário Oficial da União (Portaria n° 495)	18.07.2022

Referência normativa

Referência	Ementa
LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012	Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal
LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011	Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal
LEI Nº 12.965, DE 23 DE ABRIL DE 2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
LEI Nº 13.709, DE 14 DE AGOSTO DE 2018	Lei Geral de Proteção de Dados Pessoais (LGPD)
DECRETO-LEI N° 2.848, DE 7 DE DEZEMBRO DE 1940	Código Penal Brasileiro
DECRETO Nº 7.724, DE 16 DE MAIO DE 2012	Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.
DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012	Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018	Aprova a Política Nacional de Segurança de Infraestruturas Críticas
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.
DECRETO Nº 10.195, DE 30 DE DEZEMBRO DE 2019	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Educação.
DECRETO Nº 10.139, DE 28 DE NOVEMBRO DE 2019	Dispõe sobre a revisão e a consolidação dos atos normativos inferiores a decreto.
DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020	Aprova a Estratégia Nacional de Segurança Cibernética
DECRETO Nº 10.569, DE 9 DE DEZEMBRO DE 2020	Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas
INSTRUÇÃO NORMATIVA GSI/PR Nº 1, DE 27 DE MAIO DE 2020 e suas Normas Complementares	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal
INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021	Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal

1 Objetivo

A Política Corporativa de Segurança da Informação e Proteção de Dados (PSI-MEC) tem por objetivo definir e implantar no âmbito do Ministério da Educação os princípios, diretrizes e instrumentos da Política Nacional de Segurança da Informação instituída pelo Decreto n° 9.637, de 26 de dezembro de 2018, considerando a estrutura de gestão definida na Instrução Normativa n° 01, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República.

Esse documento considera, ainda, o disposto no Decreto n° 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética, e as instruções relacionadas à segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República. Todos os instrumentos normativos gerados a partir deste documento são parte integrante da Política Corporativa de Segurança da Informação e Proteção de Dados (PSI-MEC) e emanam dos princípios e diretrizes nela estabelecidos.

2 Escopo

A PSI-MEC abrange os domínios de segurança e defesa cibernética, segurança física e proteção de dados organizacionais e tem por escopo as ações destinadas preservação da disponibilidade, integridade, confidencialidade e autenticidade das informações e dados, bem como a proteção de dados pessoais e a privacidade, incluindo:

a) Estabelecer diretrizes no que se refere a comportamentos, procedimentos e normas de segurança da informação, comunicação e proteção de dados;

b) Estabelecer uma estrutura de gestão de segurança da informação, comunicação e proteção de dados adequada às diretrizes institucionais, considerando um conjunto de papéis, responsabilidades e instrumentos normativos e organizacionais;

c) Estabelecer orientações gerais de segurança da informação, comunicação e proteção de dados em harmonia com a legislação vigente, as boas práticas e a gestão eficiente dos riscos associados.

As diretrizes e orientações previstas nesta Política, nas demais normas específicas associadas e suas eventuais metodologias, manuais, procedimentos e documentos correlatos são aplicadas a todos os servidores, demais colaboradores e terceiros do Ministério da Educação que tenham acesso às informações e dados e aos recursos de Tecnologia da Informação e Comunicação.

3 Conceitos e definições

Na forma do art. 6° da Instrução Normativa n° 01, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, todos os termos e definições utilizados neste documento se baseiam no Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

4 Papéis e responsabilidades

Esta Política Corporativa de Segurança da Informação e Proteção de Dados envolve os seguintes papéis e responsabilidades:

a) Administradores de recursos de Tecnologia da Informação e Comunicações: equipe técnica responsável por um sistema de processamento de informações, serviço ou infraestrutura de TIC.

b) Custodiante da informação (qualquer pessoa que detém a posse das informações e dados): responsável por garantir a segurança das informações e dados sob sua posse e comunicar sobre situações que comprometam essa garantia;

c) Gestor da informação (colegiado, autoridade ou dirigente): responsável por classificar as informações e dados sob sua gestão e definir procedimentos e critérios de acesso;

d) Proprietário do ativo de informação: refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

e) Usuário de informação (ou usuário): pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação no Ministério da Educação, formalizada por meio da assinatura de termo de responsabilidade.

5 Princípios

As ações de segurança da informação, comunicações e proteção de dados do Ministério da Educação tem como norte as definições contidas na Política Nacional de Segurança da Informação (PNSI), bem como pelos seguintes princípios orientadores:

a) Alinhamento estratégico e sistêmico, que considera o alinhamento da Política Corporativa de Segurança da Informação e Proteção de Dados (PSI-MEC) com o planejamento estratégico institucional, com o modelo de governança e com a Política de Gestão de Riscos, Controles Internos e Integridade do Ministério da Educação (PGRCI/MEC) – bem como também perante a legislação e os demais regulamentos específicos aplicáveis à Administração Pública Federal e/ou emanados dos órgãos governantes superiores;

b) Universalidade e uniformidade, que considera a abrangência, gradual e permanentemente, a todos os processos organizacionais observando os mesmos conceitos, parâmetros, referenciais técnicos e procedimentos em todas as unidades e níveis corporativos - de forma integrada, respeitando as especificidades e a autonomia das unidades corporativas;

c) Transparência, que considera a obrigação fundamental de prestar informações confiáveis, relevantes e tempestivas à sociedade visando à participação social na proposição e no monitoramento da execução das políticas públicas geridas pelo Ministério da Educação - também refletida no dever institucional e dos agentes públicos de garantir o sigilo das informações e dados imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

d) Corresponsabilidade, constituída pelo dever de todas as partes envolvidas em conhecer e respeitar a Política Corporativa de Segurança da Informação e Proteção de Dados do Ministério da Educação e as normas específicas a ela associadas;

e) Continuidade dos processos e serviços críticos essenciais ao funcionamento do Ministério da Educação e ao cumprimento de sua missão institucional – protegendo sua disponibilidade e segurança e definindo uma estratégia adequada de prevenção, gestão e recuperação de incidentes, visando à continuidade do negócio e à redução dos impactos em ocorrências de interrupção causadas por desastres e/ou falhas; e

f) Educação, comunicação e cooperação para fomento e aprimoramento das práticas de promoção da cultura em segurança da informação.

6 Diretrizes

A gestão de segurança da informação deve ser suportada por ações e métodos que visem à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, tratamento de incidentes, tratamento das informações e dados, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional dos processos institucionais estratégicos, operacionais e táticos, considerando, sob caráter geral, o seguinte:

a) Informações e dados como ativos: toda e qualquer informação e dado gerado, custodiado, manipulado, utilizado ou armazenado no Ministério da Educação compõe o ativo de informação relevante para as suas atividades e devem ser protegidos e tratados com vistas à preservação dos princípios de disponibilidade, integridade, confidencialidade e autenticidade, bem como a proteção de dados pessoais e a privacidade, conforme as normas em vigor estabelecidas;

b) Classificação da informação como requisito: todo ativo de informação deve ser classificado e tratado segundo sua classificação de segurança da informação, de maneira a proteger adequadamente as informações e dados na sua criação, coleta, utilização, custódia e descarte;

c) Segregação de funções: sempre que processualmente viável, devem ser segregadas funções ou áreas de responsabilidade conflitantes, para que ninguém detenha controle de um processo crítico na sua totalidade, visando reduzir os riscos de mau uso, acidental ou deliberado, dos ativos de informação;

d) Estabelecer controles adequados à relevância e ao risco: as medidas e controles de segurança devem ser estabelecidos considerando a relevância dos ativos de informação e os níveis de risco associados – considerando o ambiente, o valor e a criticidade das informações e dados – de forma proporcional e balanceada, visando sempre a prevenção da ocorrência de incidentes;

e) Menor privilégio e mínimo acesso: pessoas e aplicações devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma determinada tarefa, tendo como condição a ciência expressa dos termos desta Política, as responsabilidades e compromissos decorridos deste acesso e o conhecimento das penalidades cabíveis pela inobservância das regras previstas;

f) Responsabilização individual: todos os usuários são responsáveis pela segurança dos ativos de informação que estejam sob sua custódia e pelo uso e guarda de suas credenciais de acesso, sendo vedada a exploração de eventuais vulnerabilidades – que, assim que identificadas, devem ser imediatamente comunicadas às instâncias superiores;

g) Corresponsabilidade de terceiros: todos os contratos de prestação de serviços, firmados pelo Ministério da Educação deverão conter cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, incluindo a assinatura de Termo de Responsabilidade pelas empresas contratadas e de Termo de Ciência pelos colaboradores diretamente envolvidas na execução dos serviços contratados;

h) Restrição de uso dos ativos de informação: o acesso e uso das informações e dados que não sejam de domínio público e dos ativos de informação do MEC são controlados e limitados às atribuições necessárias para cumprimento das atividades dos solicitantes e usuários devidamente autorizados e utilizados no estrito interesse do custodiante, apenas para as finalidades profissionais, lícitas, éticas, administrativamente aprovadas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização do proprietário do ativo de informação;

i) Uso seguro dos ativos de informação: apenas os ativos de informação homologados e autorizados pelo MEC devem ter uso permitido, desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário do ativo de informação responsável. Os ativos de informação devem ter documentação atualizada, riscos mapeados, capacidade e contingência adequadas e sua operação deve estar de acordo com as normas, cláusulas contratuais e a legislação em vigor;

Essas diretrizes gerais constituem os pilares da gestão de segurança da informação e proteção de dados do Ministério da Educação e norteiam a construção das ações, planos e normas associadas que objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política. Assim, considerando o rol mínimo estabelecido no Inc IV do art. 12 da Instrução Normativa GSI/PR n° 1, de 27 de maio de 2020, com base nas diretrizes gerais, ficam estabelecidas as seguintes diretrizes específicas, por tema.

6.1 Tratamento da informação

Toda informação e dado criado manuseado, armazenado, transportado, descartado ou custodiado pelo Ministério da Educação é de sua responsabilidade e deve ser classificado e tratado adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, bem como a proteção de dados pessoais e a privacidade, de forma explícita ou implícita, em harmonia com a legislação aplicável, em especial a Lei n° 12.527, de 18 de novembro de 2011 (LAI), o Decreto nº 7.724, de 16 de maio de 2012, e o Decreto nº 7.845, de 14 de novembro de 2012.

Toda informação e dado institucional, se eletrônica, será armazenada nos servidores de arquivos e bases de dados sob gestão e administração da Subsecretaria de Tecnologia da Informação e Comunicação e, se não eletrônica, mantida em local físico adequado.

Toda informação e dado institucional sob a forma eletrônica deverá estar salvaguardada por meio de cópia de segurança (backup) em solução que garanta sua preservação e recuperação, quando necessária, conforme disposto em normas e procedimentos específicos sob responsabilidade da Subsecretaria de Tecnologia da Informação e Comunicação.

As informações e dados classificados, considerando a legislação vigente, que sejam produzidos, armazenados e/ou transportados em meio eletrônico utilizarão criptografia compatível com o respectivo grau de sigilo, em especial as informações de autenticação de usuários das aplicações geridas pelo MEC.

No descarte de informações e dados institucionais deverão ser observadas – além das próprias regras de sua respectiva classificação – as políticas, as normas e os procedimentos internos a serem estabelecidos em regramento próprio, bem como a temporalidade prevista na legislação, em especial atenção às definições da Lei n° 12.527, de 18 de novembro de 2011.

Ao aplicar uma classificação a um documento e/ou informação/dado, todos os agentes responsáveis devem usar o bom senso, adotando como princípio orientador a garantia do direito fundamental de acesso à informação. É responsabilidade de todos garantir que as informações e dados sejam classificados apropriadamente, aplicando os procedimentos pertinentes relativos à respectiva classificação, de acordo com os critérios estabelecidos.

Os agentes responsáveis pelo tratamento dos dados são responsáveis por (i) decidir a classificação das informações e dados relevantes, (ii) comunicar o valor e a classificação da informação ou dado quando for liberado ou fornecido a terceiros, e (iii) controlar o acesso às informações e dados custodiados. O usuário de informação, por sua vez, é responsável pela proteção da segurança e integridade das informações e dados em sua posse, devendo se familiarizar com as normas específicas do custodiante e com a legislação pertinentes.

6.2 Controles de acesso

Todo usuário de informação que faça uso dos recursos de Tecnologia da Informação e Comunicação do Ministério da Educação deverá possuir uma conta de acesso única e intransferível, que permita seu reconhecimento individual de maneira inequívoca e cuja concessão e gerenciamento serão regulamentadas em norma específica associada.

O agente responsável pelo tratamento dos dados é responsável pela concessão e revogação dos privilégios de acesso às informações sob sua tutela, considerando sempre o princípio do menor privilégio.

6.3 Gestão de riscos

No que couber, a gestão de riscos em segurança da informação e proteção de dados deve observar as disposições da Portaria n° 563, de 30 de junho de 2020, que trata da Política de Gestão de Riscos, Controles Internos e Integridade do Ministério da Educação.

O processo de gestão de riscos em segurança da informação deve fornecer uma estrutura consistente de gerenciamento através da qual os riscos relacionados aos processos e funções críticos possam ser identificados, avaliados e tratados através dos sistemas de revisão, controle e garantia.

6.4 Gestão de continuidade

Fica estabelecido o Programa de Gestão de Continuidade de Negócio (PGCN) em Segurança da Informação e Proteção de Dados no âmbito do Ministério da Educação, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de Tecnologia da Informação e Comunicação que suportam as operações do MEC.

Toda solução, sistema, aplicação e/ou serviço crítico do Ministério da Educação deverá estar suportado pelo Programa de Gestão de Continuidade de Negócio (PGCN).

6.5 Gestão de mudanças

No que se refere à segurança da informação, o processo de Gestão de Mudanças deve ser estruturado visando aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações e dados, bem como a proteção de dados pessoais e a privacidade – sendo composto, no mínimo, pelas fases de descrição, avaliação, aprovação, implementação e verificação.

Toda mudança nos ambientes computacionais do Ministério da Educação, que tenha sido homologada e testada, necessita ser documentada e registrada.

6.6 Segurança física e do ambiente

As ações de segurança física e ambiental, no que se refere aos aspectos de segurança da informação, devem prover normas e procedimentos que abordem, no mínimo, os seguintes aspectos:

a) Controle e monitoramento de acesso físico: compreende as necessidades de controle e monitoramento de acesso às instalações e aos ambientes físicos do órgão, gestão de autorizações e manutenção de registros de acesso de pessoal autorizado e de visitantes;

b) Controles ambientais: compreende provisão e manutenção dos controles ambientais necessários, com base em uma avaliação de requisitos, que inclui, mas não se limita a, energia de reserva para facilitar um processo de desligamento ordenado (no mínimo), detecção e supressão de incêndios, controles de temperatura e umidade e detecção e mitigação de danos ambientais; e

c) Descarte seguro de equipamentos: compreende a provisão e manutenção de controles para identificação e remoção permanente de quaisquer dados sensíveis e software licenciados em equipamentos antes do descarte.

6.7 Gestão de incidentes em segurança da informação

O Ministério da Educação deve prover e manter normas e procedimentos de Resposta a Incidentes consistentes com as leis e políticas governamentais aplicáveis, incluindo, mas não se limitando à identificação de papéis e responsabilidades, investigação, procedimentos de contenção e escalonamento, documentação e preservação de evidências, protocolos de comunicação e lições aprendidas.

O processo de gestão de incidentes deve envolver também procedimentos adequados de comunicação de incidentes incluindo, mas não se limitando a, treinamento de servidores, demais colaboradores e terceiros para identificar e comunicar rapidamente incidentes e preparação e apresentação de relatórios de acompanhamento.

Cabe à Subsecretaria de Tecnologia da Informação e Comunicação a responsabilidade pela infraestrutura necessária para fins de registro e resposta aos incidentes de segurança da informação no âmbito da rede corporativa do Ministério da Educação.

6.8 Gestão de ativos

O Ministério da Educação manterá um processo de inventário e mapeamento dos ativos de informação objetivando a segurança das infraestruturas críticas que garantem suas Informações e dados.

O processo de inventário e mapeamento de ativos de informação subsidiará o conhecimento, valoração, proteção e a manutenção de seus ativos de informação e deverá ser dinâmico, periódico e estruturado, para manter a base de dados de ativos de informação atualizada.

6.9 Gestão de comunicações

Todos os sistemas de comunicação eletrônica, quer seja de origem externa ou interna, são recursos de Tecnologia da Informação e Comunicação disponibilizados pelo Ministério da Educação aos seus servidores, demais colaboradores e terceiros e devem ser utilizados precipuamente no exercício das funções institucionais, em conexão com a finalidade do órgão e de forma aderente à esta Política e à legislação vigente, podendo ser concedido ou revogado a qualquer tempo, em caráter total ou parcial, de acordo com os interesses do Ministério.

O MEC se reserva o direito de monitorar, acessar e revisar quaisquer aspectos de seus recursos de informação eletrônica e sistemas de comunicação, incluindo, entre outros, o uso da Internet, sistemas de comunicação eletrônica, sistemas de telefonia, tráfego da rede e revisar ativos armazenados em qualquer sistema de comunicação. O consentimento para tais registros e monitoramento é presumido por parte dos usuários, não cabendo qualquer contestação ou alegação de desconhecimento dessa regra.

As comunicações eletrônicas são comunicações formais, e espera-se que os usuários exerçam o mesmo cuidado e profissionalismo na aplicação desses recursos como o faria com qualquer outro expediente de comunicação formal emitido em nome do MEC. O uso dos recursos de comunicação eletrônica deverá ser disciplinado em regramento próprio, associado a esta Política.

6.10 Acesso à internet

O acesso à Internet no ambiente de trabalho do Ministério da Educação está condicionado às necessidades dos agentes públicos no exercício de suas atribuições e será regido por norma específica, em conformidade com esta PSI-MEC e demais orientações governamentais e legislação em vigor.

Cada usuário de informação é responsável por tomar todas as medidas razoáveis para utilizar os recursos de internet de forma responsável e segura - credenciais de acesso são pessoais e intransferíveis, sendo que o usuário é individualmente responsável por todas as atividades exercidas a partir de sua credencial.

Ainda, no que se refere ao acesso à internet, cada usuário deve:

a) Utilizar os recursos de forma a proteger a organização de qualquer risco legal, regulatório, operacional ou de reputação;

b) Não compartilhar suas credenciais de acesso;

c) Não acessar websites ou objetos com conteúdo inadequado ou ilegal;

d) Estar ciente de suas responsabilidades pelo uso apropriado da Internet; e

e) Estar ciente de que seu uso da internet está sujeito a registro e pode ser monitorado de acordo com as exigências das leis e regulamentos aplicáveis.

6.11 Computação em nuvem

O uso de aplicativos e serviços em nuvem deve assegurar que toda a cadeia de suprimentos de TIC baseada em provedores de serviços no ambiente de computação em nuvem seja avaliada por todos os aspectos de segurança para proteger dados, metadados, informações e conhecimentos produzidos ou custodiados pelo Ministério da Educação, incluindo o cumprimento da legislação e regulamentação nacional e estrangeira, o gerenciamento de identidades, o monitoramento e auditoria regulares e as restrições de localizações geográficas.

6.12 Desenvolvimento seguro de software

O processo de desenvolvimento de software no Ministério da Educação deve priorizar a adoção de práticas voltadas à segurança da informação como modelagem de ameaças, análise estática do código com uso de ferramentas, revisão de código, testes de segurança direcionados – objetivando a minimização do surgimento de vulnerabilidades.

Os requisitos de segurança da informação deverão compor a lista de requisitos desde a concepção dos projetos de desenvolvimento e/ou aquisição de software – incluindo a definição da camada responsável pela validação do atendimento a esses requisitos.

A monitoração da performance de aplicações deverá ser realizada preferencialmente mediante análise dinâmica ponto a ponto, não sendo admitida a operação de aplicações em ambiente de produção enquanto perdurar qualquer falha de segurança considerada crítica.

6.13 Auditoria e conformidade

O uso dos recursos de Tecnologia da Informação e Comunicação disponibilizados pelo Ministério da Educação é passível de monitoramento e auditoria – incluindo a análise regular de registros de eventos (*log*) com aplicação, sempre que viável, de softwares utilitários específicos para monitoramento do uso de sistemas computacionais.

Sempre que possível, deverão ser implementados e mantidos mecanismos que permitam a rastreabilidade dos recursos de TIC através de estratégias como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede corporativa.

Como medida de preservação de evidências, sempre que tecnicamente possível, todo e qualquer ativo de informação deverá ser configurado para armazenar registros históricos de registros de eventos (*log*) em formato que permita a completa identificação dos fluxos de dados e das operações de seus usuários e/ou administradores. Esses registros devem ser armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos e os ativos de informação devem ser configurados de forma a armazenar seus registros de eventos (*log*) não apenas localmente, como também remotamente, por meio de tecnologia aplicável.

7 Estrutura de gestão de segurança da informação

A estrutura de Gestão de Segurança da Informação do Ministério da Educação possui a seguinte composição:

a) Alta administração: representada pela autoridade máxima do Ministério da Educação ou o seu substituto nomeado oficialmente, responsável por adotar as decisões acerca do tratamento das informações e dados vinculados à atuação institucional do Ministério.

b) Subsecretaria de Tecnologia da Informação e Comunicação: unidade responsável pela gestão da informação e proteção de dados em meio eletrônico no âmbito do MEC, apoia as unidades na definição de procedimentos para proteção de suas informações e dados, monitora e avalia as práticas de segurança da informação e coordena ações de conscientização e treinamento, bem como de tratamento de incidentes de segurança da informação, considerando as suas competências institucionais previstas no Decreto n° 10.195, de 30 de dezembro de 2019;

c) Comitê de Governança Digital (CGD-MEC): órgão colegiado de natureza deliberativa e de caráter permanente, de cunho estratégico e executivo, instituído para deliberar sobre assuntos relativos à Governança Digital e às ações, aos programas, às políticas e aos projetos de Tecnologia da Informação e Comunicação no âmbito do Ministério da Educação, conforme competências estabelecidas na Portaria MEC n° 565, de 28 de julho de 2021.

d) Subcomitê de Segurança da Informação e Proteção de Dados (SSIP-MEC): colegiado subordinado ao Comitê de Governança Digital (CGD-MEC) responsável por tratar de assuntos relacionados à segurança da informação, a privacidade e a proteção de dados pessoais no âmbito do Ministério da Educação, conforme competências estabelecidas na Portaria MEC n° 10.012, de 25 de novembro de 2021, considerado como estrutura equivalente àquela prevista no art. 20 da Instrução Normativa GSI/PR n° 01, de 27 de maio de 2020;

e) Gestor de Segurança da Informação: servidor formalmente designado pela Portaria MEC n° 1.110, de 24 de dezembro de 2021, para exercer as competências definidas no art. 19 da Instrução Normativa GSI/PR n° 01, de 27 de maio de 2020;

f) Dirigente de unidade ou subunidade: responsável por conscientizar servidores, demais colaboradores e terceiros em relação aos conceitos e práticas de segurança da informação, bem como incorporá-las aos processos de trabalho da unidade. Em caso de comprometimento da segurança da informação, devem tomar medidas administrativas para que sejam adotadas ações corretivas em tempo hábil;

g) Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR-MEC): equipe responsável por receber, analisar e responder às notificações e atividades relacionadas a incidentes cibernéticos no âmbito do Ministério da Educação, prevista no art. 22 da Instrução Normativa GSI/PR n° 01, de 27 de maior de 2020, e regulamentada pela Norma Complementar n° 05/IN01/DSIC/GSIPR;

h) Servidores, demais colaboradores e terceiros: qualquer pessoa que tenha acesso a informações e dados do Ministério da Educação, responsável pela segurança da informação dos ativos a que tenha acesso;

Quanto à composição normativa, a gestão de segurança da informação do Ministério da Educação obedece à seguinte estrutura:

a) Política (nível estratégico): documento que define objetivos, princípios e diretrizes de alto nível que traduzem a visão estratégica do órgão nessa temática e orientam a elaboração de normas, procedimentos e ações de segurança da informação e proteção de dados;

b) Normas Complementares (nível tático): especificam, no plano tático, as regras, as escolhas tecnológicas e os controles que deverão ser implementados para execução dos objetivos e diretrizes oriundas da Política de Segurança da Informação e Proteção de Dados, dotando-a de instrumentos de implementação; e

c) Procedimentos (nível operacional): instrumentalizam o disposto nas normas, orientando e direcionamento sua aplicação.

8 Penalidades

Ações que violem a Política Corporativa de Segurança da Informação e Proteção de Dados do Ministério da Educação caracterizam infração funcional e poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurado aos envolvidos o contraditório e a ampla defesa.

9 Atualização e revisão

A Política Corporativa de Segurança da Informação e Proteção de Dados do Ministério da Educação deverá ser revisada em função de alterações na legislação pertinente, das diretrizes superiores do Governo Federal, de alterações nos normativos internos, quando considerada necessária ou no prazo máximo de quatro anos, a contar da data de sua publicação, mediante proposição pelo Subcomitê de Segurança da Informação e Proteção de Dados e aprovação pelo Comitê de Governança Digital.

O Subcomitê de Segurança da Informação e Proteção de Dados poderá expedir normas complementares associadas à PSI-MEC, no âmbito de sua competência regimental, visando detalhar particularidades e procedimentos relativos à sua implementação no âmbito do Ministério da Educação.

À Subsecretaria de Tecnologia da Informação e Comunicação incumbe expedir e gerir os procedimentos de nível operacional que instrumentalizam o disposto nas normas complementares e nesta Política.

10 Classificação das informações

As informações e dados deverão ser classificados (agrupados em "classes") para otimizar os controles que garantem seu acesso apenas por pessoas autorizadas, conforme processo a ser definido em normativo próprio. As classes devem se alinhar ao disposto na Lei n° 12.527/2011 (Lei de Acesso à Informação) e em outras leis que definem regras de sigilo tais como sigilo fiscal, bancário, comercial e aquele relativo a denúncias.

11 Disposição finais

Esta Política Corporativa de Segurança da Informação e Proteção de Dados e suas atualizações deverão ser divulgadas amplamente a todos os servidores, demais colaboradores e terceiros do Ministério da Educação, ainda que sua atuação no Órgão seja temporária, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

É responsabilidade de todos os gestores do Ministério da Educação promover o conhecimento e a disseminação desta Política e demais normas associadas de segurança da informação aos servidores, demais colaboradores e terceiros sob a sua gestão.

As dúvidas sobre esta Política e seus documentos associados devem ser submetidas ao Subcomitê de Segurança da Informação e Proteção de Dados do Ministério da Educação.

Brasília/DF, 18 de julho de 2022.

Aprovado e publicado pela Portaria MEC n° 495, de 18 de julho de 2022

(DOU N° 136, SEÇÃO 1, PG. 95, DE 20/07/2022

ANEXO A: GLOSSÁRIO DE TERMOS

Autenticidade: informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

Divulgação não autorizada: revelação intencional ou não intencional de informações restritas a pessoas, tanto dentro como fora da organização, que não têm necessidade de conhecer essas informações.

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

E-mail: transmissão eletrônica de informações através de um protocolo de correio, como SMTP ou IMAP.

Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

Informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Mensagens: todas as mensagens, arquivos ou outros dados criados, carregados, baixados, enviados, recebidos ou armazenados em qualquer sistema de comunicações eletrônicas.

Mídias Sociais: incluem todas as formas e plataformas de comunicação e expressão públicas, baseadas na web, que reúnem as pessoas, facilitando a publicação de conteúdo para muitos públicos.

Recursos de Tecnologia da Informação e Comunicação: conjunto de aplicativos, serviços, ativos de tecnologia da informação ou outros componentes de processamento digital de informações e dados.

Sistema de Comunicação Eletrônica: correio de voz, correio eletrônico, mensagens instantâneas, áudio e vídeo, intranet ou sistema de acesso à Internet de propriedade, alugado, operado, mantido ou administrado pela organização.

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

Ministério da Educação
Comitê de Governança Digital
Subcomitê de Segurança da Informação e Proteção de Dados

gov.br/**mec**

Esplanada dos Ministérios Bloco L - Ed. Sede e Anexos
CEP: 70.047-900 - Brasília / DF
Telefones: (0xx 61) 0800-616161