Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul
Pró-Reitoria de Desenvolvimento Institucional
Diretoria de Tecnologia da Informação
Conselho Superior

Política de Segurança da Informação (PSI) do IFRS

Aprovada pelo Conselho Superior do IFRS, conforme a RESOLUÇÃO Nº 40/2025-CONSUP-REI.

Bento Gonçalves, agosto de 2025.

CAPÍTULO I
DISPOSIÇÕES GERAIS

Seção I
Dos Objetivos

Art. 1º A Política de Segurança da Informação (PSI) está alinhada às estratégias do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS), que objetiva estabelecer diretrizes, normas, procedimentos e responsabilidades para o manuseio, tratamento, controle e proteção de dados e informações produzidas ou sob sua custódia.

Seção II
Dos Princípios

Art. 2º As ações de segurança da informação do IFRS são orientadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, assim como pelos seguintes princípios:

I - disponibilidade, integridade, confidencialidade e autenticidade das informações;

II - continuidade dos processos e serviços essenciais para o funcionamento do IFRS;

III - economicidade da proteção dos ativos de informação;

IV - respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V - observância da publicidade como preceito geral e do sigilo como exceção;

VI – responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII - alinhamento estratégico da Política de Segurança da Informação com o Planejamento Estratégico do IFRS, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

VIII. conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis; e

IX. educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 3º Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito do IFRS e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 4º As normas, procedimentos, manuais e metodologias de segurança da informação do IFRS devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 5º As ações de segurança da informação devem:

I - considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do IFRS;

II - ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do IFRS;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e

IV. visar à prevenção da ocorrência de incidentes.

Art. 6º O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao IFRS.

Art. 7º Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no IFRS compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Art. 8º A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do IFRS, devem ser divulgadas amplamente a todos os usuários de informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os usuários de informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Seção III
Do Escopo

Art. 9º Esta Política de Segurança da Informação (PSI) se aplica aos seguintes grupos do IFRS:

I - todos os funcionários, sejam servidores efetivos ou temporários, do IFRS;

II - todos os contratados, estagiários, bolsistas e terceiros que prestam serviços para o IFRS;

III - todos os funcionários de parceiros;

IV - todos os discentes e visitantes; e

V - demais pessoas não abrangidas nos incisos anteriores que tenham acesso a dados ou informações do IFRS.

Art. 10 Esta Política de Segurança da Informação (PSI) refere-se:

I - aos aspectos estratégicos, estruturais, organizacionais e procedimentais, preparando a base para elaboração dos demais documentos normativos que os incorporarão;

II - aos requisitos da segurança humana;

III - aos requisitos da segurança física; e

IV - aos requisitos da segurança lógica.

Art. 11 Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo IFRS devem estar em conformidade com esta Política de Segurança da Informação.

Seção IV
Dos Termos e Definições

Art. 12 Esta Política de Segurança da Informação (PSI) considera a terminologia descrita a seguir:

I - Ativo**:** aquilo que tem valor – tangível ou intangível - para a organização (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional).

II - Ativo Crítico: equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização.

III - Autenticação: processo que busca verificar a identidade digital de uma entidade de um sistema no momento em que ela requisita acesso a esse sistema.

IV - Backup: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de perda dos originais.

V - CGSI: acrônimo de Comitê Gestor de Segurança da Informação.

VI - Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizadas não tenham conhecimento da informação, de forma proposital ou acidental.

VII - Criptografia**:** arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno).

VIII - Dados: são registros brutos de fatos, eventos, observações ou medições que, por si só, não têm significado completo. Eles precisam ser organizados, interpretados e analisados para se tornarem informação.

IX - Dados em trânsito: dados ou informações que são transmitidas entre sistemas ou dispositivos em uma rede.

X - Dados sensíveis: informações que, se acessadas, modificadas ou divulgadas indevidamente, podem causar prejuízo relevante à organização, aos indivíduos ou aos processos institucionais.

XI - Disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa ou entidade devidamente autorizada.

XII - Dispositivos não computacionais**:** dispositivos que não possuem capacidade de processamento ou execução de tarefas computacionais.

XIII - Engenharia Social: técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da SI, é considerada uma prática de má-fé, usada por

indivíduos para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes.

XIV - ETIR: Equipe de Prevenção, Tratamento e Resposta à Incidentes Cibernéticos.

XV - Hardware: parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas, que se comunicam através de barramentos.

XVI - Firewall: recurso destinado a evitar acesso não autorizado a uma determinada rede, ou a um conjunto de redes, ou a partir dela. Podem ser implementados em *hardware* ou *software*, ou em ambos.

XVII - HTTPS: Hypertext Transfer Protocol Secure. Protocolo de comunicação seguro para transferência de dados na web.

XVIII - Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

XIX - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

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

XXI - Logs: registros de eventos ou atividades em um sistema.

XXII - Malware: códigos maliciosos projetados para causar danos a sistemas.

XXIII - MFA: acrônimo de autenticação de multifatores (*multifactor authentication*).

XXIV - Navegador de Internet (browser): software utilizado para navegação na Internet, instalado nos recursos computacionais. Exemplo: Google Chrome, Internet Explorer, Mozilla Firefox.

XXV - Patch: atualização ou correção de *software* que resolve falhas, melhora a segurança ou adiciona funcionalidades.

XXVI - PDI: acrônimo de Plano de Desenvolvimento Institucional.

XXVII - Processo: sequência contínua de fatos ou operações que apresentam certa unidade ou que se reproduzem com certa regularidade: ação continuada, realização contínua e prolongada de alguma atividade.

XXVIII - Retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

XXIX - Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade.

XXX - Segurança da Informação: preservação da confidencialidade, da integridade e da disponibilidade da informação. Adicionalmente há outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade, que podem também estar envolvidas.

XXXI - Software: Programa de computador desenvolvido para executar um conjunto de ações previamente definidas.

XXXII - SSH: Secure Shell: Protocolo que fornece uma maneira segura de acessar e gerenciar sistemas remotamente.

XXXIII - Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externas à organização.

XXXIV - TLS: acrônimo de *Transport Layer Security.*

XXXV - Usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitado pelo órgão para acessar os seus ativos de informação.

XXXVI - Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO II
DA ESTRUTURA NORMATIVA

Art. 13 A estrutura normativa da Segurança da Informação do IFRS é composta por um conjunto de documentos interdependentes:

I - Política de Segurança da Informação (PSI): define as diretrizes, as competências e as responsabilidades referentes à Segurança da Informação;

II - Normas de Segurança da Informação: estabelecem os conceitos, detalhando os passos a serem executados, e as obrigações a serem observadas para o cumprimento da Política; e

III - Procedimentos de Segurança da Informação: instrumentalizam o disposto nas normas, permitindo sua direta aplicação no âmbito do IFRS.

Parágrafo único. Os documentos mencionados nos incisos II e III serão objeto de elaboração através de normas complementares.

CAPÍTULO III
DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 14 A estrutura de Gestão de Segurança da Informação deverá ser composta por:

I - Alta Administração;

II - Comitê de Segurança da Informação;

III - Gestor de Segurança da Informação;

IV -Gestor de Tecnologia da Informação;

V - Encarregado pelo Tratamento de Dados Pessoais;

VI - Responsável pela Unidade de Controle Interno;

VII - Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e

VIII - Usuários de Informação.

CAPÍTULO IV
DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I
Da Alta Administração

Art. 15 Compete à Alta Administração fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do IFRS, bem como o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados.

Seção II
Do Comitê de Segurança da Informação

Art. 16 Compete ao Comitê de Segurança da Informação:

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 - participar da elaboração da Política de Segurança da Informação (PSI) 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;

V - deliberar sobre normas internas de segurança da informação; e

VI - avaliar as ações propostas pelo gestor de segurança da informação.

Seção III
Do Gestor de Segurança da Informação

Art. 17 Compete ao Gestor de Segurança da Informação:

I - coordenar o Comitê de Segurança da Informação;

II - coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

III - assessorar a Alta Administração na implementação da Política de Segurança da Informação;

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

V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

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

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

VIII - acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Seção IV
Do Gestor de Tecnologia da Informação

Art. 18 Compete ao Gestor de Tecnologia da Informação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação, considerando a cadeia de suprimentos relacionada à solução.

Seção V
Do Encarregado pelo Tratamento dos Dados Pessoais

Art. 19 Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de

agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Seção VI
Do Responsável pela Unidade de Controle Interno

Art. 20 Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Seção VII
Da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos

Art. 21 Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no IFRS;

II - monitorar as redes computacionais;

III - detectar e analisar ataques e intrusões;

IV - tratar incidentes de segurança da informação;

V - identificar vulnerabilidades e artefatos maliciosos;

VI - recuperar sistemas de informação; e

VII - promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação.

Seção VIII
Dos Usuários

Art. 22 Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação do IFRS.

CAPÍTULO V
DIRETRIZES GERAIS

Seção I
Inventário de Ativos

Art. 23 O IFRS deverá registrar, estabelecer e manter um inventário de ativos (*hardware* ou *software*) que possa armazenar ou processar dados. Seus registros devem conter informações precisas e detalhadas dos ativos, possibilitando sua rastreabilidade.

Art. 24 Somente ativos (*hardware* ou *software*) autorizados deverão ser utilizados no ambiente do IFRS.

Art. 25 O IFRS deve garantir que os softwares utilizados em seu ambiente recebam suporte ativo de seus desenvolvedores.

Art. 26 Os *datacenters* da reitoria e das demais unidades integrantes do IFRS devem ser contempladas no mapeamento de ativos.

Art. 27 Os ativos críticos do IFRS (*hardware* ou *software*) devem ser identificados, facilitando a priorização das medidas descritas nesta política.

Seção II
Proteção de Dados

Art. 28 O IFRS deverá criar, estabelecer e manter um processo de gestão de dados que trate dos seguintes aspectos:

I - sensibilidade dos dados;

II - proprietário;

III - manuseio;

IV - limites de retenção; e

V - requisitos de descarte.

Art. 29 O descarte de dados (físico ou lógico) deve ser realizado de forma segura, garantindo que não seja recuperável.

Art. 30 O uso de criptografia para dispositivos de usuários que possuam dados sensíveis e/ou confidenciais deve ser implementado, onde suportado.

Art. 31 Onde suportado, deverá ser utilizada criptografia para dados em trânsito como TLS e SSH.

Seção III
Configuração Segura

Art. 32 O IFRS deve estabelecer e manter configurações seguras nos dispositivos de seu ambiente, utilizando *baselines* ou imagens do sistema pré-configuradas, sem se limitar somente a essas medidas.

Art. 33 Onde suportado, o bloqueio automático de sessões de usuários e ativos deve ser implementado.

Art. 34 O IFRS deve implementar e gerenciar sistemas de *firewall* nos servidores e *hosts* internos.

Art. 35 O IFRS deve configurar seus *firewalls* seguindo o princípio de "bloqueio por padrão", permitindo apenas o tráfego essencial para o funcionamento das operações institucionais.

Art. 36 O gerenciamento dos ativos e *softwares* do IFRS devem ser realizados através de protocolos seguros como, por exemplo, SSH (*Secure Shell*), HTTPS (*Hypertext Transfer Protocol Secure*) e outras soluções similares.

Art. 37 Os usuários com acesso a contas do tipo *root*¸ administrador ou equivalentes devem ser devidamente identificados.

Art. 38 Servidores de DNS confiáveis (controlados pelo IFRS ou acessíveis externamente) devem ser configurados e implementados.

Seção IV
Gestão de Acessos

Art. 39 A concessão de acesso tem por objetivo garantir aos usuários a realização de suas atividades.

Art. 40 O IFRS deverá estabelecer e manter um inventário de todas as contas gerenciadas, devendo incluir contas de usuários e administradores com informações como nome completo, nome de usuário, departamento e demais que facilitem a rastreabilidade.

Art. 41 O IFRS deverá criar, definir e manter um processo de concessão e revogação de acessos.

Art. 42 As contas inativas no ambiente do IFRS devem ser identificadas e desabilitadas.

Art. 43 As senhas utilizadas devem seguir um padrão de robustez e boas práticas de segurança da informação.

Art. 44 Onde houver suporte, o MFA deve ser utilizado.

Art. 45 O compartilhamento de credenciais de acesso dentro do ambiente do IFRS é estritamente proibido.

Art. 46 O usuário é responsável pelas atividades geradas pelas suas credenciais e irá responder por qualquer ação indevida realizada através de seu acesso.

Art. 47 Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Seção V
Gestão de Vulnerabilidades

Art. 48 O IFRS deverá definir e manter um processo de gestão de vulnerabilidades para seus ativos.

Art. 49 O IFRS deverá definir e manter um processo de remediação de vulnerabilidades de acordo com seus riscos.

Art. 50 O IFRS deve realizar a gestão de *patches*, automatizada quando possível, dos sistemas operacionais e aplicações.

Art. 51 O planejamento de atualizações deve considerar o impacto das mudanças, garantindo que *patches* pequenos de segurança e correções de *bugs* sejam aplicados rapidamente, enquanto atualizações maiores, que incluem novas funcionalidades, tenham um prazo adequado para implementação.

Seção VI
Gestão de Registros

Art. 52 O IFRS deve definir e manter um processo de gestão de *logs* para fins de auditoria, considerando questões como coleta, revisão e retenção de logs.

Art. 53 Os *logs* de auditoria devem ser armazenados de forma segura, garantindo sua integridade.

Art. 54 A sincronização de tempo dos sistemas e dispositivos devem ser padronizados.

Seção VII
Proteções de Correio Eletrônico e *Web*

Art. 55 O uso de navegadores e mensageiros eletrônicos atualizados e com suporte ativo deve ser adotado em todo o ambiente institucional.

Art. 56 A implementação de serviços de filtragem para restringir o acesso a sites potencialmente mal-intencionados ou não essenciais às funções internas deve abranger todos os ativos compatíveis.

Seção VIII
Defesas Contra *Malware*

Art. 57 Soluções *anti-malware* devem ser utilizadas, onde houver suporte, em todo o ambiente do IFRS.

Art. 58 A execução e reprodução automática para mídias removíveis deve ser desabilitada.

Seção IX
Backups

Art. 59 O IFRS deverá criar, estabelecer e manter um processo de *backup* e recuperação de dados.

Art. 60 Os *backups* devem ser realizados de forma automatizada, levando em consideração a criticidade dos sistemas e dados.

Art. 61 O IFRS deverá estabelecer e implementar meios para proteção dos dados de recuperação como, por exemplo, criptografia.

Art. 62 Os dados de recuperação devem ser alocados em uma instância isolada.

Seção X
Gestão de Rede

Art. 63 A infraestrutura de rede deverá ser atualizada periodicamente, garantindo o uso de versões estáveis em seus componentes. Deverão ser implementadas medidas que assegurem a proteção, a eficiência e a rastreabilidade dos ambientes de rede, bem como o registro e a revisão periódica das alterações de configuração, de modo a manter a segurança e a conformidade com as normas de segurança da informação.

Seção XI
Treinamento e Conscientização

Art. 64 O IFRS deverá definir e executar um programa de conscientização e treinamentos em segurança da informação, promovendo conhecimentos sobre engenharia social, práticas de autenticação, práticas de tratamento de dados e outros aspectos relevantes.

Art. 65 O conteúdo do programa de conscientização e treinamentos deve ser periodicamente revisado, adequando-se às necessidades atuais.

Seção XII
Segurança de Aplicações

Art. 66 O desenvolvimento de aplicações no ambiente do IFRS deve ser realizado considerando as melhores práticas de segurança, garantindo a proteção de dados, a mitigação de vulnerabilidades e a conformidade com normas e regulamentos aplicáveis.

Art. 67 As aplicações desenvolvidas em ambiente interno do IFRS devem ser testadas em ambiente de homologação antes de entrarem em produção.

Seção XIII
Resposta à Incidentes

Art. 68 O IFRS deverá instituir uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 69 Esta Política de Segurança da Informação pode ser revisada a qualquer tempo, observando-se o prazo máximo de 04 (quatro) anos.

Art. 70 O não cumprimento de qualquer diretriz desta política poderá ocasionar medidas administrativas, suspensão de acesso e/ou sanções legais. As penalidades impostas visam garantir a segurança da informação do IFRS.

Art. 71 A implementação das diretrizes dispostas nesta política dependerá da disponibilidade de recursos financeiros, humanos e tecnológicos do IFRS.

Art. 72 Os sistemas legados incapazes de implementar as ações previstas neste normativo deverão ser identificados, por meio do inventário de ativos, juntamente aos seus riscos e justificativas, a fim de que sejam adotadas medidas para mitigar tais riscos.

Art. 73 A periodicidade para atualização e revisão das ações previstas nas diretrizes desta política deverá ser definida por meio de normativo interno, especificando os casos individualmente.

Art. 74 Os editais de licitação, contratos, convênios, acordos e demais instrumentos de cooperação técnica com entidades prestadoras de serviços para o IFRS devem conter uma cláusula específica sobre a obrigatoriedade de cumprimento desta PSI, além da exigência de assinatura do Termo de Responsabilidade pela entidade contratada.

CAPÍTULO VII
DAS REFERÊNCIAS NORMATIVAS

Art. 75 Esta PSI está alinhada aos instrumentos normativos apresentados a seguir:

I - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2022. Segurança da Informação, segurança cibernética e proteção à privacidade. Sistemas de gestão da segurança da informação. Requisitos. ABNT: Rio de Janeiro, 2022.

II - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2022. Segurança da Informação, segurança cibernética e proteção à privacidade. Controles de segurança da informação. ABNT: Rio de Janeiro, 2022.

III - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005:2023. Segurança da Informação, segurança cibernética e proteção à privacidade. Orientações para gestão de riscos de segurança da informação. ABNT: Rio de Janeiro, 2023.

IV - BRASIL. Casa Civil. Instituto Nacional de Tecnologia da Informação. Instrução Normativa n. 07, de 29 de maio de 2020. Altera o tempo de armazenamento dos logs, trilhas de auditorias e imagens. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/instrucoes-normativas/sei_iti_-_0427993_-_instrucao_normativa_07_2020.pdf Acesso em: 24 abr. 2025.

V - BRASIL. Decreto n. 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm Acesso em: 24 abr. 2025.

VI - BRASIL. Decreto 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. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7845.htm Acesso em: 24 abr. 2025.

VII - BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 24 abr. 2025.

VIII - BRASIL. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR n. 01 de 27 de maio de 2020. Dispõe sobre a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN01_consolidada.pdf Acesso em: 24 abr. 2025.

IX - BRASIL. Gabinete de Segurança Institucional. Portaria GSI/PR n. 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370 Acesso em: 24 abr. 2025.

X - BRASIL. Gabinete de Segurança Institucional. Portaria GSI/PR n. 120, de 21 de dezembro de 2022. Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf Acesso em: 24 abr. 2025.

XI - BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI). Disponível em: https://www.gov.br/funai/pt-br/centrais-de-conteudo/publicacoes/relatorios/legislacao-de-ouvidoria/l-f-portaria_sgd_mgi_852_28-3-2023_ppsi.pdf Acesso em: 24 abr. 2025.

XII - BRASIL. Ministério da Economia/Secretaria de Governo Digital. Portaria SGD/ME nº 778, de 4 de abril de 2019. Estabelece as competências do gestor de tecnologia da informação no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/portaria-sgd-me-no-778-de-4-de-abril-de-2019 Acesso em: 22 abr. 2025.

Emitido em 19/08/2025

ANEXO DE RESOLUÇÃO Nº 40/2025 - CONSUP-REI (11.01.01.01.05)
(Nº do Documento: 18)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 27/08/2025 16:10)
JULIO XANDRO HECK
REITOR
IFRS / REI (11.01.01)
Matrícula: ###427#7

Para verificar a autenticidade deste documento entre em https://sig.ifrs.edu.br/documentos/ informando seu número: **18**, ano: **2025**, tipo: **ANEXO DE RESOLUÇÃO**, data de emissão: **27/08/2025** e o código de verificação: **20ced9a72c**