Política de Segurança da Informação e Comunicação
Instituto Federal de Brasília

PoSIC

Brasília-DF, Abril de 2025

Dispõe sobre a 2º revisão da Política de Segurança da Informação e Comunicação do Instituto Federal de Brasília.

INTRODUÇÃO

Este documento institui a Política de Segurança da Informação e das Comunicações e se aplica a todas as unidades regimentais do Instituto Federal de Brasília, a qual deverá ser adotada e cumprida por todos os servidores, colaboradores, consultores externos, estagiários, alunos e prestadores de serviço que exerçam atividades, ou quem tenha acesso a dados ou informações no ambiente do IFB.

CAPÍTULO I
DO ESCOPO

Art. 1°. A Política de Segurança da Informação e das Comunicações (PoSIC) do Instituto Federal de Educação, Ciência e Tecnologia de Brasília – IFB, tem por objetivo estabelecer diretrizes, normas, procedimentos, responsabilidades e práticas para a proteção das informações da instituição visando a continuidade dos processos institucionais críticos e à manutenção do bom uso da informação em todos os seus aspectos, possibilitado o gerenciamento da segurança de informação.

Art. 2°. A PoSIC está alinhada às estratégias do Instituto Federal de Educação, Ciência e Tecnologia de Brasília (IFB), visando garantir os princípios da confidencialidade, a integridade, a disponibilidade, a autenticidade, e irretratabilidade e a conformidade das informações produzidas ou sob sua custódia.

Art. 3°. A PoSIC deve atender aos preceitos constitucionais, ao arcabouço legal vigente, aos documentos normativos e administrativos que regem a Administração Pública Federal, bem como estar em conformidade com requisitos regulamentares e contratuais, valores éticos, assegurando o uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo único. A informação de que trata o caput será tratada independentemente de onde ela esteja, residente em memória de máquinas e dispositivos, armazenada em mídias de disco, em trânsito ou impressas em documentos e outros meios analógicos ou digitais, salvaguardando a exatidão e a integridade dos métodos de processamento e garantindo que a comunidade obtenha acesso à informação e aos ativos correspondentes sempre que for preciso e de acordo com a necessidade de conhecer e de agir de cada pessoa ou entidade, consoante com os interesses do IFB.

Art. 4°. A Gestão da Segurança da Informação - GSI deve apoiar e orientar a tomada de decisões institucionais, dirimir conflitos e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação.

CAPÍTULO II
TERMOS E DEFINIÇÕES

Art. 5°. Para efeitos desta Política, das normas e procedimentos de Segurança da Informação criados para o âmbito do IFB, serão adotados os termos e definições descritos no Anexo I.

CAPÍTULO III
CONFORMIDADE

Art. 6°. A legislação adotada nesta PoSIC está elencada no Anexo II para fins de consulta.

CAPÍTULO IV
ESTRUTURA NORMATIVA

Art. 7°. A estrutura normativa da Segurança da Informação do IFB é composta por um conjunto de documentos interdependentes:
I. Política de Segurança da Informação: define os princípios, 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;
III. Planos de Segurança da Informação: instrumentalizam o disposto nas normas, permitindo sua direta aplicação no âmbito do IFB. I
V. Programa de Gestão de Continuidade de Negócio: conjunto de informações e instruções detalhadas para a prevenção, tratamento e retorno das atividades normais em caso de ocorrência de incidentes e eventos, conforme os riscos avaliados. O Programa é constituído por:

Planos de Gerenciamento de Incidente — contêm informações de contato da equipe técnica que tratará o incidente bem como instruções gerais da prevenção, tratamento e procedimentos após retorno;

Plano de Gestão de Riscos — identifica, avalia e define ações para mitigar ou eliminar os riscos que podem impactar a segurança da informação na instituição, sendo descritos os procedimentos para monitorar, responder e controlar os riscos, além de priorizá-los com base na probabilidade de ocorrência e no impacto potencial.

Planos de Continuidade de Negócio — contém informações de contato dos responsáveis pelo remanejo de ativos e recursos necessários para continuar as atividades durante a contingência, bem como instruções gerais do preparo, do remanejo de ativos e recursos e dos procedimentos de retorno às atividades normais.

CAPÍTULO V
DAS DIRETRIZES

Seção I
Das Disposições Gerais

Art. 8°. O cumprimento desta política de segurança e os documentos delas advindos deverão ser avaliados periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Governança Digital (CGD), buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 9°. O CGD deve priorizar as ações de investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias do IFB e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 10. O CGD deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 11. O IFB, além das diretrizes estabelecidas nesta PoSIC deve também se orientar pelas melhores práticas e procedimentos de SIC, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 12. É vedado comprometer a integridade, a confidencialidade, a disponibilidade, a autenticidade, e irretratabilidade e a conformidade das informações criadas, manuseadas, armazenadas, transportadas ou custodiadas pelo IFB.

Art. 13. Os contratos firmados pelo IFB devem conter cláusulas que determinem a observância da PoSIC e seus respectivos documentos.

Art. 14. Serão elaboradas normas complementares para esse documento.

Art. 15. As diretrizes e princípios de segurança da informação descritas nesta Política devem ser observadas por todos da comunidade que executem atividades direta ou indiretamente relacionadas ao IFB durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 16. O IFB deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando as legislações em vigor.

Seção II
Da Abrangência

Art. 17. Esta Política se aplica a todas as áreas do IFB e comunidade em contato com qualquer informação de propriedade ou custódia do IFB que incluem:
I - Reitoria (considerando o endereço e qualquer pessoa localizada neste endereço, incluindo núcleos remotos diretamente subordinados, sendo servidor ou discente do IFB ou não);
II - Campus (inclusive campus em construção ou de projeção futura, considerando o endereço e qualquer pessoa localizada neste endereço, sendo servidor ou discente do IFB ou não);
III - Representantes de entidades externas (Participantes do Conselho Superior ou que recebem ou produzem informações de propriedade ou de custódia do IFB);
IV - Fornecedores e Prestadores de serviço (limitado aos endereços e informações do IFB);
V - Qualquer pessoa natural ou pessoa jurídica de direito público ou privado que obtiver contato com qualquer informação de propriedade ou de custódia do IFB ou na iminência de ter contato.

Parágrafo único: Todos são responsáveis e devem estar comprometidos com a segurança da informação.

Art. 18. A PoSIC/IFB e as suas normas devem ser divulgadas a toda comunidade do IFB e dispostas de maneira que seus conteúdos possam ser consultados a qualquer momento.

Art. 19. Os contratos, convênios, acordos e outros instrumentos semelhantes celebrados com o IFB devem atender à PoSIC/IFB.

Art. 20. Esta política também se aplica, no que couber, ao relacionamento do IFB com outros órgãos e entidades públicas ou privadas.

Seção III
Das Instâncias

Art. 21. O Comitê de Governança Digital (CGD), antigo Comitê Gestor de Tecnologia da Informação (CGTI), instituído pela Portaria IFB nº 2 de maio de 2016, é uma instância de natureza consultiva e propositiva, de caráter permanente, vinculado à Reitoria, que determina as prioridades dos programas de investimentos em Tecnologia da Informação (TIC), às estratégias de TIC e aprova as políticas de segurança da informação e comunicações do Instituto;

Art. 22. São instâncias de implementação, fiscalização e atualização desta PoSIC:
I – O Comitê de Governança Digital (CGD);
II – Diretoria de Tecnologia da Informação e Comunicação (DTIC): instância administrativa/ executiva responsável por propor as políticas e programas do IFB na área de informática e telecomunicações, bem como por sua implementação e gestão;
III – Equipe de Prevenção Tratamento de Incidentes de Redes de Computadores (ETIR): instância a ser instituída, responsável a dar tratamento de primeiro nível aos incidentes de segurança da informação;

IV - Gestor de Segurança da Informação: servidor responsável pelas ações de segurança da informação no âmbito do IFB;
V – Unidade Administrativa: qualquer instância administrativa do IFB a exemplo dos Campi, unidades ligadas aos Campi, núcleos de pesquisa e centros com funcionalidades específicas.

Seção IV
Do Tratamento da Informação

Art. 23. Todo ativo de informação criado, adquirido ou custodiado pelo agente público, no exercício de suas atividades, é considerado um bem e deve ser protegido de acordo com as regulamentações de segurança existentes com o objetivo de minimizar riscos às atividades e serviços prestados pelo IFB, preservando sua imagem.

Art. 24. O tratamento das informações pessoais deve considerar o respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, conforme o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), normativos internos e legislações aplicáveis.

Art.25. As informações produzidas ou custodiadas pelo IFB devem ser descartadas conforme o seu nível de classificação.

Seção V
Da Classificação da Informação

Art. 26. As informações custodiadas ou de propriedade do IFB devem ser classificadas levando-se em consideração seu valor, criticidade, sensibilidade e requisitos legais e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.

Art. 27. O proprietário da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade conforme as orientações a serem definidas em norma complementar ou, se não houver, seguir o que estabelece o Conarq.

Art. 28. A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Seção VI
Da Sensibilização, Conscientização e Capacitação

Art. 29. O IFB desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação.

Seção VII
Da Gestão dos Ativos de Informação

Art. 30. O custodiante do ativo de informação deve ser o responsável pelo armazenamento, operação, administração, preservação e possível descarte do ativo de informação.

Art. 31. Os bens ativos de informação devem:
I – Ser inventariados e protegidos;
II – Ser identificados os seus proprietários e custodiantes;
III – Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
IV – Ter a sua entrada e saída nas dependências do IFB autorizadas e registradas por autoridade competente;
V – Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;
VI – Ser regulamentados por norma específica quanto a sua utilização; e
VII – Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares.

Art. 32. O proprietário do ativo de informação deve criar e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 33. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 34. Os sistemas de informação e os aplicativos do IFB devem ser protegidos contra ataques ou ameaças, indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 35. O acesso dos usuários externos aos ativos de informação (bem patrimonial) e sua utilização, quando autorizados, deve ser condicionado à ciência e ao aceite do responsável, conforme dita esta PoSIC.

Seção VIII
Da Aquisição, Do Desenvolvimento e Da Manutenção de Sistemas

Art. 36. O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Art. 37. O IFB deve, em norma específica, estabelecer critérios e metodologias de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades e manutenção.

Art. 38. Apenas pessoas autorizadas pela DTIC devem ter acesso ao ambiente de desenvolvimento, testes e produção, aos códigos-fonte e dados dos sistemas de informação do IFB.

Parágrafo único: Os ambientes de desenvolvimento, testes e produção devem ser segregados para prevenir acessos não autorizados e reduzir riscos.

Art. 39. Toda modificação ou atualização em sistemas de informação do IFB devem ser documentadas e aprovadas antes de serem implementadas.

Seção IX
Do Plano de Investimento em SIC

Art. 40. Os investimentos em segurança da informação serão realizados de forma planejada e consolidados em um plano de investimento registrado no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).

Art. 41. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco, e será submetido ao CGD.

Seção X
Da Propriedade Intelectual

Art. 42. Na condição de propriedade intelectual, protegida por lei, nenhum aplicativo poderá ser utilizado no IFB sem a devida aquisição da licença de uso.

Parágrafo único: A gestão das licenças de uso dos aplicativos será de responsabilidade do gestor de cada unidade administrativa.

Seção XI
Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 43. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC.

Art. 44. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no IFB.

Art. 45. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 46. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

Seção XII
Da Gestão de Descarte

Art. 47. Nenhuma mídia armazenadora de dados deve ser descartada sem o devido tratamento, objetivando a segurança das informações nela contidas.

Parágrafo único: Entende-se por mídia qualquer dispositivo físico capaz de armazenar dados, a exemplo de mídias magnéticas, ópticas, eletrônicas e papel.

Art. 48. Caberá à Política de Descarte a ser estabelecida no IFB definir, em função da criticidade da informação, o tempo para destruição física da mídia e para o seu armazenamento e reaproveitamento.

Seção XIII
Do Tratamento de Incidentes de Rede

Art. 49. O IFB deverá constituir a ETIR.

§ 1º Na constituição da ETIR, o IFB deverá definir o modelo de implantação que melhor se adequar às necessidades e limitações da instituição, dentre os especificados na Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009, e observar as diretrizes nela estabelecidas e nas demais normas relacionadas ao tema.

§ 2º A ETIR deverá possuir um regimento interno próprio e que deverá ser referendado pelo CGD.

§ 3º Gestor de Segurança da Informação, servidor responsável pelas ações de segurança da informação no âmbito do IFB deverá presidir a ETIR.

§ 4º O Gestor de Segurança da Informação terá, dentre outras atribuições, a de ser a conexão com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.

Art. 50. A ETIR deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo do CTIR gov.

Seção XIV
Da Gestão de Riscos

Art. 51. O IFB deve estabelecer processos de Gestão de Riscos de Segurança da Informação - GRSI que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.

Art. 52. A GRSI é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação, levando em consideração o planejamento, a execução, análise crítica e melhoria da SIC no IFB.

Art. 53. As proteções devem estar alinhadas aos riscos identificados.

Art. 54. A gestão de riscos de TI deve avaliar os riscos relativos à segurança dos ativos de informação e à conformidade com exigências regulatórias ou legais.

Seção XV
Da Gestão de Continuidade de Negócio

Art. 55. O IFB deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

Art. 56. As ações de continuidade do IFB devem ser adotadas por todos os titulares de unidade administrativa, de forma a proteger a reputação e a imagem institucional.

Art. 57. As informações de propriedade ou custodiadas pelo IFB, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades do órgão. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservam sua integridade, conforme o nível de classificação atribuído.

Seção XVI
Da Auditoria e Conformidade

Art. 58. Deve ser realizada, com periodicidade não superior a 4 (quatro) anos, a verificação de conformidade das práticas de SI do IFB desta PoSIC e de suas normas e procedimentos complementares, bem como com a legislação específica de SI.

Art. 59. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados pelo IFB.

Art. 60. A verificação de conformidade será realizada de forma planejada, mediante calendário de ações proposto pelo CGD.

Art. 61. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos percebidos.

Art. 62. Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SI por período superior a 4 (quatro) anos.

Art. 63. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 64. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

Seção XVII
Dos Controles de Acesso

Art. 65. O IFB deve sistematizar a concessão de acesso como forma de evitar a quebra de segurança da informação.

Art. 66. O acesso às informações custodiadas ou de propriedade do IFB pelos agentes públicos deve ser restrito ao necessário para o desempenho de suas funções.

Art. 67. O acesso físico às instalações do IFB deverá ser regulamentado com o objetivo de garantir a segurança dos agentes públicos e a proteção dos seus ativos.

Seção XVIII
Do Uso de Recursos Computacionais

Art. 68. O uso de recursos computacionais do IFB pelos agentes públicos deve ser direcionado exclusivamente para realização das atividades profissionais desempenhadas pelo órgão no limite dos princípios da ética, razoabilidade e legalidade.

Art. 69. Não é permitida a utilização de programas que violem direitos autorais, conforme legislação em vigor.

Parágrafo Único: Demais questões acerca do uso de recursos computacionais serão tratados em norma complementar específica.

Seção XIX
Das Normas Específicas de Segurança

Art. 70. Os aspectos de segurança física e do ambiente (controles de acesso), lógica (uso de e-mail, internet) e de recursos humanos, serão tratados em documentos independentes, a fim de complementar com maior especificidade e detalhamento as normas e recomendações de segurança no trato das informações.

Parágrafo único: Todos os procedimentos relacionados à segurança da informação, definidos em instruções específicas, devem estar de acordo com esta Política, e uma vez divulgados, passam a ser parte integrante desta.

Art. 71. Deverá ser estabelecido por procedimento específico o descarte seguro de mídias de armazenamento de dados, visando assegurar a remoção de dados sensíveis.

Art. 72. Devem ser previstos procedimentos que visem resguardar o acesso não autorizado a informações e dados pessoais que estejam em meio físico ou digital, adotando políticas de segurança sempre que possível.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 73. É dever do agente público do IFB conhecer e zelar pelo cumprimento da PoSIC.

Art. 74. Os agentes públicos são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como crachá, *login*, senha eletrônica, certificado digital e endereço de correio eletrônico.

Parágrafo único: A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

Art. 75. Cabe a Alta Gestão do IFB
I – Comprometer-se em proteger todos os ativos de informação da instituição;
II – Formalizar esta PoSIC;
III – Garantir a provisão dos recursos necessários para a implementação da PoSIC no IFB;
IV – Promover no IFB a cultura de segurança da informação, por meio de atividades de sensibilização, conscientização, capacitação e especialização.
V – Constituir grupo de trabalho para realizar auditoria de segurança da informação;

Art. 76. Cabe ao CGD
I – Aprovar a Política de Segurança da Informação Comunicação;
II – Aprovar as normas específicas de Segurança da Informação Comunicação;
III – Desempenhar as atividades determinadas em Normas e Regulamentos ao Comitê Gestor de Segurança da Informação e Comunicação- CGSIC;
IV – Exercer outras atribuições que lhes forem atribuídas em regimento interno.

Art. 77. Cabe ao CGD como instância de Segurança da Informação e Comunicação
I – Desenvolver a cultura de segurança da informação e das comunicações na Instituição;
II – Coordenar as ações de segurança da informação;
III – Propor, aprovar e publicar normas e procedimentos complementares à PoSIC;
IV – Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIC;
V – Avaliar criticamente a PoSIC, visando a sua aderência aos objetivos institucionais do IFB e à legislação vigente, e propor sua revisão, quando necessário;
VI – Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
VII – Receber e consolidar os resultados dos trabalhos de auditoria de segurança da informação e remetê-los à Reitoria;
VIII – Responder às demandas dos órgãos de controle quando referentes à segurança da informação no IFB;
IX – Realizar e/ou acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;
X – Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação;
XI – Propor ações de investimentos em segurança da informação do IFB;
XII– Assegurar que as áreas finalísticas desenvolvam seu Plano de Continuidade de Negócios para o IFB, dentro de sua área de competência;

XIII – Assessorar a Reitoria nos assuntos relativos à segurança da informação.

Art. 78. Cabe ao Gestor de Segurança da Informação

I - Receber informações sobre incidentes de segurança;

II - Coordenar a resposta a incidentes de segurança;

III - Preparar evidências para ações legais decorrentes de um incidente;

IV - Analisar incidentes de forma a prevenir sua recorrência;

V - Promover a cultura de SI, juntamente com as instâncias superiores;

VI - Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

VII - Propor a alocação de recursos materiais e humanos necessários à realização de ações de SI e a plena consecução da PoSIC e suas normas complementares;

VIII - Presidir e coordenar as ações da ETIR;

IX - Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI;

X - Propor Normas Técnicas relativas à SI;

XI – Indicar representantes para participar de fóruns de debates com instituições que desenvolvam projetos de pesquisa ou estudos sobre segurança da informação e da comunicação;

XII - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

XIII - assessorar a alta administração na implementação da Política de Segurança da Informação;

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

XV - 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 ou na entidade;

XVI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

XVII - propor recursos necessários às ações de segurança;

XVIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

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

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

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

Art. 79. Cabe à ETIR:

I – Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II – Auxiliar na recuperação de sistemas;

III – Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SI e avaliando condições de segurança de redes por meio de verificações de conformidade;

IV – Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V – Analisar ataques e intrusões na rede do IFB;

VI – Executar as ações necessárias para tratar quebras de segurança;
VII – Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
VIII – Cooperar com outras equipes de Tratamento e Resposta a Incidentes;
IX – Participar de atividades de formação, tais como fóruns, redes nacionais e internacionais relativas à SI;

Art. 80. Cabe ao Gestor do Ativo de Informação
I – Promover a segurança dos ativos de informação sob sua responsabilidade;
II – Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PoSIC;
III – Conceder e revogar acessos aos ativos de informação;
IV – Comunicar à ETIR a ocorrência de incidentes de SI;
V – Designar custodiante dos ativos de informação, quando aplicável;
VI - Realizar o tratamento e a classificação da informação.

Art. 81. Cabe ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso de execução/alteração, de acordo com os requisitos definidos pelo gestor da informação e em conformidade com esta PoSIC.

Parágrafo único: O acesso de leitura às informações obedecerá ao disposto na Lei de Acesso à Informação Pública (Lei nº 12.527/2012).

Art. 82. Cabe ao titular da Unidade Administrativa
I – Corresponsabilizar com a ETIR pelo monitoramento e orientações relativas à medidas de segurança da informação em sua unidade;
II – Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SI;
III – Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SI;
IV – Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SI por parte dos usuários sob sua supervisão;
V – Autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;
VI – Comunicar à ETIR os casos de quebra de segurança; e
VII – Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 83. Cabe ao Encarregado pelo Tratamento de Dados Pessoais:
I - conduzir o diagnóstico de privacidade,
II - 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.

Art. 84. Cabem aos terceiros e fornecedores, conforme previsto em contrato:
I – Tomar conhecimento desta PoSIC;
II – Fornecer listas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;

III – Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

Art. 85. Cabem aos usuários:
I – Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PoSIC, bem como os demais normativos e resoluções relacionados à SI;
II – Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação;
III – Comunicar os incidentes que afetam a segurança dos ativos de informação ao ETIR ou ao responsável direto/chefia imediata.

CAPÍTULO VII
DA ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 86. O Comitê de Governança Digital fará a vez do Comitê de Gestor de Segurança da Informação e Comunicação - CGSIC, com as seguintes competências:
I – Assessorar na implementação das ações de segurança da informação no Instituto;
II – Constituir grupos de trabalho para tratar temas e propor soluções específicas sobre segurança da Informação; e
III – Propor Normas e Procedimentos internos relativos à segurança da informação, em conformidade com a legislação existente sobre o tema.

Art. 87. Fica instituído, no âmbito do IFB o Gestor de Segurança da Informação, com as seguintes competências:
I – Promover cultura de segurança da informação;
II – Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III – Propor recursos necessários às ações de segurança da informação;
IV – Coordenar a equipe de tratamento e resposta a incidentes em redes computacionais;
V – Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;
VI – Manter contato direto com o Departamento de Segurança da Informação (DSI) do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação; e
VII – Propor normas relativas à segurança da informação.

Parágrafo único: O gestor de segurança da informação será designado em expediente próprio e deverá reportar-se sempre ao Comitê de Segurança da Informação.

CAPÍTULO VIII
DAS PENALIDADES

Art. 88. Nos casos em que houver o descumprimento ou violação de um ou mais itens da PoSIC ou de suas Normas, procedimentos ou atividades pertinentes à Segurança da Informação, estes serão tratados conforme legislação vigente e/ou normativos específicos.

CAPÍTULO IX
DA ATUALIZAÇÃO

Art. 89. A PoSIC e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 4 (quatro) anos.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 90. A presente Política deve ser lida em conjunto com as obrigações previstas na Política de Proteção de Dados Pessoais do IFB, nas normativas internas e documentos correlatos ao tema.

Art. 91. Os casos omissos serão resolvidos pelo Comitê de Governança Digital (CGD).

CAPÍTULO XI
DA DIVULGAÇÃO

Art. 92. A PoSIC e suas atualizações, bem como as normas complementares, devem ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados que habitualmente trabalham no IFB.

CAPÍTULO XII
DA VIGÊNCIA

Art. 93. Esta Portaria Normativa entra em vigor na data de sua assinatura.

ANEXO I

TERMOS E DEFINIÇÕES

Para fins desta Portaria Normativa, entende-se por:

I - **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II – **Agente público:** aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao IFB;

III – **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição [ISO/IEC 13335-1:2004];

IV - **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco;

V - **Ativo**: qualquer coisa que tenha valor para a organização;

VI - **Ativo de informação**: qualquer componente (humano, tecnológico, físico, ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como locais onde se encontram esses meios e as pessoas que a eles tem acesso;

VII - **Ativo de informação classificada**: ativo de informação com informação classificada;

VIII **Auditabilidade**: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;

IX - **Auditoria**: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões.

X - **Auditoria em Segurança da Informação:** processo de avaliação da situação atual dos controles de segurança da informação implementados;

XI - **Autenticidade**: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

XII **Avaliação de Risco**: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

XIII **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;

XIV **- Contingência:** indisponibilidade ou perda de integridade da informação que os controles de segurança não tenham conseguido evitar;

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

XVI - **Controle:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também é usado como sinônimo para proteção ou contramedida;

XVII - **Custodiante do ativo**: unidade administrativa responsável pelo armazenamento, operação, administração e preservação de ativos, mesmo que transitória.

XVIII - **Custodiante da informação**: colaborador responsável pela guarda adequada do dado;

XIX - **Dado:** representação de uma determinada situação ou evento em determinado espaço e tempo, sob uma forma apropriada ao armazenamento, processamento ou transmissão, não fornecendo julgamento nem interpretação para a tomada de decisões;

XX - **Dado Pessoal**: informação relacionada a pessoa natural identificada ou identificável;

XXI - **Dado Pessoal Sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XXII - **Desastre**: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período superior ao tempo objetivo da recuperação;

XXIII - **Dispositivo ou recurso de tecnologia da informação e comunicações (TIC):** todo e qualquer equipamento que permita a armazenagem e/ou veiculação de informações ou dados, por qualquer processo, seja ele óptico, gráfico, magnético, eletrônico ou outros;

XXIV - **Documento:** toda a base de conhecimento, fixada materialmente, suscetível de ser utilizada para consulta, estudo ou prova;
Documento de domínio público: documento ou obra (artística, invenção desenho industrial, etc.) que pode ser livremente reproduzido, apresentado ou explorado sem necessidade de autorização ou pagamento de direitos autorais por esgotamento do prazo previsto em lei ou por outro motivo que tenha feito expirar a propriedade intelectual;

XXV - **Documento de natureza pública**: documento relativo ou pertencente à coletividade, de uso comum a todos, universalmente, conhecido ou sem restrição de acesso a qualquer pessoa;

XXVI – **Evento de segurança da informação:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de

controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação [ISO/IEC TR 18044:2004];

XXVII – **Gestor:** agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas do uso da informação;

XXVIII - **Gestão Arquivística de Documentos**: conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente intermediária, visando sua eliminação ou recolhimento para guarda permanente.

XXIX – **Incidente:** é indicado por um simples ou por uma série de eventos de Segurança da Informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação;

XXX - **Incidente de segurança da informação**: um simples ou uma série de eventos de segurança da informação, indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XXXI – **Informação:** dados e fatos dotados de relevância e propósito que foram organizados e comunicados de forma coerente e com significado e a partir dos quais se podem tirar conclusões e interpretações;

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

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

XXXIV - **Não-repúdio**: propriedade da informação que não possa ter seu envio ou contestados, rejeitados ou repudiados por seu emissor ou por seu receptor;

XXXV - **Plano de incidente e tratamento de resposta**: conjunto de ações claramente definidas e documentadas para serem usadas quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

XXXVI - **Plano de continuidade de negócios:** conjunto de procedimentos que devem ser adotados quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços;

XXXVII **- Plano de incidente e tratamento de resposta:** conjunto de ações claramente definidas e documentadas, para serem usadas quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

XXXVIII – **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e das Comunicações;

XXXIX - **Risco:** combinação da probabilidade de ocorrência de um evento e de suas consequências;

XL - **Rótulo**: identificação física ou eletrônica da classificação atribuída à informação;

XLI - **Segurança da informação:** preservação da confidencialidade, da integridade e da disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também estão envolvidas;

XLII - **Segurança institucional:** conjunto de ações integradas destinadas à proteção de pessoas, processos de negócio e ativos da Instituição;

XLIII - **SI:** Segurança da Informação;

XLIV - **Titular do dado**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XLV - **Tratamento da informação:** recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XLVI - **Usuário externo:** qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao IFB;

XLVII - **Usuário interno:** qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente ao IFB;

XLVIII - **Verificação de conformidade em segurança da informação**: procedimentos que fazem parte da avaliação de conformidade que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação da Instituição;

XLIX – **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

ANEXO II

REFERÊNCIAS LEGAIS E NORMATIVAS

As referências legais e normativas utilizadas para a elaboração da PoSIC são:

I – Constituição Federal de 1988, reformada em 2008;

II – Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

III – Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

IV – Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

V - Decreto nº 10.641, de 2 de março de 2021, altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

VI - Decreto nº 7.845, de 14 de novembro de 2012, que 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; (duplicada)

VII – Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores – Internet;

VIII – Lei nº 9.610, de 19 de fevereiro de 1998, altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências;

IX – Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

X - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

XI - Decreto nº 8.539, de 8 de outubro de 2015, que dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

XII – Norma Complementar no 03/IN01/DSIC/GSI/PR, de 03 de julho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta;

XIII – Norma ABNT NBR ISO/IEC 27001:2006 – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;

XIV – Norma ABNT NBR ISO/IEC 27002:2013 – Técnicas de segurança - Código de práticas para a segurança da informação;

XV - Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 de outubro de 2008, que estabelece a Metodologia de Gestão de Segurança da Informação e Comunicações;

XVI - Norma Complementar nº 04/IN01/DSIC/GSIPR, de 25 de fevereiro de 2013, que estabelece Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;

XVII - Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;
XVIII - Norma Complementar nº 06/IN01/DSIC/GSIPR, de 23 de novembro de 2009, que estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
XIX - Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;
XX - Norma Complementar nº 10/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
XXI - Norma Complementar nº 11/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, que estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;
XXII – Decreto nº 7.845, de 14 de novembro de 2012, que 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;
XXIII – Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
XXIV – Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12965 de 2014;
XXV - Lei Nº 13.853, de 8 de julho de 2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências;
XXVI – Decreto nº 9.637, de 26 de dezembro de 2018, que 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;
XXVII - Portaria Normativa nº 003, de 30 de março de 2012, que normatiza o uso do correio eletrônico institucional em atendimento à Resolução nº 34/2011 - CS/IFB.
XXVIII - Portaria 3/2024 - RIFB/IFBRASILIA, DE 15 de abril de 2024, que altera o Regimento Interno do Comitê de Governança Digital, no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Brasília - IFB.

Documento Digitalizado Público

2º Revisão da Política de Segurança da Informação e Comunicação - PoSIC

Assunto: 2º Revisão da Política de Segurança da Informação e Comunicação - PoSIC
Assinado por: Luciana Matos
Tipo do Documento: Regulamento
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original

Documento assinado eletronicamente por:

- **Luciana Bastos Matos**, **TECNICO EM ASSUNTOS EDUCACIONAIS**, em 11/04/2025 15:54:52.

Este documento foi armazenado no SUAP em 11/04/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 695473
Código de Autenticação: 3dbde98868