MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

PORTARIA 1/2021 - CGTI/REITORIA/IFPB, de 29 de junho de 2021.

O REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA , nomeado pelo Decreto Presidencial de 22-10-2018, publicado no Diário Oficial da União em 23-10-2018, no uso de suas atribuições legais, e:

CONSIDERANDO a INSTRUÇÃO NORMATIVA 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, e o disposto em seu Art. 9º:

É obrigatório a todos os órgãos e as entidades da administração pública federal possuir uma Política de Segurança da Informação, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

RESOLVE:

Art. 1º Aprovar a nova Política de Segurança da Informação - POSIN, elaborada pela Comissão de revisão da atual Política de Segurança da Informação e Comunicações - POSIN - Processo n° 23381.004741.2020-80, conforme PORTARIA 967/2020 - REITORIA/IFPB, e apreciada pelo Comitê de Governança Digital - CGD - em reunião virtual realizada em 26/11/2020, conforme Ata publicada no portal da TI do IFPB, opção Documentos/Atas.

Art. 2º Esta portaria entra em vigor a partir desta data, revogadas as disposições em contrário.

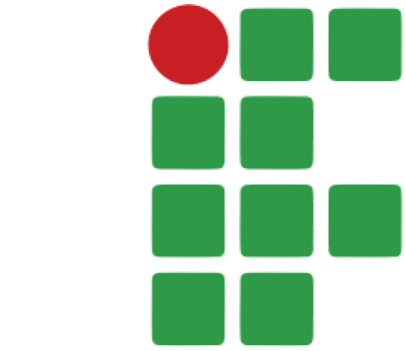
CÍCERO NICÁCIO DO NASCIMENTO LOPES
Reitor

Documento assinado eletronicamente por:

- **Cicero Nicacio do Nascimento Lopes**, **REITOR - CD1 - REITORIA**, em 29/06/2021 11:06:36.

Este documento foi emitido pelo SUAP em 28/06/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 201583
Código de Autenticação: 0ad4eefeb2



INSTITUTO
FEDERAL
Paraíba

Política de Segurança da Informação

2020- 2024

Sumário

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
07/20	1.0	Versão inicial	Equipe elaboração POSIN
08/20	1.02	Versão final	Equipe elaboração POSIN
08/20	1.03	Versão final	Equipe elaboração POSIN

1. Escopo

A Política de Segurança da Informação, também representada pela sigla POSIN, tem por objetivo fornecer diretrizes, responsabilidades, competências e apoio da alta direção na implementação da gestão de segurança da informação do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB).

É uma declaração formal da Instituição sobre o seu compromisso com a proteção das informações que contém as diretrizes para a segurança do manuseio, tratamento, controle e proteção das informações no âmbito deste Instituto.

Esta política abrange de forma mandatória em sua Reitoria, todos os *campi*, incluindo os em implantação, além de demais unidades do IFPB. Atua também em todos os usuários que de forma direta ou indireta se relacionam com a instituição.

Os quesitos desta Política de Segurança da Informação serão aplicados de maneira idêntica a todos os sistemas de informação e serviços de comunicação de domínio e/ou uso do IFPB, como sistemas administrativos, acadêmicos, e-mail institucional assim como também sites hospedados no domínio deste Instituto.

2. Conceitos e Definições

TERMOS / ABREVIAÇÕES	SIGNIFICADO
Ameaça	Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
Análise de Riscos	Uso sistemático de informações para identificar fontes e estimar o risco.
Ataque	Ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro ou indisponível.

Ativos de Informação	Os meios de armazenamento, transmissão e processamento da informação, os equipamentos. necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.
Comitê de Segurança da Informação (CSI)	Comitê responsável de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da Instituição.
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 da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.
Custodiante do ativo de informação	Pessoa física que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação, materializados ou não, que não lhe pertencem, mas que estão sob sua custódia.
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)	Equipe responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança.
Gestor de Segurança da Informação	Responsável pelas ações de segurança da informação e comunicações no âmbito da Instituição.
Política de Segurança da Informação	Documento aprovado pela autoridade responsável da Instituição, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.
Redes Sociais	Estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.
Tecnologia da Informação (T.I.)	Ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.
Usuário	Pessoa física, seja servidor ou equiparado, discente, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação da instituição, formalizada por meio da assinatura de Termo de Responsabilidade.

3. Princípios

A Política de Segurança da Informação deve seguir os valores e princípios do IFPB, os quais são: Ética, Desenvolvimento Humano, Inovação, Qualidade e Excelência, Transparência, Respeito, Compromisso Social e Ambiental, além dos seguintes princípios básicos:

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

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

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;

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Legalidade: garantia de que todas as ações de Segurança da Informação e Comunicação deverão obedecer aos princípios constitucionais, administrativos e à legislação vigente.

4. Diretrizes Gerais

4.1. Tratamento da Informação

Deverá ser realizado um planejamento de ações visando o tratamento, armazenamento, identificação, cópia de segurança e classificação das informações de tal forma a garantir a integridade, autenticidade, disponibilidade

e confidencialidade para evitar o uso dessas informações por usuários ou sistemas não autorizados.

4.2. Segurança Física e do Ambiente

Processo referente à proteção de todos os ativos físicos do IFPB, englobando instalações físicas, internas e externas, em todas as localidades em que a instituição se fizer presente.

As instalações, equipamentos, redes e sistemas de computadores, exceto os sistemas e portais destinados a fornecer informações ao público, deverão possuir mecanismos adequados de controle de acesso físico e/ou lógico, que possibilitem a identificação das pessoas e/ou usuários que as utilizem.

Todos os usuários e qualquer outra pessoa que entre na instituição deverão possuir algum tipo de identificação visível e ter seu acesso registrado, onde possa ser visualizada a data e hora de sua entrada e saída.

A autenticação desses usuários, quando for o caso, poderá ser por senha, biometria ou outro fator de autenticação, estes métodos poderão ser utilizados de maneira combinada. A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio usuário, a qualquer tempo, ou por determinação da unidade de T.I., especialmente quando houver suspeita de uso indevido ou de violação.

Qualquer tipo de informação, classificada como restrita ou sigilosa, referente a conteúdos que dizem respeito à instituição, deverá ser guardada em lugar seguro, como por exemplo: cofres, armários e mobílias que possuam algum tipo de fechadura quando não estiverem em uso, ou restritas às pessoas autorizadas quando armazenadas em portais ou sistemas de informação.

Qualquer tipo de equipamento de armazenagem e processamento de informação com tombamento (Ex.: estações de trabalho, notebooks, dispositivos móveis) só poderão ser utilizados fora das dependências do instituto ou do departamento de sua responsabilidade com autorização prévia da chefia imediata

e anuência da Coordenação de Patrimônio da Reitoria/Campus e protegido de forma adequada contra furto, roubo ou perda da informação.

Nos casos de invalidação temporária ou definitiva das credenciais de acesso de agentes públicos, o acesso aos ativos de informação da Autarquia dar-se-á mediante as condições estabelecidas para os visitantes.

4.3. Gestão de Incidentes em Segurança da Informação

A gestão de incidentes em segurança da informação tem por objetivo em assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação [ABNT NBR ISO/IEC 27001, 2013].

Deverá ser mantida uma equipe para tratamento e resposta a incidentes de tecnologia da informação que será responsável por receber, filtrar, classificar e responder as solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências.

4.4. Gestão de Ativos

As informações e dados produzidos ou recebidos pela IFPB, em decorrência do desempenho de seu mandato, serão considerados públicos, ressalvadas as exceções previstas na legislação aplicável ou que são de caráter restrito ou sigiloso.

Os ativos de informação devem:

- ser inventariados e protegidos;
- ter identificação dos seus proprietários e custodiantes;
- ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

- ter a sua entrada e saída nas dependências da instituição autorizadas e registradas por autoridade competente;
- 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;
- ser regulamentados por norma específica quanto a sua utilização; e
- ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Cada ativo de informação do IFPB deverá ter um gestor designado pelo CGTI ou Comitê de Segurança da Informação.

A definição do custodiante do ativo de informação deve ser feita formalmente pelo gestor do ativo de informação. A ausência desta designação pressupõe que o gestor é o próprio custodiante.

O Comitê de Segurança da Informação deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Os recursos tecnológicos e as instalações de infraestrutura devem possuir planejamentos de ações que visem a proteção contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Durante todo o ciclo de vida de um ativo de informação, sua manipulação e uso observarão medidas especiais de segurança compatíveis com seu grau de sigilo e em conformidade com a legislação vigente e normas complementares adotadas pelo IFPB.

4.5. Gestão do Uso dos Recursos Operacionais e de Comunicações

Todos os usuários do IFPB têm o direito ao uso dos recursos de tecnologia da informação e comunicação de acordo com as diretrizes de seu perfil, definidas por meio de requisitos técnicos ou por determinação específica da Reitoria ou dos órgãos da administração superior dos *campi*. Para usuários temporários, como visitantes, palestrantes e etc., o acesso será temporário e limitado à navegação.

Um termo de responsabilidade para uso dos recursos de tecnologia da informação – RTIC, deverá ser assinado para todo e qualquer usuário em potencial do IFPB. Este termo poderá assumir a forma eletrônica através dos sistemas internos ou através do sistema de autenticação.

4.5.1. Acesso à Internet

Todos os usuários têm o direito de acesso à Internet dentro da infraestrutura do IFPB, conforme as permissões de acesso estipuladas nas normas de segurança da instituição. Esse acesso deverá ser feito para fins diretos e complementares às atividades da Instituição, para o enriquecimento intelectual de seus usuários ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de suas atividades.

Os acessos realizados nesse ambiente são monitorados pela equipe de Tecnologia da Informação responsável, na Reitoria e nos *campi*, com o objetivo de garantir o cumprimento desta política.

4.5.2. E-mail

O e-mail ou correio eletrônico é um serviço oferecido pelo IFPB como um recurso profissional e acadêmico para apoiar os usuários cadastrados no cumprimento dos objetivos institucionais e são passíveis de auditoria. Os usuários que o utilizarem deverão assegurar que o endereçamento da

mensagem esteja correto. Seu uso é exclusivo para fins Institucionais sendo vedada qualquer forma de *spam*[1].

4.5.3. Mídias Sociais

O IFPB em seu âmbito geral que inclui a Reitoria e todos *campi* só reconhece oficialmente as redes sociais listadas no portal institucional. Qualquer outro perfil deverá ser desconsiderado

Toda informação publicada nos meios de comunicação digitais oficiais do IFPB será de responsabilidade do usuário que realizou a publicação.

4.5.4. Computação em nuvem

O IFPB dispõe, para todos servidores (técnicos administrativos e professores) e para os alunos, um espaço na nuvem para armazenamento de arquivos, editores de documentos online e hospedagem de e-mail institucional. Estes documentos são na forma de uso de escritório.

Para demais serviços oferecidos pelo IFPB que ainda não estão na nuvem, o Instituto irá dispor de norma própria e específica para cada um.

4.6. Controles de Acesso

O acesso aos recursos de tecnologia da informação dentro da infraestrutura da instituição terá controles físicos e/ou lógicos com o objetivo de proteger equipamentos, sistemas, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

O acesso aos serviços de rede do IFPB que necessitem de autenticação só será permitido a usuários cadastrados.

---

[1] *Spam* é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

4.7. Gestão de Riscos

A Gestão de Riscos é um processo contínuo, que inclui planejamento, execução, verificação e revisão das ações. Estas fases do processo objetivam manter em níveis aceitáveis os riscos de T.I. a que estão sujeitos os ativos de informação do IFPB.

Para a gestão de riscos será definida, em norma complementar, seguindo diretriz superior já implantada no âmbito do IFPB, a metodologia de construção daquele processo, onde deverá constar análise e avaliação de riscos, e definir a periodicidade no levantamento de risco nos ativos de informação do IFPB, visando, sempre, sua proteção.

Todos os riscos levantados, mesmo os mais baixos, identificados como aceitáveis, deverão ter sua evolução acompanhada para permitir a detecção de possíveis mudanças no impacto ou probabilidade de ocorrência.

4.8. Gestão de Continuidade

A implantação do processo de Gestão de Continuidade de Negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação [06/IN01/DSIC/GSIPR].

Um Plano de Continuidade de Negócios (PCN), deverá ser desenvolvido, implementado e testado periodicamente para garantir a continuidade dos serviços críticos do IFPB. Será baseado em metodologias e boas práticas e aprovado pelo Comitê de Segurança da Informação.

4.9. Auditoria e Conformidade

Todo e qualquer usuário estará sujeito a auditoria de suas ações durante a utilização dos recursos de tecnologia da informação. Os procedimentos de

auditoria e de monitoramento de uso dos recursos serão realizados periodicamente pela Diretoria Geral de Tecnologia da Informação (DGTI) e/ou áreas responsáveis pela Tecnologia da Informação nos campi com o objetivo de observar o cumprimento desta política pelos usuários e com vistas à gestão de desempenho e segurança.

Havendo evidência de qualquer atividade que possa comprometer o desempenho e/ou a segurança dos recursos de tecnologia da informação ou que infrinja a Política de Segurança da Informação, será permitido à DGTI ou a área responsável pela T.I. no campus, auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso da fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário, à direção geral do campus, à Reitoria do IFPB e/ou à Equipe de Tratamento e Resposta a Incidentes de Tecnologia da Informação a depender da gravidade.

4.10. Software de terceiros

A DGTI/IFPB dentro de suas atribuições é responsável pelo provimento dos softwares dentro da Instituição. Sendo assim, é vedado o uso de qualquer outro tipo sem a devida aprovação da DGTI. Havendo necessidade de algum tipo que ainda não tenha sido provido, deverá ser solicitado uma análise do software para o setor competente. Uma norma complementar deverá dispor do uso de cada tipo de software dentro do âmbito institucional.

É permitida a instalação de softwares ou aplicativos locais nos equipamentos da Instituição (computadores, *smartphones*, *tablets* e etc.), para apoio às atividades administrativas e de ensino, a exemplo das suítes de escritório, desde que está seja realizada após a análise prévia do setor responsável pela T.I. nos campi ou na Reitoria.

5. Competências

Compete ao gestor de segurança da informação:

- presidir o Comitê de Segurança da Informação ou estrutura equivalente;
- assessorar a alta administração na implementação da Política de Segurança da Informação;
- estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- 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;
- incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;
- verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e
- 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.

Compete ao Comitê de Segurança da Informação:

- Promover a cultura de Segurança da Informação no âmbito da Instituição;
- Coordenar a elaboração ou a revisão da Política de Segurança da Informação, normas e procedimentos relacionados;
- Acompanhar as investigações e avaliações dos dados decorrentes de quebras de segurança;
- Propor recursos necessários às ações de Segurança da Informação;

- Instituir a Equipe de Tratamento e Respostas a Incidentes;
- Acompanhar o estudo de novas tecnologias, no que diz respeito a possíveis impactos sobre Segurança da Informação.

Compete à Diretoria Geral de Tecnologia da Informação:

- Planejar, coordenar, executar e avaliar os projetos, procedimentos, normas e ações que possibilitem a operacionalização e manutenção desta política em articulação com as Pró-Reitorias, Direções Gerais e demais áreas de Tecnologia da Informação dos *campi*.

6. Penalidades

Em caso de descumprimento desta política de segurança da informação serão aplicadas as sanções e penalidades cabíveis tomando como base a legislação em vigor, em especial o que consta na:

- Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;
- Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;
- Código Penal, através do Decreto-Lei nº 2848/1940;
- Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;
- Decreto nº 7.845 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;
- Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

- Lei no 12.527, de 18 de novembro de 2011 (Lei de acesso a informações);
- Lei complementar no 131, de 27 de maio de 2009 (Lei da Transparência);
- Decreto nº 9.637, de 26 de dezembro de 2018 (Política Nacional de Segurança da Informação);
- Decreto nº 10.222, de 5 de fevereiro de 2020 (Estratégia Nacional de Segurança Cibernética);
- Instrução Normativa 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.

7. Política de Atualização

Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação do IFPB, incluindo a própria política, devem ser revisados a cada quatro anos ou sempre que se fizer necessário.