MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CEARA

RESOLUÇÃO Nº 07/CATI, DE 27 DE JANEIRO DE 2025

Institui a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação, no âmbito da Universidade Federal do Ceará (UFC).

O REITOR DA UNIVERSIDADE FEDERAL DO CEARÁ, no uso de suas atribuições legais e estatutárias, em atendimento à recomendação expressa do Comitê Administrativo de Tecnologia da Informação e Governança Digital (CATI), em sua reunião de 27 de janeiro de 2025, e considerando a documentação apresentada por meio do processo administrativo SEI nº 23067.002575/2026-35,

RESOLVE:

Art. 1º Instituir a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação, no âmbito da Universidade Federal do Ceará (UFC), na forma do Anexo desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua aprovação.

Reitoria da Universidade Federal do Ceará, em 27 de janeiro de 2025.

CUSTÓDIO LUÍS SILVA DE ALMEIDA
Reitor

Documento assinado eletronicamente por **CUSTODIO LUIS SILVA DE ALMEIDA**, **Reitor**, em 29/01/2026, às 18:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufc.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6128478** e o código CRC **CCF342F2**.

Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação

Versão 1.0

Fortaleza, janeiro de 2025

Histórico de Versões

Data	Versão	Descrição	Autor
27/01/2025	1.0	Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.	Superintendência de Tecnologia da Informação

Sumário

UNIVERSIDADE FEDERAL DO CEARÁ

POLÍTICA DE DESENVOLVIMENTO DE PESSOAS EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Responsável	Superintendência de Tecnologia da Informação
Aprovado por	Comitê Administrativo de Tecnologia da Informação e Governança Digital da UFC
Políticas Relacionadas	– Lei Geral de Proteção de Dados Pessoais – Política Nacional de Desenvolvimento de Pessoas – Política Nacional de Segurança da Informação – Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020; – Instrução Normativa SGD/ME Nº 117, de 19 de novembro de 2020; – Programa de Privacidade e Segurança da Informação (PPSI - Portaria SGD/MGI nº 852, DE 28 de março de 2023); – Plano de Desenvolvimento de Pessoas da UFC; Política de Segurança da Informação da UFC - Política de Privacidade e Proteção de Dados Pessoais
Localização de armazenamento	https://sti.ufc.br/documentos/politicas-normas-e-resolucoes/politicas-de-privacidade-e-seguranca/
Data de Aprovação	27/01/2025
Data de revisão	
Versão	1.0

1 INTRODUÇÃO

A necessidade da compreensão de que a informação é o ativo mais importante de qualquer atividade nas organizações é uma das razões que fazem a segurança da informação necessária, necessitando dessa forma de ações que sensibilizem toda a comunidade universitária (professores, alunos e servidores) a desenvolver uma cultura em segurança da informação.

A Segurança da Informação (SI), está cada vez mais se firmando como uma área de grande importância nas organizações devido ao grande avanço das tecnologias de informação e comunicação. O fluxo das informações perpassa pela convergência de muitas tecnologias, requerendo assim de seus usuários cuidados para a preservação da informação, tornando esse fluxo mais seguro, evitando assim os riscos envolvidos em uma possível perda.

A implementação desta cultura comprometida com a segurança dos processos no que diz respeito ao sigilo, à integridade e autenticidade no tratamento das informações nas organizações, exige o constante treinamento dos seus usuários.

Desta feita, a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação tem por objetivo estabelecer diretrizes, princípios e conceitos para conscientizar e capacitar a comunidade acadêmica da Universidade Federal do Ceará (UFC) e que em algum momento têm acesso ou realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes, tais como o **Decreto n° 9.991**, de 28 de agosto de 2019 e o **Decreto 9.637**, de 26 de dezembro de 2018.

2 PROPÓSITO

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação surge em resposta à crescente importância da proteção de dados e informações sensíveis. Alguns fatores que determinam a necessidade dessa política incluem:

1. **Ameaças Cibernéticas:** O aumento das ameaças cibernéticas e ataques à segurança da informação destaca a importância de contar com uma equipe bem treinada e consciente dos riscos.
2. **Regulamentações:** Normas e regulamentações cada vez mais rigorosas exigem que as organizações protejam a privacidade e a segurança dos dados, o que impulsiona a necessidade de políticas específicas e treinamento para os colaboradores.
3. **Educação Continuada:** O ambiente de segurança da informação está em constante evolução, exigindo uma abordagem de educação continuada para garantir que todos da comunidade universitária estejam atualizados sobre as melhores práticas e ameaças emergentes.

Os objetivos básicos da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação incluem:

1. **Conscientização:** Educar a comunidade universitária sobre as melhores práticas de segurança da informação e os riscos associados, aumentando a conscientização sobre a importância da proteção de dados.
2. **Treinamento:** Fornecer treinamento específico para todos em diferentes níveis organizacionais, garantindo que todos compreendam suas responsabilidades na proteção da informação.
3. **Conformidade:** Assegurar que todos estejam alinhados com as regulamentações de privacidade e segurança, minimizando o risco de não conformidade e potenciais penalidades.
4. **Resposta a Incidentes:** Preparar a comunidade universitária para lidar com incidentes de segurança da informação de maneira eficaz, reduzindo o impacto de possíveis violações.

Em última análise, a Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação tem como o seu objetivo maior mobilizar toda comunidade universitária quanto a importância da SI, buscando trabalhar a consciência do público para a importância e o valor da informação, assegurando os pilares da integridade,

confidencialidade e autenticidade da informação para garantir confiabilidade nos processos de trabalho desta instituição.

3 ESCOPO

Esta Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação se aplica a toda comunidade universitária da UFC, incluindo gestores, prestadores de serviços, estagiários, contratados e alunos que tenham acesso e/ou utilizem dados institucionais, incluindo os dados pessoais.

4 TERMOS E DEFINIÇÕES

Ameaça Cibernética: refere-se a qualquer potencial perigo ou incidente que visa explorar vulnerabilidades em sistemas computacionais, redes ou serviços online. Estas ameaças são geralmente perpetradas por agentes mal-intencionados, como hackers, criminosos cibernéticos ou grupos organizados, e têm como objetivo comprometer a integridade, confidencialidade ou disponibilidade de informações digitais.

Ativos: recursos valiosos, tangíveis e intangíveis, detidos por uma entidade, que contribuem para seu valor econômico, estratégico ou operacional. Esses incluem equipamentos, instalações físicas, dados, conhecimento dos colaboradores, propriedade intelectual, relacionamentos comerciais e outros elementos cruciais para o sucesso e segurança de uma organização. Na esfera de segurança da informação, a identificação e proteção eficaz desses ativos são essenciais para mitigar riscos e garantir a integridade, confidencialidade e disponibilidade das informações críticas;

Ativos de Informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que valor para um indivíduo ou organização;

Autenticidade: refere-se à garantia de que uma entidade, seja uma pessoa, sistema ou informação, é genuína e não foi falsificada. Em transações e comunicações,

a autenticidade valida a identidade das partes envolvidas, assegurando a origem legítima das informações;

Comunidade Universitária: refere-se ao conjunto de pessoas que compõem uma instituição de ensino superior, incluindo estudantes, professores, funcionários administrativos e demais membros que participam ativamente da vida acadêmica e administrativa da universidade;

Confiabilidade: significa que o objeto ou processo é estável, preciso e pode ser confiado para desempenhar suas funções conforme esperado ao longo do tempo.

Confidencialidade: envolve a proteção de informações sensíveis contra acesso não autorizado. Garante que apenas as pessoas ou sistemas autorizados possam acessar e visualizar determinados dados, preservando a privacidade e a segurança das informações;

Conscientização: atividade que tem por finalidade orientar o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade, para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Dado: refere-se a elementos brutos e objetivos, geralmente na forma de fatos, números, símbolos ou palavras. São as unidades mínimas de informação que, por si só, podem não ter significado relevante;

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

Dado Sensível: refere-se a informações pessoais que, quando utilizadas de maneira inadequada ou comprometidas, podem resultar em discriminação ou riscos significativos para a privacidade e segurança do indivíduo.

Encarregado: pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Engenharia Social: técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da segurança da informação, é considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de indivíduos, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes;

Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

Incidente de Segurança: refere-se a qualquer evento que comprometa a integridade, confidencialidade ou disponibilidade de dados, sistemas de informação ou recursos tecnológicos. Esses incidentes podem variar em escala e natureza, incluindo desde ataques cibernéticos sofisticados até ações não intencionais, como erros humanos.

Informação: surge quando os dados são processados, organizados ou interpretados de maneira significativa. É o resultado do contexto aplicado aos dados, tornando-os compreensíveis e úteis. A informação tem o propósito de transmitir conhecimento, proporcionando insights, entendimento ou orientação;

Integridade: assegura que os dados ou sistemas não foram comprometidos ou corrompidos, mantendo sua precisão e confiabilidade ao longo do tempo;

LGPD: legislação brasileira que tem como objetivo proteger os direitos fundamentais de privacidade e liberdade dos indivíduos em relação ao tratamento de seus dados pessoais. A lei estabelece princípios, direitos e deveres para organizações que lidam com informações pessoais, buscando garantir transparência, segurança e consentimento adequado no processamento desses dados. A LGPD também confere aos titulares de dados o direito de acessar, corrigir e excluir suas informações, promovendo uma cultura de responsabilidade e cuidado na gestão de dados no ambiente digital;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Programa de Privacidade e Segurança da Informação (PPSI): caracteriza-se como um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação e tem como valores: a maturidade; a resiliência; a efetividade;

a colaboração e a inteligência. O Programa foi instituído por meio da PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023 e implementa ações de Privacidade e Segurança da Informação no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), conforme art. 3º do DECRETO Nº 7.579, DE 11 DE OUTUBRO DE 2011.

Privacidade: refere-se ao direito fundamental de indivíduos controlarem o acesso, a divulgação e o uso de suas informações pessoais. Envolve a capacidade de manter certos aspectos da vida e das comunicações fora do alcance público, protegendo a autonomia e a liberdade pessoal.

Segurança da Informação: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Treinamento: refere-se a um processo educacional projetado para desenvolver habilidades, conhecimentos e competências específicas em indivíduos ou grupos.

5 DECLARAÇÕES DA POLÍTICA

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação da UFC deve estar alinhada:

- com Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 14 de agosto de 2018);
- com a Política Nacional de Desenvolvimento de Pessoas (Decreto 9.991, de 28 de agosto de 2019);
- com a Política Nacional de Segurança da Informação (Decreto 9.637, de 26 de dezembro de 2018);

- com Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;
- com Instrução Normativa SGD/ME Nº 117, de 19 de novembro de 2020;
- com o Programa de Privacidade e Segurança da Informação (PPSI - Portaria SGD/MGI nº 852, DE 28 de março de 2023);
- com o Plano de Desenvolvimento de Pessoas da UFC;
- com a Política de Segurança da Informação da UFC;
- com a Política de Proteção de Dados Pessoais da UFC;

5.1 Diretrizes Gerais

Os treinamentos da UFC estão alinhados com as melhores práticas de tratamento de dados pessoais, privacidade e segurança da informação, em especial as recomendações do PPSI:

I - Melhores práticas de tratamento de dados;
II - Como reconhecer ataques de engenharia social;
III - Melhores práticas de autenticação;
IV - Causas da exposição não intencional de dados;
V - Como reconhecer e relatar incidentes de segurança;
VI - Boas práticas de segurança;

Os níveis de conhecimento e habilidades necessários para os integrantes da comunidade universitária desempenharem eficazmente suas funções relacionadas à privacidade e segurança da informação possuem como elementos-chave:

I - **Conscientização Básica:** Compreensão dos princípios fundamentais de privacidade e segurança da informação e conhecimento sobre os riscos associados à manipulação inadequada de dados.

II - **Treinamento Específico:** Capacidade de aplicar as melhores práticas de segurança da informação em contextos específicos e treinamento regular para se manter atualizado sobre as ameaças cibernéticas emergentes.

III - **Conformidade e Regulamentação:** Familiaridade com as leis e regulamentos relevantes de privacidade e segurança da informação e habilidade para aplicar as políticas internas em conformidade com as normas externas.

IV - **Gestão de Dados:** Competência na manipulação adequada de dados, incluindo coleta, armazenamento e compartilhamento seguro e conhecimento sobre a classificação de dados e a aplicação de medidas apropriadas de proteção.

V - **Resposta a Incidentes:** Treinamento para lidar com incidentes de segurança da informação, incluindo procedimentos de notificação e resolução e habilidade para colaborar efetivamente em uma resposta coordenada a eventos de segurança.

VI - **Conscientização do Usuário:** capacidade de educar e sensibilizar colegas sobre práticas seguras de manipulação de dados e habilidade para comunicar eficazmente os riscos e as medidas preventivas.

VII - **Colaboração e Comunicação:** Habilidade para trabalhar em equipe e comunicar eficazmente as questões de segurança.

VIII - **Ética e Integridade:** Compromisso com a ética na manipulação de dados e informações confidenciais e adesão aos princípios de integridade e responsabilidade no ambiente de trabalho.

IX - **Gerenciamento de riscos:** Competência para avaliar e elaborar respostas aos riscos.

É importante adaptar as exigências conforme as funções específicas de cada colaborador, garantindo que todos desempenhem um papel ativo na proteção dos ativos de informação da organização.

6 METAS E RESULTADOS ESPERADOS

A UFC espera:

I - promover o desenvolvimento pessoal em privacidade e segurança da informação;

II - estabelecer metas institucionais como referência para o planejamento das ações de desenvolvimento em privacidade e segurança da informação;

III - atingir um nível de conhecimento considerável em privacidade e segurança da informação;

IV - estabelecer uma cultura que valoriza e prioriza a segurança da informação;

V - melhorar a comunicação sobre questões de segurança; e

VI - promover a colaboração entre os diferentes departamentos da comunidade universitária;

7 PAPÉIS E RESPONSABILIDADES

Cabe à Superintendência de Tecnologia da Informação (STI) a responsabilidade de planejar e coordenar a execução das atividades de ensino em privacidade e segurança da informação.

Cabe ao Gestor de Segurança da Informação da UFC, estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação, conforme previsto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

Cabe ao Encarregado orientar os funcionários e os contratados da UFC, a respeito das práticas de desenvolvimento pessoal a serem tomadas em relação à proteção de dados pessoais.

Cabe à toda a comunidade universitária da UFC a responsabilidade de implementar os conceitos ensinados nos programas de conscientização e treinamento em Privacidade e Segurança da Informação.

8 AÇÕES DE DESENVOLVIMENTO PRIORITÁRIAS

As ações de desenvolvimento prioritárias da UFC estão definidas a seguir:

I - ações que visam ao atendimento às necessidades da UFC;

II - curso abordando os princípios básicos de Privacidade e Segurança da Informação;

III - treinamentos sobre a temática de Privacidade e Segurança da Informação;

IV - ações destinadas ao reconhecimento de responsabilidades sobre proteção de dados;

V - ações que busquem elevar a maturidade e a resiliência da UFC, em termos de privacidade e segurança da informação que estejam alinhadas com o PPSI;

VI - conscientização de segurança da informação sobre reconhecimento e relato de potenciais indicadores de ameaça interna; e

VII - conscientização para novos servidores da UFC, no momento de acolhida Institucional.

9 DISPOSIÇÕES FINAIS

Esta política deverá ser revisada a cada 02 (dois) anos e sempre que necessário, a partir do início de sua vigência.

Esta política entra em vigor na data de sua publicação.

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2013

_____. **ABNT NBR ISO/IEC 27002:2013**: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 8.112, de 11 de dezembro de 1990. **Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais)**. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso à Informação (LAI)**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 9.637, de 26 de dezembro de 2018. **Política Nacional de Segurança da Informação – PNSI**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 9.991, de 28 de agosto de 2019**. Dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da Administração Pública Federal Direta, Autárquica e Fundacional.** Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9991.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 10.222, de 5 de fevereiro de 2020. **Aprova a Estratégia Nacional de**

Segurança Cibernética. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 10.641, de 2 de março de 2021. **Altera a Política Nacional de Segurança da Informação – PNSI**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10641.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 10.748, de 16 de julho de 2021. **Institui a Rede Federal de Gestão de Incidentes Cibernéticos**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria GSI/PR nº 93, 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: 28 set. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa nº 01, maio de 2020**. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.** Disponível em: <https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN01_consolidada.pdf>. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa nº 03, maio de 2021. **Dispõe sobre os processos relacionados à Gestão de Segurança da Informação nos Órgãos e nas Entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN03_consolidada.pdf >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar nº 17, abril de 2013**. Dispõe sobre a Atuação e Adequações para Profissionais a Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/dsic/legislacao/NC17.pdf >. Acesso em: 28 set. 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar nº 18, abril de 2013**. Dispõe sobre as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.** Disponível em: < https://www.gov.br/gsi/pt-br/dsic/legislacao/NC18.pdf >. Acesso em: 28 set. 2023.

BRASIL. Ministério do Meio Ambiente. Portaria 100, março de 2012**. Dispõe sobre diretrizes e objetivos relativos à Política de Desenvolvimento dos Servidores do**

Ministério do Meio Ambiente. Disponível em: < https://www.ibama.gov.br/component/legislacao/?view=legislacao&legislacao=126824 >. Acesso em: 28 set. 2023.

BRASIL. Secretaria de Governo Digital. Portaria SGD/MGI nº 852, março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI. Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908 >. Acesso em: 28 set. 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação. Novembro 2022**. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 28 set. 2023.

UNIVERSIDADE DE FEDERAL DA BAHIA. SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO. **Plano de conscientização em segurança da informação. Março de 2023**. Disponível em: < https://sti.ufba.br/plano-de-conscientizacao-em-seguranca-da-informacao >. Acesso em: 28 set. 2023.

BRASIL. Ministério de Gestão e da Inovação em Serviços Públicos. **Norma Complementar nº 18, abril de 2013. D Plano de Desenvolvimento de Pessoas 2023.** Disponível em: < https://www.gov.br/servidor/pt-br/acesso-a-informacao/servidor/carreiras/eppgg/sobre-a-carreira/desenvolvimento-profissional-1/arquivos/formularios/plano_de_desenvolvimento_de_pessoas_2023.pdf >. Acesso em: 28 set. 2023

MINISTÉRIO DA ECONOMIA. Instrução Normativa SGD/ME nº117, novembro de 2020. **Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional**. Disponível em: < https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596 > Acesso em: 28 set 2023.

Governo do Rio Grande do Sul. Subsecretaria de Gestão e Desenvolvimento de Pessoas. **Política de Gestão e Desenvolvimento de Pessoas.** Disponível em: < https://gestaodepessoas.rs.gov.br/politica-de-gestao-de-pessoas/ >. Acesso em: 28 set. 2023.

CENTER INTERNET SECURITY. **Security Awareness Skills Training Policy Template for CIS Control 14**. Mar. 2023. Disponível em: < https://www.cisecurity.org/insights/white-papers/security-awareness-skills-training-policy-template-for-cis-control-14 > . Acesso em: 28 set 2023.

_____. **ISO/IEC 29151:2017**: Information technology — Security techniques — Code of practice for personally identifiable information protection. Genebra, 2017.

_____. **NIST Special Publication 800-50:** Building an Information Technology Security Awareness and Training Program. Gaithersburg, 2003.

_____. **NIST Special Publication 800-53 revisão 4**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, 2013. Acesso em: 29 set 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Public Draft: The NIST Cybersecurity Framework 2.0, 2023. Disponível em: https://www.nist.gov/cyberframework/framework. Acesso em: 28 set 2023.