



UNIVERSIDADE FEDERAL DO AMAZONAS UFAM

Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação

**Maio
2024**

POLÍTICA DE DESENVOLVIMENTO DE PESSOAS EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

UNIVERSIDADE FEDERAL DO AMAZONAS

Professor Doutor Sylvio Mário Puga Ferreira

Reitor

COMITÊ DE GOVERNANÇA DIGITAL

Professor Doutor Sylvio Mário Puga Ferreira

Reitor

David Lopes Neto

Pró-Reitor de Ensino de Graduação

Adriana Malheiro Alle Marie

Pró-Reitor de Pesquisa e Pós-Graduação

Almir Oliveira de Menezes

Pró-Reitor de Extensão

Maria Vanusa do Socorro de Souza Firmo

Pró-Reitor de Gestão de Pessoas

Maria da Glória Vitória Guimarães

Pró-Reitor de Planejamento e Desenvolvimento Institucional

Angela Neves Bulbol de Lima

Pró-Reitor de Administração e Finanças

Jorge Carlos Magno Silva de Lima

Diretor do Centro de Tecnologia da Informação e Comunicação

Arquelau Carvalho do Nascimento Neto

Encarregado pelo Tratamento de Dados Pessoais

Carlos Moisés Medeiros

Ouvidor

Dinorvan Fanhaimpork

Auditor



CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Jorge Carlos Magno

Diretor

COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Márcia Regina Moraes de Paula

Coordenadora de Segurança da Informação

PRO-REITORIA DE GESTÃO DE PESSOAS

DEPARTAMENTO DE DESENVOLVIMENTO DE PESSOAS

ASSESSORIA DE COMUNICAÇÃO

EQUIPE TÉCNICA DE ELABORAÇÃO E REVISÃO

Arquelau Neto

Gilberto Aires Libania

Márcia Regina Moraes de Paula

Robert Pessinga da Silva

Histórico de Versões

Data	Versão	Descrição	Autor
07/05/2024	1.0	Elaboração da Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação.	Equipe técnica de elaboração e revisão



SUMÁRIO

1. PROPÓSITO	4
2. ESCOPO	4
3. TERMOS E DEFINIÇÕES	4
4. DECLARAÇÕES DA POLÍTICA	7
4.1 Declaração de Comprometimento da Alta Administração da UFAM	7
4.2 Disposições Gerais	7
4.3 Fundamentações Legais e Normativas	8
4.4 Metas e resultados esperados	11
4.5 Papéis e Responsabilidades	12
4.6 Orçamento	14
4.7 Treinamento e Conscientização	14
4.8 Ações de desenvolvimento prioritárias	17
4.9 Procedimentos para solicitações de ações de desenvolvimento de pessoas	20
4.10 Afastamento para capacitação	20
5. DISPOSIÇÕES FINAIS	21
6. REVISÃO E ATUALIZAÇÃO	22
7. VIGÊNCIA	22
ANEXO A - Levantamento de cursos com ênfase em segurança da informação	



1.PROPÓSITO

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação tem por objetivo estabelecer diretrizes, princípios e conceitos para conscientizar e capacitar os servidores e sensibilizar a comunidade acadêmica que se relacionam com a Universidade Federal do Amazonas e que em algum momento têm acesso ou realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, (Lei Geral de Proteção de Dados Pessoais - LGPD), do Decreto nº 9.991, de 28 de agosto de 2019 (Política Nacional de Desenvolvimento de Pessoas) e o Decreto 9.637, de 26 de dezembro de 2018 (Política Nacional de Segurança da Informação) e outras normas vigentes citadas nas fundamentações legais e normativas.

2.ESCOPO

Esta Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação deve abranger todo âmbito da Universidade Federal do Amazonas. Visa promover uma cultura de educação, conscientização, treinamento e responsabilidade de todos em relação à privacidade e à segurança da informação. Aplica-se a toda comunidade acadêmica da UFAM, incluindo servidores (ativos ou inativos), gestores, técnicos administrativos em educação, docentes, discentes, terceirizados, estagiários e prestadores de serviços, que tenham acesso e/ou utilizem dados institucionais, incluindo os dados pessoais.

3.TERMOS E DEFINIÇÕES

- a) 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;

- b) Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- c) 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;
- d) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- e) 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;
- f) 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);
- g) DPO (Data Protection Officer): Encarregado de Tratamento de Dados;
- h) 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;
- i) Vazamento de Dados: Transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo.



- j) Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;
- k) LGPD: Sigla de Lei Geral de Proteção de Dados;
- l) Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- m) Desenvolvimento Pessoal: Processo contínuo de aprimoramento e crescimento individual que envolve a busca por conhecimento, habilidades e competências para alcançar o máximo potencial em todas as áreas da vida;
- n) PDP: Sigla de Plano de Desenvolvimento de Pessoas;
- o) Escolas de Governo: Entidades de ensino da Administração Pública que trabalham com formação e aperfeiçoamento profissional dos servidores públicos.
- p) Formação Continuada: Evento de ensino que tem por finalidade desenvolver e ampliar a capacidade profissional dos servidores públicos.
- q) Política de Gestão de Pessoas: é um conjunto de princípios e diretrizes da Universidade Federal do Amazonas que orienta as práticas em gestão de pessoas e visa a obtenção de resultados almejados pela organização, pelos integrantes da equipe de trabalho e pela sociedade.
- r) Política de Segurança da Informação e Comunicações: sigla POSIC, documento aprovado pelo Conselho Superior de Administração da UFAM com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança de informação na instituição;
- s) 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;



- t) Segurança da Informação: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- u) Privacidade: Direito fundamental de proteção dos dados pessoais e confidenciais, garantindo a inviolabilidade da intimidade, da honra, da imagem e da vida privada;
- v) 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;
- w) Integridade: Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- x) PPSI: Sigla do Programa de Privacidade e Segurança da Informação, 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.

4.DECLARAÇÕES DA POLÍTICA

4.1 Declaração de Comprometimento da Alta Administração da UFAM

A Universidade Federal do Amazonas através da alta administração, na pessoa do(a) Magnífico(a) Reitor(a), declara-se comprometido(a) em reconhecer a importância da disseminação da cultura de proteção à privacidade e da segurança da informação para garantir a confidencialidade, integridade e disponibilidade dos dados e informações confidenciais em sua posse, bem como garantir a confiança dos usuários da comunidade acadêmica e servidores ativos e inativos e terceirizados, que são fundamentais para ajudar a prevenir e proteger os ativos e a reputação da instituição e que estejam conscientes e bem treinados em boas práticas de privacidade e segurança da informação.



4.2 Disposições Gerais

A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação da Universidade Federal do Amazonas, tem como objetivo estabelecer e manter um programa de conscientização contínua com ênfase em privacidade e segurança da informação, educando os usuários da instituição, sobre como interagir com ativos e dados corporativos e pessoais de maneira segura, garantindo o entendimento e os conhecimentos e comportamentos necessários para ajudar a garantir a segurança pessoal e da instituição, e deve estar alinhada com:

- a Lei Geral de Proteção de Dados Pessoais;
- a Política Nacional de Desenvolvimento de Pessoas;
- a Política Nacional de Segurança da Informação;
- a Instrução Normativa GSI/PR nº 1;
- a Instrução Normativa SGD/ME Nº 117;
- o Programa de Privacidade e Segurança da Informação (PPSI);
- o Plano de Desenvolvimento de Pessoas da UFAM;
- a Política de Segurança da Informação da UFAM;
- a Política de Gestão de Pessoas da UFAM;
- a Política de Proteção de Dados Pessoais da UFAM;
- a Gestão de Continuidade de Negócios e de Riscos institucionais;

4.3 Fundamentações Legais e Normativas

As referências legais e normativas utilizadas para a elaboração desta Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação da Universidade Federal do Amazonas, devem estar alinhada com:



- Lei nº 13.709, de 14 de agosto de 2018: institui a Lei Geral de Proteção de Dados Pessoais (LGPD), Art. 6º, inciso VII, Art. 46, Art. 47, Art. 49, Art. 50;
- 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(PNDP);
- Decreto nº 10.506, de 02 de outubro de 2020: Altera o Decreto nº 9.991, que dispõe sobre a PNDP da APF direta, autárquica e fundacional, e regulamenta dispositivos da Lei nº 8.112, de 11 de dezembro de 1990, quanto a licenças e afastamentos para ações de desenvolvimento, e a Instrução Normativa Nº 21 - SGP-ENAP/SEDGG/ME, de 1º de fevereiro de 2021;
- Portaria MEC nº 27, de 15 de janeiro de 2014 - Plano Nacional de Desenvolvimento Profissional dos Servidores Técnico-Administrativos em Educação no âmbito das Instituições federais de Ensino;
- Decreto 9.637, de 26 de dezembro de 2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
- Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020: Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- Instrução Normativa GSI/PR nº 6, de 23 de dezembro de 2021:Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal;
- NC nº 08 //IN01/DSIC/GSIPR: Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;



- NC nº 17 /IN01/DSIC/GSIPR: Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;
- NC nº 18 /IN01/DSIC/GSIPR: Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;
- NC nº 20 /IN01/DSIC/GSIPR: Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal, direta e indireta;
- Instrução Normativa SGD/ME Nº 117, de 19 de 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;
- Norma ABNT NBR ISO/IEC 27001:2013 – Especifica requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI), Art 7.3 Conscientização;
- Norma ABNT NBR ISO/IEC 27002:2013 Fornece diretrizes e código de práticas para normas e controles de gestão de segurança da informação, Art. 7.2.2 Conscientização, educação e treinamento em segurança da informação;
- Portaria SGD/MGI nº 852, de 28 de março de 2023: Institui o Programa de Privacidade e Segurança da Informação (PPSI), no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, e tem como valores: a maturidade; a resiliência; a efetividade; a colaboração e a inteligência;



- Resolução nº 27/2019 - CONSUNI/UFAM: Trata do Plano de Desenvolvimento de Pessoas da UFAM - PROGESP/; e a Nota Informativa nº 2 CGPDD/DEDDI/SEGEP/MP, de 30 de março de 2015 (Legalidade do pagamento de Programa de Incentivo Educacional);
- Decreto nº 5.825, de 29 de junho de 2006 - diretrizes para elaboração do Plano de Desenvolvimento dos Integrantes do Plano de Carreira dos Cargos Técnico-Administrativos em Educação; Decreto nº 5.824, de 29 de junho de 2006 - Estabelece procedimentos para a concessão do Incentivo à Qualificação e o Guia de Procedimentos para o Enquadramento 2ª Etapa/2005 - Ministério da Educação;
- Processo nº 002/2023 – CONSAD e SEI 23105.041618/2022-71: Programa de Auxílio à Qualificação - PROAQ: Institui promover o desenvolvimento institucional da Universidade, conjugado com o desenvolvimento dos seus servidores, gerenciado pela Pró-Reitoria de Gestão de Pessoas (PROGESP/DDP);
- Política de Segurança da Informação e Comunicação da UFAM: Artigo 10, item i) Conscientização e Treinamento: tem por objetivo internalizar conceitos e boas práticas de segurança da informação na cultura da instituição, por meio de ações permanentes de divulgação, treinamento e educação, para minimizar riscos de segurança da informação;

4.4 Metas e resultados esperados

A Universidade Federal do Amazonas deve:

- Promover o desenvolvimento pessoal em privacidade e segurança da informação;
- Estabelecer metas institucionais como referência para o planejamento das ações de desenvolvimento em privacidade e segurança da informação;



- Atingir um nível de conhecimento considerável em privacidade e segurança da informação, capaz de reconhecer e avaliar riscos, após sua conclusão;
- Avaliar o desempenho e comprometimento dos servidores com as metas e necessidades institucionais ao final de cada processo de desenvolvimento;
- Aumentar a conscientização sobre as melhores práticas de privacidade e segurança da informação;
- Capacitar os colaboradores para lidar com dados sensíveis de forma adequada;
- Reduzir riscos de violações de privacidade e vazamento de informações.

4.5 Papéis e Responsabilidades

A responsabilidade compartilhada de planejar, elaborar e coordenar a execução das atividades de ensino em privacidade e segurança da informação, caberá à Pró-Reitoria de Gestão de Pessoas, ao Centro de Tecnologia da Informação e Comunicação, e ao Encarregado pelo Tratamento de Dados Pessoais, especificadas abaixo:

Cabe à Pró-Reitoria de Gestão de Pessoas, implementar, fomentar, executar, controlar e firmar parcerias para promover programas e ações de capacitação e desenvolvimento de pessoas, relacionados à segurança da informação e privacidade, independentemente de sua fonte de recursos financeiros, e estabelecer normas definindo os requisitos metodológicos para sua implementação, monitorando sua eficácia.

Cabe ao Gestor de Segurança da Informação da Universidade Federal do Amazonas, estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação e privacidade, conforme previsto nos art.15 e 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e em parceria com a Assessoria de Comunicação, promover para fins de conscientização a divulgação



da política e das normas internas de segurança da informação da instituição através dos canais de comunicação disponíveis.

Cabe ao Encarregado de tratamento de dados orientar os funcionários e os contratados da Universidade Federal do Amazonas a respeito das práticas de desenvolvimento pessoal a serem tomadas em relação à proteção de dados pessoais, implementando controles para eficácia dos resultados.

Cabe à Assessoria de Comunicação - ASCOM editar, publicar e divulgar as campanhas de conscientização, treinamentos, cartilhas, boletins nas mídias institucionais da UFAM, mediante conteúdo-base delineado conjuntamente pela Pró-Reitoria de Gestão de Pessoas, pelo Centro de Tecnologia da Informação e pelo Encarregado do Tratamento de Dados Pessoais, com o objetivo de divulgar conteúdos de valores sobre privacidade e segurança da informação periodicamente através das nossas redes sociais, portais e sites institucionais, tendo como público alvo nossos funcionários (ativos e aposentados), alunos e/ou toda comunidade do meio acadêmico que tem acesso a nossa rede como meio de informações ou trabalho. Divulgar periodicamente, por intermédio da internet, intranet ou por outros meios, os eventos constantes no Plano de Desenvolvimento de Pessoas.

Cabe à Alta Administração da Universidade Federal do Amazonas por meio do Comitê de Governança Digital (CGD) responsabilidade pela aprovação do programa de desenvolvimento de pessoas em ações relacionadas à segurança da informação e privacidade, incluindo a obrigatoriedade de participação em curso básico relacionado à privacidade e segurança da informação, abrangendo tópicos como proteção de dados, boas práticas de segurança cibernética, como pré-requisito para toda força de trabalho da UFAM em conformidade com a LGPD e normativos internos, bem como prover recursos financeiros e suporte técnico para a implementação eficaz desta política.

Cabe aos gestores/dirigentes de departamentos/unidades, a responsabilidade de planejar e estimular a participação em ações de capacitação de seus subordinados e designar responsáveis pela privacidade e segurança da informação em cada setor para



coordenar e solicitar treinamento para cada área específica aos processos de trabalho de sua unidade, além de conscientizar e monitorar a comunidade acadêmica sob sua supervisão em relação aos conceitos e incorporando práticas de segurança da informação, como preceitua a Política de Segurança da Informação da UFAM.

Cabe a todos os servidores, terceirizados e usuários da comunidade acadêmica da Universidade Federal do Amazonas a obrigação e responsabilidade de participar regularmente de programas de treinamento e conscientização sobre privacidade e segurança da informação, implementando e difundindo os conceitos ensinados e seguir as diretrizes e procedimentos estabelecidos com a responsabilidade de proteger as informações confidenciais e a privacidade dos dados, identificando e relatando imediatamente qualquer incidente de segurança ou violação de dados no âmbito da instituição.

4.6 Orçamento

A Universidade Federal do Amazonas deve:

- Somente realizar despesas com ações de desenvolvimento de pessoas em privacidade e segurança da informação, após aprovação do PDP, conforme disposto no art. 16 do Decreto nº 9.991, de 28 de agosto de 2019;
- Destinar orçamento a ações de desenvolvimento internos para execução de cursos presenciais ou híbridos, em segurança da informação e privacidade, como planejamento do LAD - Levantamento das Ações de Desenvolvimento para ações de curta duração: cursos, congressos, encontros, conferências, seminários, simpósios, fóruns, mesas-redondas ou outros eventos de mesma natureza;
- Alocar recursos adequados e utilizar de modo efetivo os recursos orçamentários destinados ao fomento do desenvolvimento de pessoas em privacidade e segurança da informação;



- Publicar na internet, de forma transparente e objetiva, todas as despesas com as ações de desenvolvimento de pessoas em privacidade e segurança da informação, conforme disposto no art. 16 do Decreto nº 9.991, de 28 de agosto de 2019;
- Analisar o custo-benefício das despesas realizadas no exercício anterior com as ações de desenvolvimento de pessoas em privacidade e segurança da informação, conforme disposto no art. 3º do Decreto nº 9.991, de 28 de agosto de 2019.
- O planejamento das ações de desenvolvimento de pessoas em privacidade e segurança da informação da Universidade Federal do Amazonas deve estar de acordo com os princípios da economicidade e da eficiência, conforme disposto no art. 3º do Decreto nº 9.991, de 28 de agosto de 2019.

4.7 Treinamento e Conscientização

Deve ser previsto que a Universidade Federal do Amazonas realize periodicamente atividades de um programa de conscientização e campanhas sobre privacidade e segurança da informação, para todos os membros da força de trabalho, com dicas de boas práticas do uso da internet em computadores e dispositivos móveis em geral, publicação e distribuição de cartilhas, boletins e folhetos (impressos e/ou digitais), além de realização de workshops, palestras e seminários com especialistas na área.

Ações permanentes de conscientização por meio de campanhas nas mídias institucionais, sob gerenciamento da Assessoria de Comunicação - ASCOM, voltadas a toda a comunidade acadêmica, a partir da edição de um conteúdo básico indicado pelo CTIC, CGD e Encarregado de Dados.

Os treinamentos pela Universidade Federal do Amazonas devem estar alinhados com as melhores práticas de tratamento de dados pessoais, privacidade e segurança da informação, em especial as recomendações do guia do framework PPSI:

- I. Como reconhecer ataques de engenharia social;



Treinar os membros da força de trabalho para reconhecer ataques de engenharia social, como phishing, golpes de telefone e chamadas realizadas por impostores, pretexto e uso não autorizado.

II. Melhores práticas de autenticação;

Treinar os servidores sobre a importância de habilitar utilizar as melhores práticas de autenticação segura como MFA (Multi-factor Authentication – Autenticação de múltiplos fatores), composição de senha e gestão de credenciais.

III. Melhores práticas de tratamento de dados;

Treinar os servidores sobre como identificar e armazenar, transferir, arquivar e destruir informações sensíveis adequadamente (incluindo dados pessoais). Isso também inclui o treinamento sobre práticas recomendadas de mesa e tela limpas, quadros físicos e virtuais limpos e armazenar dados e ativos com segurança.

IV. Sobre as causas da exposição não intencional de dados;

Treinar os servidores para estarem cientes das causas da exposição não intencional de dados. Como a entrega incorreta de dados sensíveis, perda de dispositivo móvel/portátil ou publicação de dados para públicos indesejados.

V. Como reconhecer e relatar incidentes de segurança da informação;

Treinar os servidores para serem capazes de identificar os indicadores mais comuns de um incidente e serem capazes de relatar tal incidente.

VI. Como identificar e comunicar se os seus ativos institucionais estão desatualizados em relação a segurança;

Treinar os servidores para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em ferramentas e processos automatizados. É



importante incluir nesse treinamento a etapa de notificação do pessoal de TI sobre quaisquer falhas em processos e ferramentas automatizadas que estejam ocorrendo.

VII. Sobre os perigos de se conectar e transmitir dados institucionais em redes inseguras;

Treinar os servidores sobre os perigos de se conectar e transmitir dados em redes inseguras para atividades corporativas. Se a organização tiver funcionários remotos, o treinamento deve incluir orientação para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.

VIII. Treinamento de competências e conscientização de segurança para funções específicas;

Para servidores que atuem em funções específicas, realize o treinamento de conscientização de segurança e de competências específicas para estas funções, como listados em planilha anexo A.

Garantir treinamentos específicos voltados à privacidade e segurança da informação, como ações de desenvolvimento internos para o público em geral no PDP ou indicados via Escolas de Governo, através do LAD - Levantamento de Ações de Desenvolvimento e divulgado no Calendário de Ações de Desenvolvimento.

Garantir que todos os responsáveis pelo desenvolvimento de software recebam treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicas. O treinamento deve incluir princípios gerais de segurança e práticas padrão de segurança para aplicações. O treinamento deve ser realizado periodicamente, é interessante estabelecer uma cultura de segurança entre os desenvolvedores.

Garantir que todos os responsáveis pela rede de dados e datacenter recebam treinamento para administração e configuração segura do ambiente de comunicação de



dados. O treinamento deve ser realizado periodicamente, buscando estabelecer uma cultura de segurança entre os administradores.

Garantir ações de capacitação dos agentes responsáveis pelo uso dos recursos criptográficos, observando as normas vigentes, os procedimentos de credenciamento de segurança, e o tratamento de informação classificada.

IX. Outras temáticas emergentes que poderão ser abordadas em treinamentos;

Inclusão de treinamento específico voltado aos servidores recém-ingressos na instituição como parte da capacitação do programa de integração de pessoal da Ufam;

Inclusão de treinamento específico voltado aos gestores no PDG (Plano de Desenvolvimento de Gestores), que é gerenciado pela Progesp;

Inclusão de treinamento em segurança da informação e privacidade, como pré-requisitos para participação no Programa de Gestão por Resultados EVT/PGR nas modalidades presencial e teletrabalho.

Treinamento sobre Políticas e regulamentos relevantes (Compliance), como GDPR, LGPD, ISO, NIST, HIPAA, entre outros.

Garantir treinamentos especializados em TI/SI e firmando parcerias com Escolas de Governo ou fomentando em Escolas Privadas de conteúdo específico contratadas conforme anexo A, além garantir voucher de certificações internacionais, conforme estabelecida no DOU Nº 68, de 10 Abril 2013 - Seção 1, Portaria nº 12, de 9 de abril de 2013, que homologa a NC nº 18 /IN01/DSIC/GSIPR, e cita a lista de entidades certificadoras como: CompTIA, EXIN, EC-Concil entre outras.

A Universidade Federal do Amazonas, através do Plano de Desenvolvimento de Pessoas, deve definir os níveis de conhecimento e habilidade necessários para os servidores incluindo gestores, técnicos administrativos em educação, docentes, discentes,



terceirizados, estagiários e prestadores de serviços, executarem deveres e tarefas relacionadas à Privacidade e Segurança da Informação.

4.8 Ações de desenvolvimento prioritárias

Durante a realização do planejamento das ações prioritárias de desenvolvimento de pessoas deve-se criar um quadro com a programação das atividades, no qual contenha para cada ação de desenvolvimento do servidor e/ou colaborador da Universidade Federal do Amazonas:

Formato de quadro da programação: nome do evento ou ação; período; modalidade; carga horária; público alvo; vagas; período inscrições; local de inscrições; relatório final.

As ações de desenvolvimento prioritárias da Universidade Federal do Amazonas devem ser definidas dentre as relacionadas a seguir:

I. ações que visam ao atendimento às necessidades diagnosticadas com base em avaliações da instituição e, ou, de seu planejamento estratégico da Universidade Federal do Amazonas;

II. curso introdutório financiado pela Universidade Federal do Amazonas, principalmente nas ações voltadas exclusivamente aos servidores recém-ingressos, abordando os princípios básicos de Privacidade e Segurança da Informação na administração pública, entre outros;

III. treinamentos básicos devem ser obrigatórios previstos em legislação específica LGPD e normativos internos sobre a temática de Privacidade e Segurança da Informação;

IV. ações destinadas ao desenvolvimento gerencial e reconhecimento de responsabilidades sobre proteção de dados e segurança da informação;



V. ações que busquem elevar a maturidade e a resiliência da Universidade Federal do Amazonas, em termos de privacidade e segurança da informação que estejam alinhadas com o PPSI;

VI. as ações de treinamento e conscientização realizadas pela Universidade Federal do Amazonas que visam de forma contínua manter os servidores e/ou colaboradores atualizados sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade e de segurança da informação da organização;

VII. cursos de caráter permanente coordenados e realizados em parceria com as escolas de governo, outras instituições privadas e/ou pessoas físicas direcionado a segurança da informação, privacidade e proteção de dados pessoais, conforme as funções das pessoas envolvidas com o tratamento de dados pessoais e segurança cibernética;

VIII. exercícios práticos de conscientização de segurança da informação que simulam ataques cibernéticos;

IX. gamificação como metodologia motivacional para elevar o engajamento da equipe e o comprometimento nos treinamentos, definindo objetivos claros e estabelecer sistemas de recompensas para ajudar os participantes a absorverem os aprendizados de forma rápida, descontraída e cativante;

X. conscientização de segurança da informação sobre reconhecimento e relato de potenciais indicadores de ameaça interna;

XI. treinamento em privacidade e segurança da informação baseado em funções para o servidor e/ou colaborador designando papéis e responsabilidades;



XII. treinamentos presenciais ou EAD regulares e workshops, palestras, seminários sobre privacidade e segurança da informação devem ser periódicos, além de apoio à participação em eventos externos, como conferências e cursos especializados;

XIII. Incentivo à obtenção de certificações reconhecidas pelo mercado e pelo meio acadêmico, através de programas de formação continuada e especialização na área de privacidade e segurança da informação.

4.9 Procedimentos para solicitações de ações de desenvolvimento de pessoas

Os procedimentos para solicitações de ações de desenvolvimento de pessoas em privacidade e segurança da informação devem estar previstos no Plano de Desenvolvimento de Pessoas do órgão.

A solicitação para participação de servidor da Universidade Federal do Amazonas em ações de desenvolvimento deve ser feita mediante as regras vigentes para inscrição nas ações de desenvolvimento.

A participação em ação de desenvolvimento que implica em despesas diárias e passagens somente pode ser realizada se o custo total da ação for compatível ao custo da participação em evento similar na própria localidade de exercício do interessado, podendo ser aprovada, mediante justificativa, pela autoridade competente.

Servidores ou colaboradores podem solicitar treinamentos específicos em privacidade e segurança da informação, a sua chefia imediata, que avaliará as solicitações, devendo articular-se para sempre priorizar a participação dos seus subordinados nas ações de desenvolvimento conforme a necessidade e de acordo com esta Política.



4.10 Afastamento para capacitação

É considerado afastamento para participação relevante em ações de desenvolvimento da Universidade Federal do Amazonas a:

- I. Licença para capacitação, nos termos do disposto no art. 87 da Lei nº 8.112, de 11 de dezembro de 1990;
- II. Participação em programa de pós-graduação stricto sensu no País, conforme o disposto no art. 96-A da Lei nº 8.112, de 11 de dezembro de 1990;
- III. Realização de estudo no exterior, conforme o disposto no art. 95 da Lei nº 8.112, de 1990.

Os afastamentos podem ser concedidos pela Universidade Federal do Amazonas, entre outros critérios, quando a ação de desenvolvimento:

- I. Estiver prevista no PDP do órgão ou da entidade do servidor;
- II. Estiver alinhada ao desenvolvimento do servidor nas competências relativas ao Art. 19, II do Decreto Nº 9.991, de 28 de agosto de 2019;
- III. Dispor de horário ou o local que inviabilize o cumprimento das atividades previstas ou a jornada semanal de trabalho do servidor;

Os afastamentos podem ser interrompidos, a qualquer tempo, a pedido do servidor ou no interesse da administração da Universidade Federal do Amazonas.

A licença para capacitação da Universidade Federal do Amazonas deve observar a Lei Nº 8.112, de 11 de dezembro de 1990, o que consta no decreto Nº 9.991, de 28 de agosto de 2019 e demais normas correlatas.



5.DISPOSIÇÕES FINAIS

Para garantir a efetividade desta política na obrigatoriedade do treinamento como pré-requisito básico em segurança da informação e privacidade, será implementado um mecanismo de mensuração da participação nos cursos:

Registro de Presença: O servidor deverá registrar sua presença nos cursos por meio de sistemas internos ou plataformas de treinamento.

Avaliações de Aprendizado: Os servidores serão avaliados quanto ao conhecimento adquirido. Avaliações podem ser realizadas após a conclusão dos cursos.

Relatórios Periódicos: O coordenador responsável designado pelo setor gerará relatórios periódicos com informações sobre a participação da sua equipe nos cursos. Esses relatórios serão compartilhados com os gestores.

Penalidades: A área responsável pelo desenvolvimento de pessoas acompanhará regularmente a participação nos cursos. Servidores que não cumprirem a obrigatoriedade do pré-requisito básico definido, estarão sujeitos a medidas disciplinares, como advertências ou outras penalidades previstas na legislação interna.

A eficácia desta política será avaliada regularmente por meio de monitoramento, pesquisas de satisfação, auditorias internas, feedback dos colaboradores e análise de incidentes de segurança e com base nessas avaliações, serão implementadas melhorias contínuas e revisões periódicas dos programas de treinamento, para fortalecer a conscientização e a postura de segurança da instituição. essencial para manter a integridade e a confidencialidade das informações.



6. REVISÃO E ATUALIZAÇÃO

Esta política deverá ser revisada e atualizada anualmente ou conforme necessário para garantir sua relevância e assegurar as melhores práticas e conformidades frente às mudanças regulatórias e tecnológicas.

7. VIGÊNCIA

Esta política entra em vigor na data de sua publicação.