UNIVERSIDADE FEDERAL DO AMAZONAS
UFAM

Política de Segurança da Informação e Comunicações
PoSIC

Maio 2024

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

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 Vitório 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

EQUIPE TÉCNICA DE ELABORAÇÃO E REVISÃO

Márcia Regina Moraes de Paula

Gilberto Aires Libania

Relatoria no CONSAD

Professor Doutor José Luiz de Souza Pio

Histórico de Versões

Data	Versão	Descrição	Autor (a)
11/03/2020	1.0	Elaboração da Política de Segurança da Informação e Comunicações.	Márcia de Paula
08/08/2022	1.1	Inclusão de versionamento.	Márcia de Paula
26/08/2022	1.2	Revisão dos fundamentos legais e normativas.	Gilberto Libania
25/09/2022	1.2.1	Formatação.	Márcia de Paula
09/05/2024	2.0	Revisão e inclusão das sugestões da relatoria no CONSAD.	Márcia de Paula e Gilberto Libania

SUMÁRIO

1. FINALIDADE

A Política de Segurança da Informação e Comunicações (PoSIC) da Universidade Federal do Amazonas (UFAM), de cunho estratégico, é uma declaração formal da Instituição acerca do seu comprometimento com vistas a prover e assegurar proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os servidores (técnicos administrativos e docentes), colaboradores, consultores externos, prestadores de serviços, estagiários e discentes que exerçam atividades no âmbito da UFAM ou quem quer que tenha acesso a dados ou informações no ambiente da UFAM. O seu propósito é estabelecer diretrizes, normas e procedimentos, atribuindo responsabilidades e competências adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes à UFAM.

2. FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicações da UFAM são:

a) **Lei nº 13.709, de 14 de agosto de 2018:** institui a Lei Geral de Proteção de Dados Pessoais (LGPD), alterada pela Lei nº 13.853, de 8 de julho de 2019, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências;

b) **Lei nº 12.527, de 18 de novembro de 2011:** regula o acesso a informações, previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal, e dá outras providências;

c) **Lei nº 9.983, de 14 de julho de 2000:** dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

d) **Lei nº 8.429 de 2 de junho de 1992:** dispõe sobre as sanções aplicáveis em virtude da prática de atos de improbidade administrativa, de que trata o § 4º do art. 37 da Constituição Federal; e dá outras providências, alterada pela Lei nº 14.230, de 25 de outubro de 2021;

e) **Lei nº 8.159, de 8 de janeiro de 1991:** dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

f) **Lei nº 8.027 de 12 de abril de 1990:** dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;

g) **Decreto 1.171, de 22 de junho de 1994:** aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

h) **Decreto nº 9.637, de 26 de dezembro de 2018:** institui a Política Nacional de Segurança da Informação - PNSI nos órgãos e entidades da Administração Pública com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional, dispõe sobre a governança da segurança da informação e dá outras providências, alterado pelo Decreto nº 9.832, de 12 de junho de 2019, para dispor sobre o Comitê Gestor da Segurança da Informação;

i) **Decreto nº 7.845, de 14 de novembro de 2012:** regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

j) **Decreto nº 10.332, de 28 de abril de 2020:** institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências, revoga o Decreto nº 8.638, de 15 de janeiro de 2016;

k) **Decreto nº 11.529, de 16 de maio de 2023:** institui o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a

Política de Transparência e Acesso à Informação da Administração Pública Federal;

l) **Instrução Normativa GSI/PR nº 01, 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, alterada pela Instrução Normativa GSI nº 2 - 24 de julho de 2020;

m) **Instrução Normativa GSI/PR nº 02, de 5 de fevereiro de 2013:** dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

n) **Instrução Normativa GSI/PR nº 03, de 6 de março de 2013:** dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

o) **Instrução Normativa GSI/PR nº 03 - 28 de maio de 2021:** dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

p) **Instrução Normativa GSI/PR nº 05 - 31 de agosto de 2021:** dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

q) **Instrução Normativa GSI/PR nº 06 - 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;

r) **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);

s) **Norma ABNT NBR ISO/IEC 27002:2013:** fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações;

t) **Norma ABNT NBR ISO/IEC 27005:2019:** fornece diretrizes para o processo de gestão de riscos de segurança da informação.

3. DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

A alta administração da UNIVERSIDADE FEDERAL DO AMAZONAS, na pessoa do(a) Reitor(a), declara-se comprometida em proteger todos os seus ativos de informação, proporcionando-lhes, sempre que possível, todos os recursos que se fizerem necessários.

4. INSTÂNCIAS ADMINISTRATIVAS

Para os efeitos desta Política e das normas nela originadas, entende-se por:

a) **Comitê de Governança Digital (CGD):** instância colegiada consultiva e deliberativa no âmbito da UFAM, para deliberar sobre os assuntos relativos à implementação das ações de Governo Digital e ao uso de recursos de tecnologia da informação e comunicação, que atende ao disposto no Art. 2º do Decreto nº 10.332, de 28 de abril de 2020, responsável pela Política de Governança Digital, do qual fazem parte o Plano Diretor de Tecnologia da Informação (PDTI) e a Política de Segurança da Informação (PoSIC)

b) **Centro de Tecnologia da Informação e Comunicação (CTIC):** instância administrativa/executiva responsável por propor as políticas e programas da UFAM na área de informática e telecomunicações, bem como por sua implementação e gestão;

c) **Coordenação de Segurança da Informação (CSEGINFO):** instância responsável por propor políticas, programas e desenvolvimento, como também a implantação e manutenção dos recursos e serviços relacionados a segurança da informação e comunicação no âmbito da UFAM;

d) **Grupo de Trabalho em Segurança da Informação e Comunicação (GT-SIC):** instância técnica sob gestão da CSIC, responsável em auxiliar na gestão de SIC de forma a analisar, elaborar, classificar, políticas e normas, decidir e documentar os procedimentos e suas competências e encaminhar ao CGD para aprovação;

e) **Equipe de Tratamento e Resposta à Incidentes de Segurança da Informação e Comunicação (ETIR):** instância executiva e sob gestão do CSIC que atende as Normas Complementares nº 05/ 08/ 21/ IN01/DSIC/GSIPR, responsável por detectar, prevenir, classificar, registrar, tratar e responder aos incidentes de segurança da informação, envolvendo as redes de abrangência computacional da UFAM, e suas instituições parceiras interconectadas além de elaborar, promover ações educativas e disseminar boas práticas de segurança da informação baseadas nas políticas institucionais, e por sua implementação e gestão;

5. TERMOS E DEFINIÇÕES

Para os efeitos desta PoSIC, são estabelecidos os seguintes conceitos e definições:

a) **Ameaça:** qualquer evento que explore vulnerabilidades ou seja causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

b) **Ativo:** qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha valor para a organização;

c) **Ativos de Informação:** qualquer informação que tenha valor para a Instituição. Os meios de armazenamento, transmissão e processamento. Os sistemas de informação, além das informações em si, bem como os locais em que se encontram esses meios e as pessoas que têm acesso a eles;

d) **Autenticidade:** propriedade que estabelece a validade de que a informação foi produzida, transmitida, modificada ou destruída por um determinado remetente, de forma que o destinatário possa comprovar a origem da informação.

e) **Classificação da informação:** identificação dos níveis de proteção que as informações demandam. Atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas;
f) **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados ou não credenciado;
g) **Controle:** medida ou conjunto de medidas adotadas para gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.
h) **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
i) **Custodiante do ativo de informação:** qualquer pessoa física ou jurídica que detém a posse, mesmo que transitória, de informação produzida ou recebida pela instituição;
j) **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
k) **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;
l) **Gestão de Ativos:** processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada de seu controle;
m) **Gestão de Continuidade de Negócios:** processo contínuo de gestão e governança suportado pela alta direção de planejamento e resposta 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 e previamente definido;

n) **Gestão de Incidentes de Segurança da Informação e Comunicação:** processo contínuo que vise registrar e tratar os incidentes de segurança da informação e comunicação, fornecendo respostas ágeis e adequadas a estes, bem como soluções oportunas para incidentes recorrentes;

o) **Gestão de Segurança da Informação e Comunicações:** ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;

p) **Gestão de riscos de Segurança da Informação e Comunicações:** conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para mitigar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

q) **Incidente de segurança da informação:** evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação;

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

s) **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

t) **Não-repúdio:** propriedade que visa garantir que um autor não negue a criação e assinatura de determinado documento;

u) **Política de Segurança da Informação e Comunicações:** documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

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

w) **Risco de segurança da informação:** combinação de probabilidade de um evento indesejado associado a um ativo de informação ou a um conjunto de ativos de informação, com impacto negativo no negócio para organização;

x) **Segurança da informação:** preservação da confidencialidade, da integridade e da disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem estar envolvidas;

y) **Termo de sigilo e responsabilidade:** acordo de confidencialidade e não divulgação de informações que atribui responsabilidades ao servidor e administrador de serviço quanto ao sigilo e a correta utilização dos ativos de propriedade ou custodiados da Instituição. Prestadores de serviços que, por força de contratos de suporte e manutenção de sistemas, ficam sujeitos às mesmas condições;

z) **Tratamento da informação:** conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

aa) **Tratamento de incidentes:** processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências potenciais futuras;

bb) **Tratamento dos riscos:** processo e implementação de ações de segurança da informação e comunicações, com o objetivo de evitar, reduzir, reter ou transferir um risco;

cc) **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

6. PRINCÍPIOS

Esta política abrange os seguintes aspectos básicos da Segurança da Informação e Comunicações, destacados a seguir:

a) **Confidencialidade:** somente pessoas devidamente autorizadas pelo gestor da informação devem ter acesso à informação não pública;

b) **Integridade:** somente operações de alteração, supressão e adição autorizadas devem ser realizadas nas informações;

c) **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

d) **Autenticidade:** princípio de segurança que valida que a informação foi produzida, transmitida, modificada ou destruída por um determinado remetente;

e) **Criticidade:** princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

f) **Não-Repúdio:** garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

g) **Responsabilidade e ciência:** as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os servidores da UFAM são responsáveis pelo tratamento da informação e pela ciência e cumprimento das Normas de Segurança da Informação e Comunicações advindas desta política;

h) **Ética:** os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIC;

i) **Legalidade:** além de observar os interesses da UFAM, as ações de Segurança da Informação e Comunicações levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e direitos de uso;

j) **Publicidade:** transparência no trato da informação, observados os critérios legais;

k) **Proporcionalidade:** o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações na UFAM serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

7. ESCOPO

O escopo da Política de Segurança da Informação e Comunicações da UFAM refere-se:

a) Aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que as incorporarão;

b) Aos requisitos de segurança humana;

c) Aos requisitos de segurança física;

d) Aos requisitos de segurança lógica;

e) À sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços oriundos da informação e comunicação da UFAM.

8. ESTRUTURA DA POSIC

A POSIC da UFAM é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

a) **Política de Segurança da Informação e Comunicações (PoSIC):** constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação e Comunicações e será detalhada em documentos denominados Normas.

b) **Normas de Segurança da Informação e Comunicações (Normativas):** estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas instâncias em que a informação é

tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações determinadas pelo Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações no âmbito da Administração Pública Federal.

c) **Procedimentos de Segurança da Informação e Comunicações (Procedimentos):** instrumentalizam o disposto nas Normas, permitindo a direta aplicação nas atividades da UFAM, cabendo a cada gestor a responsabilidade de gerá-los. Cada procedimento poderá ainda ser detalhado em instruções.

9. DIRETRIZES GERAIS

a) É política da UFAM prover para a sua comunidade o acesso a fontes de informação locais, nacionais e internacionais, promovendo um ambiente de produção, uso e compartilhamento do conhecimento e de comprometimento com a liberdade acadêmica.

b) Zelar pela Segurança da Informação e Comunicações é dever de todos, independentemente de forma ou meio pelo qual a informação seja apresentada ou compartilhada, deve-se protegê-la adequadamente.

c) O acesso à informação será regulamentado por normas específicas de tratamento da informação.

d) Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela UFAM é considerada seu patrimônio e deve ser protegida.

e) Os recursos disponibilizados pela UFAM, de sua propriedade, são fornecidos com o propósito único de garantir o desempenho das suas atividades.

f) As normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação serão definidas de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor.

g) A UFAM, como usuário dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança.

10. DIRETRIZES ESPECÍFICAS

a) **Gestão de Segurança da Informação:** deve-se estabelecer macroprocesso que consiste na implementação desta política e demais controles voltados para iniciar, implementar, manter e promover a melhoria contínua da gestão de segurança da informação na instituição, a partir do apoio dos responsáveis descritos nesta política. Tais controles devem objetivar a preservação da confidencialidade, integridade e disponibilidade da informação, e, adicionalmente propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade.

b) **Classificação e Tratamento das Informações:** deve-se instituir processo que vise garantir que cada informação tenha o tratamento de segurança adequado à sua importância para a instituição. A informação deve ser classificada em termos de seu valor, requisitos legais, criticidade e sensibilidade de modo a evitar modificação ou divulgação não autorizada.

c) **Controle de acesso à informação e aos recursos e serviços de tecnologia da informação e comunicação:** deve-se garantir que o acesso à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação. As regras de controle de acesso a todos os sistemas institucionais, internet, intranet, informações, dados, instalações físicas da instituição, bem como uso de senhas, e-mail, telefonia digital, dispositivos móveis, estações de trabalho, redes sociais e computação em nuvem, deverão ser definidas e regulamentadas por normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição. O acesso aos recursos e serviços de tecnologia da informação deve ser compatível com as necessidades institucionais e acadêmicas dos usuários. O acesso às informações que não sejam públicas deve ser restrito às pessoas

que tenham necessidade de conhecê-las e se submetem a controles compatíveis com a classificação quanto à confidencialidade. Havendo necessidade de acesso a informações não públicas por pessoas com vínculo transitório com a instituição, é obrigatório o aceite de termo de sigilo e responsabilidade.

d) **Gestão de Riscos de Segurança da Informação e Comunicação:** deve-se estabelecer processo contínuo e aplicado que tenha por objetivo realizar o diagnóstico preventivo de riscos de segurança da informação com intuito de definir quais são aceitáveis e quais necessitam de controles especiais, priorizando seu tratamento e evitando a ocorrência de incidentes. O apetite a risco, a probabilidade e o impacto da materialização do risco devem direcionar a definição dos controles a serem adotados. Os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação. As normas estabelecidas devem estar em conformidade com a Política de Gestão de Riscos da Universidade Federal do Amazonas.

e) **Gestão de Incidentes de Segurança da Informação e Comunicação:** deve-se estabelecer processo que vise registrar e tratar os incidentes de segurança da informação e comunicação, fornecendo respostas ágeis e adequadas a estes, bem como soluções oportunas para incidentes recorrentes. Para incidentes relacionados especificamente a serviços de TIC, deve-se instituir Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) responsável por receber, analisar e responder a incidentes relacionados à segurança em redes de computadores. As regras de comunicação, registro e tratamento devem ser definidas e regulamentadas por normas internas. Todos os agentes públicos e colaboradores da instituição são responsáveis por informar aos responsáveis os incidentes de segurança do qual tenham ciência ou suspeita, bem como colaborar, na respectiva área de competência, na identificação e no tratamento de incidentes em segurança da informação.

f) **Gestão de Continuidade de Negócios:** disposta em política específica, harmoniza-se com os processos de gestão de segurança da informação e

comunicação e tem por objetivo, em relação à segurança da informação, garantir níveis adequados de disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informações essenciais ao funcionamento dos processos críticos de negócio da instituição. A segurança da informação deve ser parte integrante do processo global de continuidade, de forma que os requisitos de segurança da informação necessários para a continuidade do negócio da instituição sejam contemplados.

g) **Gestão de Ativos Associados à Informação:** deve-se instituir processo que identifique os ativos associados à informação e ao processamento da informação, definindo localização, custodiante e importância do ativo para a instituição. Tal inventário deve fornecer uma compilação de valor para a Gestão de Riscos de Segurança da Informação.

h) **Auditoria e Conformidade:** Com o intuito de possibilitar auditoria e fornecer evidências de conformidade aos requisitos e eficácia dos processos gestão de segurança da informação, deve-se estabelecer registros identificáveis e recuperáveis, com controles que disponha sobre identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição. Estes registros devem servir como evidência da aderência aos requisitos desta política, bem como promover a *accountability*, ao reportar desvios e violações a normas, de modo que ações corretivas possam ser tomadas e os responsáveis responsabilizados por suas ações. Todos os agentes públicos e colaboradores da instituição são responsáveis por verificar regularmente as conformidades e manter tais registros dentro de sua área de atuação.

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. As ações devem ser compatíveis com os papéis, responsabilidades e habilidades da pessoa, permitindo que as mesmas respondam de acordo com os requisitos de segurança da informação da sua área

de atuação. É de responsabilidade dos dirigentes das unidades e demais gestores da instituição, conscientizar servidores e colaboradores sob sua supervisão em relação aos conceitos e às práticas de segurança da informação, incorporando práticas de segurança da informação aos processos de trabalho de sua unidade. Serão incluídas, de ofício, no Plano de Desenvolvimento de Pessoas do Órgão, ações de desenvolvimento relativas a esta Política, inclusive por meio de ações obrigatórias direcionadas aos servidores recém-empossados.

11. COMPETÊNCIAS E RESPONSABILIDADES

A implementação, o controle e a gestão da PoSIC são de responsabilidade da seguinte infraestrutura de gerenciamento:

a) A autoridade máxima é o Reitor(a), responsável pela aprovação da Política de Segurança da Informação e Comunicação da UFAM;

b) Ao Comitê de Governança Digital (CGD) compete:
   i) Formular e conduzir diretrizes relacionadas para a Gestão de Segurança da Informação e Comunicação e a Política de Segurança da Informação e Comunicação, bem como avaliar periodicamente sua efetividade;
   ii) Propor a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação;
   iii) Apoiar a implantação de soluções para eliminação ou minimização de riscos;
   iv) Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;
   v) Acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;
   vi) Executar outras funções que, por sua natureza, lhe estejam afetas ou lhe tenham sido atribuídas.

c) Ao Gestor de Segurança da Informação e Comunicação compete:

i) Promover e disseminar a cultura de segurança da informação e comunicação.
ii) Propor normas e procedimentos relativos à Segurança da Informação e Comunicações;
iii) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança.
iv) Propor recursos necessários às ações de Segurança da Informação e Comunicações;
v) Realizar e acompanhar estudos de novas tecnologias e impactos na segurança da informação e comunicações;
vi) Coordenar as ações de segurança da informação e comunicações;

d) À Equipe de Tratamento de Incidentes em Redes de Computadores (ETIR) compete:

i) Coordenar as atividades de tratamento e resposta aos incidentes em redes de computadores;
ii) Agir proativamente com o objetivo de prevenir incidentes de segurança a partir do monitoramento de alertas e vulnerabilidades dos recursos e serviços de tecnologia da informação e comunicação, e por meio da divulgação de práticas e recomendações de segurança da informação e comunicação;
iii) Executar ações reativas, a partir da notificação de incidentes de segurança, de análise e resposta, avaliando causas e responsáveis e demais ações necessárias para tratar violações de segurança;
iv) Realizar coleta e preservação de evidências de incidentes de segurança em redes em conformidade com exigências legais pertinentes.
v) Fornecer indicadores quantitativos acerca dos incidentes ocorridos que subsidiem o planejamento em segurança da informação.
vi) Cooperar com outras equipes de tratamento e resposta a incidentes;
vii) Executar vigilância tecnológica contínua pertinente a sua área de atuação.

12. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e as Normas de Segurança da Informação e Comunicação como também suas atualizações deverão ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados da UFAM, e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.

a) As áreas atingidas por esta PoSIC são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento.
b) As áreas deverão submeter suas propostas de normas ao Comitê Governança Digital para análise, discussão e aprovação no âmbito do Comitê;
c) Após aprovação, estas normas e procedimentos serão divulgadas aos interessados pela área responsável por sua proposição e manutenção.

13. REVISÕES E ATUALIZAÇÃO

Esta PoSIC como todos os instrumentos normativos gerados pela própria, será revista e alterada sempre que se fizer necessário, sendo ainda obrigatória a sua revisão anual.

14. VIOLAÇÕES, PENALIDADES E SANÇÕES

Nos casos em que houver o descumprimento ou violação de um ou mais itens da Política ou das suas normas, procedimentos ou atividades pertinentes à Segurança da Informação e Comunicação, estas serão tratadas conforme legislação e regulamentos internos institucionais aplicáveis, sem prejuízo de outras penalidades previstas nas esferas civil e penal, em especial o que consta:

a) Na Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;

b) No Código de Ética do Servidor Público do Poder Executivo Federal, aprovado pelo Decreto n nº 1.171/1994;

c) No Código Penal, através do Decreto-Lei n nº 2.848/1940;

d) Da Lei nº 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

e) No Decreto nº 4.553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança, da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

15. VIGÊNCIA

A presente Política entra em vigor a partir da data de sua publicação.