

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 07/03/2018 | Edição: 45 | Seção: 1 | Página: 46-47-61

Órgão: Ministério da Integração Nacional/Superintendência do Desenvolvimento da Amazônia

DIRETORIA COLEGIADA

RESOLUÇÃO N° 20, DE 1º DE FEVEREIRO DE 2018

A DIRETORIA COLEGIADA DA SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA-SUDAM, com base no disposto na Lei Complementar nº 124, de 03 de Janeiro de 2007 e, no uso das atribuições que lhe confere o art. 6º, II, do anexo I do Decreto nº 8.275, de 27/06/2014, publicado no DOU de 30/06/2014 e o art. 10, II do Regimento Interno desta Autarquia; e

Considerando o disposto no processo nº 59004.000345/2014-80, resolve:

Art. 1º - Aprovar a Política de Segurança da Informação e das Comunicações - POSIC e seus anexos I e II, dispondo sobre o manuseio, tratamento, controle e a proteção dos dados, informações e conhecimentos produzidos na SUDAM.

Art. 2º - O objetivo consiste em estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações na SUDAM.

Parágrafo único. A POSIC obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.

Art. 3º - Para fins dessa Política, considera-se.

I - Acesso: possibilidade de consulta ou reprodução de documentos e arquivos;

II - Agente Público: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, à SUDAM;

III - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

IV - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

V - Ativo da Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - Ativo Sigiloso: qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;

VII - Autenticação: ato de comprovar que um objeto ou pessoa é realmente verdadeiro (a) e autêntico (a).

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

IX - Ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua autenticidade, confidencialidade, integridade e disponibilidade;

X - Classificação da informação: grau de sigilo dado à informação, documento, material, área ou instalação;

XI - Colaborador: pessoa que presta serviço em razão de contratos administrativos firmados na forma da Lei e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação de qualquer tipo, convênios e termos congêneres;

XII - Comitê de Segurança da Informação e das Comunicações da SUDAM (CSIC): grupo de servidores com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da SUDAM;

XIII - Comitê Estratégico de Tecnologia da Informação e Comunicação da SUDAM (CETIC) - grupo de servidores com a responsabilidade de estabelecer as políticas e diretrizes de tecnologia da informação alinhadas às estratégicas da SUDAM;

XIV - Confidencialidade: garantia de que somente pessoas/órgãos ou sistemas autorizados tenham acesso às informações transmitidas ou mantidas em redes ou sistemas de comunicação;

XV - Contingência: descrição de medidas a serem tomadas por uma organização, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos;

XVI - Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XVII - Cópia de Segurança: copiar dados em meio separado do original, de forma a protegê-los de qualquer eventualidade;

XVIII - Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

XIX - Criptografia: é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da chave criptográfica);

XX - Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XXI - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda da Administração;

XXII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

XXIII - Evento: ocorrência identificada em um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente conhecida que possa ser relevante para a segurança da informação;

XXIV - Gestão de Continuidade de Negócios: processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos causados nas operações da instituição caso se concretizem. Fornece e mantém um nível aceitável de serviço face às rupturas e desafios à operação normal do dia-a-dia;

XXV - Gestão de Segurança da Informação e das Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos aos quais os seus ativos de informação estão sujeitos, equilibrando-os com os custos operacionais e financeiros envolvidos;

XXVI - Gestor da Informação ou Custodiante do ativo da informação: pessoa física ou unidade da SUDAM que detém a posse, mesmo que transitória, de informação produzida ou recebida pela Instituição, cuja a responsabilidade consiste em administrar e proteger as informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

XXVII - Gestor de Segurança da Informação e das Comunicações: é responsável pelas ações de segurança da informação e das comunicações no âmbito da SUDAM, designado formalmente pelo Superintendente;

XXVIII - Grau de sigilo: gradação de segurança atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;

XXIX - Hardware: parte física do computador, formada por componentes eletrônicos.

XXX - Incidente de segurança: indício de fraude, sabotagem, desvio, falha, perda ou evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores;

XXXI - Incidentes de segurança críticos: ataques de alto risco ou possíveis comprometimentos. Uma ação imediata é necessária para abrandar o impacto destes incidentes de segurança;

XXXII - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXXIII - Informações críticas: informações de extrema importância para a sobrevivência da instituição;

XXXIV - Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

XXXV - Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXXVI - Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que a SUDAM mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, num nível previamente definido, em casos de incidentes;

XXXVII - Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXVIII - Redes Computacionais: conjunto de equipamentos interligados com o objetivo de permitir a troca de dados entre computadores e a partilha de recursos de hardware e software;

XXXIX - Segurança da Informação e das Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XL - Senha ou palavra-chave: é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema;

XLI - Sigilo: segredo de conhecimento restrito a pessoas credenciadas e protegido contra revelação não autorizada;

XLII - Sistema de Segurança da Informação: proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta restrita a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

XLIII - Software: programa de computador desenvolvido para executar um conjunto de ações previamente definidas;

XLIV - Termo de Compromisso: termo assinado pelo representante legal da empresa contratada, concordando em dar ciência a todos os seus funcionários, por ocasião de seu ingresso nas dependências da instituição, sobre a Política de Segurança da Informação e das Comunicações da SUDAM e suas Normas Complementares;

XLV - Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

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

XLVII - Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XLVIII - Usuários: servidores, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação da Superintendência do Desenvolvimento da Amazônia, formalizada por meio da assinatura do Termo de Responsabilidade;

XLIX - Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Art. 4º - Além dos princípios constitucionais que regem a Administração Pública Federal, são princípios da POSIC:

I - Responsabilidade: os agentes públicos devem conhecer e respeitar a POSIC da SUDAM e devem ser responsabilizados pelos atos que comprometem a segurança da informação;

II - Integridade: garante a inviolabilidade das informações produzidas ou recebidas com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital;

III - Publicidade: transparência das informações públicas, observados os critérios legais;

IV - Celeridade: as ações de segurança da informação e das comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;

V - Clareza: as regras de segurança da informação e das comunicações devem ser precisas, concisas e de fácil entendimento.

Art. 5º - São Preceitos da POSIC:

I - Auditabilidade: todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial;

II - Controles automáticos: sempre que possível, os controles de segurança automáticos deverão ser utilizados;

III - Defesa em profundidade: controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança;

IV - Exceção aprovada: exceções à POSIC deverão sempre ter aprovação da Diretoria Colegiada;

V - Menor privilégio: usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

VI - Mínima dependência de segredos: os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam;

VII - Resiliência: os sistemas e processos devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

VIII - Segregação de função: funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos; e

IX - Substituição da segurança em situações de emergência: controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

Art. 6º - São Diretrizes Gerais da POSIC:

I - Organização da Segurança da Informação:

a) A Política da Segurança da Informação e das Comunicações, ficará disponível permanentemente nos canais de comunicação interno e externo da SUDAM a todos os usuários após sua publicação;

b) Todos os mecanismos de proteção utilizados para a segurança da informação deverão ser mantidos para preservar a continuidade do negócio (regular exercício das funções institucionais);

c) O cumprimento dessa política, bem como das normas complementares e procedimentos de segurança da informação na SUDAM deverão ser auditados periodicamente, de acordo com os critérios definidos pelo Comitê de Segurança da Informação e das Comunicações (CSIC);

d) A SUDAM deverá criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e a sua rede interna;

e) As medidas de proteção deverão ser planejadas e os gastos na aplicação de controles deverão ser compatíveis com valor do ativo protegido;

f) O acesso às informações e sistemas dependerá da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;

g) A classificação deverá ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte;

h) Todas as regras corporativas sobre uso de internet e intranet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação da SUDAM deverá sempre ser privilegiada;

i) O correio eletrônico é uma ferramenta disponível e obrigatória para todos os servidores da SUDAM e deverá ser usado para fins exclusivamente corporativos e relacionados às atividades do usuário no âmbito da autarquia; e

j) De forma a promover a gestão dos ativos de informação e fomentar os aspectos de segurança, a SUDAM deverá instituir normas complementares que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação, observadas por todos os usuários.

II - Recursos Humanos:

a) Todos os usuários da SUDAM e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação desta autarquia e tenham acesso aos ativos da informação, deverão assinar Termo de Responsabilidade (Anexo A) quanto às informações e conhecimentos da SUDAM, o qual deverá conter todos os requisitos de segurança da informação;

b) Toda informação produzida ou recebida pelos usuários ou agentes públicos, por ocasião da função exercida e/ou atividade profissional contratada, pertence à SUDAM. As exceções deverão ser explícitas e formalizadas entre as partes;

c) As responsabilidades pela segurança da informação deverão ser definidas nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da SUDAM;

d) Todos os usuários deverão ser conscientizados e treinados nos procedimentos de segurança da informação;

e) Todo agente público deverá ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade da SUDAM e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas;

f) O controle operacional de uma atividade crítica não poderá ser atribuição exclusiva de uma única pessoa;

g) Em caso de afastamento, mudança de responsabilidades e de unidade ou de atribuições dentro da organização, far-se-á necessária a revisão imediata dos direitos de acesso e uso dos ativos;

h) Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuídos;

i) Todo ativo produzido pelo usuário no exercício de sua função deverá ser mantido pela SUDAM, garantindo o reconhecimento e o esclarecimento da propriedade do acervo para a Instituição; e

j) A conta de acesso é sigilosa, pessoal, intrasferível e de responsabilidade exclusiva do usuário.

III - Gestão de Riscos:

a) As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações da SUDAM deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estar alinhadas a esta Política de Segurança da Informação e Comunicação. Esse processo deverá ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação, contemplando inclusive as contratações de soluções de TI - para as quais deverá ser elaborado um Plano de Tratamento de Riscos.

IV - Gestão da Continuidade:

a) A SUDAM deverá elaborar e manter o Programa de Gestão de Continuidade de Negócios - PCN, aqui entendido como o "processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção".

b) O Programa de Gestão de Continuidade de Negócios da SUDAM deverá ser composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:

b.1) Plano de Gerenciamento de Incidentes (PGI): plano de ação claramente definido e documentado, a ser usado quando ocorrer um incidente, abrangendo as principais pessoas, recursos, serviços e ações necessárias para implementar o PGI.

b.2) Plano de Continuidade de Negócios (PCN): documentação dos procedimentos e informações necessárias para que a SUDAM mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, num nível previamente definido, em casos de incidentes.

b.3) Plano de Recuperação de Negócios (PRN): documentação dos procedimentos e informações necessárias para que a SUDAM operacionalize o retorno das atividades críticas à normalidade.

c) Os planos acima definidos deverão ser testados e revisados periodicamente, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

d) Para subsidiar a elaboração de seu PCN, a SUDAM deverá definir quais são suas atividades críticas, ou seja, quais devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de tal forma que permitam atingir os seus objetivos mais críticos.

e) Os procedimentos previstos no PCN deverão ser executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, incluindo as pessoas, processos, infraestrutura e recursos de tecnologia da informação e comunicações.

V - Tratamento de incidentes em redes computacionais:

a) As diretrizes específicas e procedimentos próprios relacionados ao tratamento de incidentes em redes computacionais deverão ser fixados em norma complementar, considerando:

a.1) Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas.

a.2) O tratamento do incidente deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

a.3) O Gestor de Segurança da Informação, ou os membros do Comitê de SIC, terá como dever durante o gerenciamento de incidentes de segurança em redes de computadores, acionar as autoridades policiais competentes para a adoção dos procedimentos legais que julgar necessários, observando os

procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizando a continuidade dos serviços da SUDAM, sem prejuízo de suas demais atribuições, quando houver ilícito(s) criminal(is).

Art. 7º Compete às unidades:

I - Diretoria Colegiada - DICOL

a) Prover apoio às unidades da SUDAM para o cumprimento da POSIC;

b) Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização; e

c) Assegurar os recursos necessários para a implementação e gestão da POSIC da SUDAM; e

d) Instituir o Comitê de Segurança da Informação e das Comunicações - CSIC.

II - Comitê de Segurança da Informação e das Comunicações - CSIC

a) Assessorar a SUDAM na implementação das ações de segurança da informação e das comunicações;

b) Elaborar e submeter à Diretoria Colegiada propostas de normas e políticas de uso dos recursos de informação, tais como:

b.1) gerenciamento de identidade e controle de acesso lógico;

b.2) controle de acesso físico;

b.3) controle de acesso à Internet;

b.4) utilização do correio eletrônico;

b.5) utilização de equipamentos de tecnologia da informação e das comunicações;

b.6) utilização de programas e aplicativos;

b.7) utilização de armazenamento lógico;

b.8) monitoração e auditoria de recursos tecnológicos; e

b.9) contingência e continuidade dos serviços de tecnologia da informação e das comunicações.

c) Garantir o acesso ao conjunto de documentos da POSIC e suas normas complementares no âmbito da SUDAM;

d) Rever periodicamente a POSIC e normas relacionadas;

e) Dirimir dúvidas e deliberar sobre questões não contempladas na POSIC e normas relacionadas;

f) Propor e acompanhar planos de ação para aplicação da POSIC, assim como campanhas de conscientização dos usuários;

g) Receber e analisar as comunicações de descumprimento das normas referentes à POSIC, apresentando parecer à Diretoria Colegiada para deliberação;

h) Propor a constituição de grupos de trabalho para tratar de temas específicos ao Superintendente;

i) Eleger o Gestor de Segurança da Informação, submetendo-o ao Superintendente para designação formal; e

j) Reunir-se periodicamente e quando for necessário.

Parágrafo único. O CSIC será presidido pelo titular da Diretoria de Administração - DIRAD e, em seus afastamentos ou impedimentos, pelo titular da Coordenação de Gestão de Tecnologia da Informação - CTI.

III - Gestor de Segurança da Informação e das Comunicações

a) Promover a cultura de segurança da informação e das comunicações no âmbito da SUDAM;

- b) Coordenar a Equipe de Tratamento e Resposta a Incidentes em redes computacionais;
- c) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;
- d) Identificar e encaminhar os incidentes de segurança classificados como críticos para o Comitê de SIC;
- e) Propor ao Comitê de SIC recursos necessários às ações de segurança da informação;
- f) Propor ao Comitê de SIC modificações à POSIC e normas relativas à segurança da informação e das comunicações;
- g) Acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;
- h) Manter contato permanente e estreito com o Departamento de Segurança da Informação e das Comunicações do Gabinete de Segurança Institucional - DSIC, para o trato de assuntos relativos à segurança da informação e das comunicações; e
- i) Garantir a guarda dos Termos de Responsabilidade e controle de assinatura de todos os usuários.

IV - Gestores das Unidades Administrativas

- a) Garantir aos colaboradores sob sua gestão, o acesso e cumprimento da POSIC e suas Normas Complementares;
- b) Garantir, caso se aplique, a assinatura do Termo de Responsabilidade (Anexo A) dos colaboradores que atuam no complexo predial da SUDAM em Projetos e/ou Termo de Cooperação externos a instituição, disponibilizando a autarquia quando solicitado; e
- c) Incorporar as diretrizes da POSIC nos processos de trabalho de suas unidades de gestão.

V - Coordenação de Gestão de Pessoas - CGP

- a) Garantir a todos os servidores e estagiários, o conhecimento da POSIC e suas Normas Complementares;
- b) Garantir a assinatura e a guarda do Termo de Responsabilidade (Anexo A) dos servidores e estagiários; e
- c) Comunicar à CTI, imediatamente, os ingressos, desligamentos, afastamentos e as movimentações de servidores e estagiários, com vistas a regularizar o acesso aos ativos da informação.

VI - Gestores de Contratos de Prestação de Serviços

- a) Garantir a assinatura do Termo de Compromisso (Anexo B) do representante legal da empresa;
- b) Garantir ao representante legal da empresa ou seu preposto, o acesso à POSIC e suas Normas Complementares;
- c) Garantir que o representante legal da empresa ou seu preposto dê ciência a todos os funcionários, sobre a POSIC e suas Normas Complementares, por ocasião de seu ingresso nas dependências da SUDAM;
- d) Garantir que o representante legal da empresa ou seu preposto encaminhe a cientificação disposta no subitem acima, para a devida guarda; e
- e) Comunicar à CTI, imediatamente, os ingressos, desligamentos, substituição de posto de serviço e as movimentações dos funcionários das empresas, com vistas a regularizar o acesso aos ativos da informação.

VII - Instituições que atuam no complexo predial da SUDAM e utilizam seus recursos de tecnologia da informação

- a) Garantir a todos os seus usuários, o conhecimento do conjunto de documentos atualizados que compõem a POSIC e suas Normas Complementares;

b) Garantir a assinatura do Termo de Responsabilidade (Anexo A) dos usuários, disponibilizando à SUDAM quando solicitado; e

c) Comunicar à CTI, imediatamente, os ingressos, desligamentos, afastamentos e as movimentações dos usuários, com vistas a regularizar o acesso aos ativos da informação.

VIII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)

a) Realizar ações reativas de tratamento dos incidentes após serem notificados;

b) Reduzir/eliminar os efeitos dos incidentes o mais rápido possível;

c) Buscar as causas, danos e responsáveis pelos incidentes ocorridos; e

d) Analisar e documentar as evidências do incidente e o tratamento adotado em resposta aos incidentes, enviando o Relatório de Tratamento de Incidentes ao Gestor de Segurança da Informação e Comunicações.

IX - Gestor da Informação

a) Manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação da SUDAM, tomando as ações necessárias para cumprir tal responsabilidade;

b) Garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo gestor da informação;

c) Tratar e atribuir nível de classificação das informações sob sua responsabilidade;

d) Comunicar tempestivamente ao Gestor de Segurança da Informação e das Comunicações sobre situações que comprometam a segurança das informações sob custódia;

e) Comunicar eventuais limitações para cumprimento dos critérios definidos para segurança da informação, ao Gestor de Segurança da Informação e das Comunicações, para que este decida quanto à cessão ou não da informação.

f) Solicitar à Coordenação de Gestão de Tecnologia da Informação que conceda ou revogue acessos aos usuários para as informações sob sua responsabilidade;

Art. 8º - As unidades apresentadas abaixo, de acordo com suas competências, deverão manter um processo permanente de divulgação das normas e procedimentos, bem como capacitar, conscientizar e sensibilizar os usuários à correta conduta da utilização desta POSIC:

a) ASCOM - Assessoria de Comunicação;

b) AGI - Assessoria de Gestão Institucional;

c) CGP - Coordenação de Gestão de Pessoas; e

d) CTI - Coordenação de Gestão de Tecnologia da Informação.

Art. 9º - O descumprimento das determinações da POSIC e suas Normas Complementares caracteriza infração funcional e sujeita o infrator às sanções administrativas, civis e penais, previstas na legislação pertinente e nos regulamentos internos da SUDAM, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 10 - Os casos omissos e as dúvidas com relação a essa POSIC e suas Normas Complementares serão submetidos ao Comitê de Segurança da Informação e das Comunicações da SUDAM.

Art. 11 - Esta Resolução entra em vigor na data de sua publicação.

PAULO ROBERTO CORREIA DA SILVA

Superintendente

KEILA ADRIANA RODRIGUES DE JESUS

Diretora de Planejamento e Articulação de Políticas

MARGARETH DOS SANTOS ABDON

Diretora de Administração

CARLOS EDILSON DE ALMEIDA MANESCHY

Diretor de Gestão de Fundos, de Incentivos e de Atração de Investimentos

Este conteúdo não substitui o publicado na versão certificada.

Número da Política	Versão	Versão	Folha
001/2017	12/09/2017	06	21 de 22



SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA

ANEXO A - TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____ e lotado no (a) _____ da SUDAM, DECLARO, sob pena das sanções cabíveis nos termos da legislação vigente, que assumo a responsabilidade por:

- I. Prestar total obediência à Política de Segurança da Informação e das Comunicações (POSIC) da SUDAM e suas Normas Complementares vigentes ou que venham a ser implantadas a qualquer tempo no âmbito desta Superintendência;
- II. Tratar o(s) ativo(s) de informação como patrimônio da SUDAM;
- III. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da SUDAM;
- IV. Contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;
- V. Utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da SUDAM;
- VI. Responder, perante a SUDAM, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Local, _____ de _____ de _____

Assinatura

Número da Política	Versão	Versão	Folha
001/2017	12/09/2017	06	22 de 22



SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA

ANEXO B - TERMO DE COMPROMISSO

Pelo presente instrumento, eu _____, CPF n° _____, RG n° _____, representante legal da empresa _____, CNPJ n° _____ que, em razão do CONTRATO N.º NNNN/AAAA, celebrado com esta autarquia, DECLARO, sob pena das sanções cabíveis nos termos da legislação vigente relacionadas à segurança da informação, que assumo a responsabilidade por:

- I. Dar ciência aos empregados, representantes, agentes e subcontratados, que estiverem sob a minha responsabilidade, independentemente do tipo e da duração de seus contratos de trabalho, os princípios e diretrizes estabelecidos na Política de Segurança da Informação e das Comunicações (POSIC) da SUDAM e suas Normas Complementares, por ocasião de seu ingresso nas dependências da SUDAM;
- II. Encaminhar ao Gestor do Contrato, para a devida guarda, cópia dos Termos de Responsabilidade assinados pelos colaboradores que prestam serviço na SUDAM; e
- III. Comunicar ao Gestor do Contrato, os ingressos, desligamentos, substituição de posto de serviço e as movimentações dos empregados, representantes, agentes e subcontratados, que estiverem sob a minha responsabilidade, com vistas a regularizar o acesso aos ativos da informação da SUDAM;

_____de _____de _____

Assinatura