MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL (MIDR)
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA (SUDAM)
DIRETORIA COLEGIADA (DICOL)

RESOLUÇÃO Nº 877, DE 18 DE DEZEMBRO DE 2023

A DIRETORIA COLEGIADA DA SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA (SUDAM), com base no disposto na Lei Complementar nº 124, de 3 de Janeiro de 2007 e, no uso das atribuições que lhe confere o Parágrafo Único do art. 10, do Anexo I, do Decreto nº 11.230, de 7 de outubro de 2022 e o art. 6º, II e III do Regimento Interno da Sudam;

Considerando o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, e diante dos fatos e fundamentos constantes no Processo nº CUP: 59004.000345/2014-80,

RESOLVE:

Art. 1º - Aprovar a Política de Segurança da Informação e das Comunicações (POSIC) da Superintendência do Desenvolvimento da Amazônia (SUDAM), na forma do Anexo I (SEI 0555880), desta Resolução.

Art. 2º - Aprovar o Termo de Responsabilidade e o Termo de Compromisso referentes à Política de Segurança da Informação e das Comunicações (POSIC) da Sudam, na forma dos anexos II e III (SEI 0555880), respectivamente.

Art. 3º - Revogar a Resolução nº 20/2018 (SEI 0049631).

Art. 4º - Esta Resolução entra em vigor na data de sua publicação.

Paulo Roberto Galvão da Rocha
Superintendente

Wilson Luiz Alves Ferreira
Diretor de Administração

Jorge Frota Pereira Junior
Diretor de Gestão de Fundos, Incentivos e de Atração de Investimentos

Aharon Alcolumbre
Diretor de Promoção do Desenvolvimento Sustentável

Documento assinado eletronicamente por **Paulo Roberto Galvão da Rocha**, **Superintendente**, em 18/12/2023, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jorge Frota Pereira Junior**, **Diretor**, em 18/12/2023, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Aharon Alcolumbre**, **Diretor**, em 18/12/2023, às 17:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Wilson Luiz Alves Ferreira**, **Diretor**, em 18/12/2023, às 17:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.sudam.gov.br /sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0560479** e o código CRC **99799D8B**.

Referência: Processo nº 59004.000345/2014-80 SEI nº 0560479

MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Segurança da Informação e Comunicações - POSIC tem por finalidade estabelecer as diretrizes para a segurança no uso, tratamento e controle, proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação da Superintendência do Desenvolvimento da Amazônia - Sudam.

Parágrafo único. A POSIC está alinhada ao planejamento estratégico da autarquia, de forma a garantir a autenticidade, confidencialidade, disponibilidade e integridade das informações eletrônicas institucionais.

Art. 2º Para a segurança da informação na Sudam serão rigorosamente observados os princípios constitucionais, legais e regimentais vigentes no âmbito da Administração Pública Federal.

CAPÍTULO II

DA ABRANGÊNCIA

Art. 3º O disposto nesta Política e nas suas Normas Complementares aplicar-se-á a todos os servidores, estagiários, prestadores de serviço e demais agentes públicos ou privados que, formalmente, executem atividades no âmbito da Sudam.

§ 1º Os contratos, convênios, termos de fomento, termos de colaboração e instrumentos congêneres, bem como os respectivos termos aditivos, conterão cláusulas específicas que imponham aos contratados/convenentes e assemelhados a obrigação de observarem o disposto nesta Política, para o exercício de suas atividades no âmbito da autarquia.

§ 2º Os estagiários serão orientados pelos seus respectivos supervisores quanto ao disposto nesta POSIC e suas normas complementares.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os fins desta POSIC, ficam estabelecidas as seguintes definições:

I - agente responsável pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR: servidor ocupante do cargo de titular da Divisão de Infraestrutura Tecnológica - DTEC, unidade pertencente à estrutura da Coordenação-Geral de Tecnologia da Informação e Comunicações – CGTIC, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

II - ativos de informação: meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e os recursos humanos que a eles têm acesso;

III - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

IV - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizado ou não credenciado;

V - criptografia: conjunto de princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra não inteligível, de forma que possa ser conhecida apenas pelo destinatário detentor da chave criptográfica;

VI - cópia de segurança: trata-se de cópia de dados em um meio separado do original, de forma a permitir a recuperação, dentro de período definido, em caso de pane na fonte original;

VII - credencial ou conta de acesso: permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso ao ambiente físico ou lógico. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha ou dispositivo digital (**token**);

VIII - disponibilidade: propriedade que garante que informações e serviços estejam acessíveis e utilizáveis sob demanda por pessoas, sistemas, órgãos ou entidades, devidamente autorizados;

IX - gestor da informação: servidor responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

X - gestor de segurança da informação: servidor responsável pelas ações de segurança da informação no âmbito da Sudam;

XI - gestão de riscos de segurança da informação: conjunto de processos que permitem identificar, analisar, avaliar e implementar medidas de proteção necessárias para o tratamento de riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

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

XIII - incidente em segurança da informação: qualquer evento indesejado ou inesperado, confirmado ou sob suspeita, que possa comprometer as operações do negócio ou ameaçar a segurança da informação em aspectos de confiabilidade, integridade, disponibilidade ou autenticidade;

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

XV - plano de continuidade de negócios: documentação dos procedimentos e das informações requeridas para que a Sudam mantenha disponíveis e operacionais seus ativos críticos de informação segundo abordagem e estratégia definidas em casos de incidentes;

XVI - segurança da informação: ações de proteção contra o acesso não autorizado, o uso indevido, a divulgação ilegal, a interrupção, a modificação ou a destruição não programada da informação e dos sistemas de informação, a fim de garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações;

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

XVII - termo de compromisso: termo assinado pelo representante legal de empresa prestadora de serviço, se responsabilizando em dar ciência aos empregados, representantes, agentes e subcontratados, dos princípios e diretrizes estabelecidos na Política de Segurança da Informação e

Comunicações da Sudam e suas normas complementares, por ocasião de seu ingresso nas dependências da autarquia.

CAPÍTULO IV

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 5º A POSIC da Sudam está fundamentada, sem prejuízo de outras legislações aplicáveis, nos seguintes normativos:

I - Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação;

II - Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

III - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme disposto na Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações;

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

V - Decreto nº 8.638, de 15 de janeiro de 2016, que institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, indireta, autárquica e fundacional;

VI - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

VII - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

VIII - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IX - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da Administração Pública Federal; e

X - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação.

CAPÍTULO V

DOS PRINCÍPIOS

Art. 6º Além dos princípios constitucionais que regem a Administração Pública Federal, as ações de Segurança da Informação e Comunicações, no âmbito da Sudam, são norteadas pelos seguintes princípios:

I - confidencialidade: propriedade de que a informação estará disponível e somente será revelada a pessoa física, sistema, órgão ou entidade que esteja autorizada e credenciada;

II - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

III - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

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

V - responsabilidade: preservação da integridade e tratamento de maneira adequada da informação, de acordo com sua classificação, bem como preservar e zelar pelos ativos de informação;

II - ética: as regras e os preceitos de ordem valorativa e moral de um indivíduo devem ser preservados sem o comprometimento da segurança da informação e comunicações;

III - celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;

IV - clareza: as regras que se fundamentam na POSIC devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão;

V - privacidade: o direito do cidadão de não ter registros pessoais e da vida privada divulgados sem sua prévia autorização devem ser assegurados; e

VI - publicidade: transparência às informações públicas, como preceito geral, respeitando a privacidade do titular, nos termos da Lei Geral de Proteção de Dados Pessoais - LGPD.

CAPÍTULO VI

DOS PRECEITOS

Art. 7º Constituem preceitos da POSIC da Sudam:

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

II - auditabilidade: eventos significantes de sistemas e processos deverão ser rastreáveis até o evento inicial;

III - controles automáticos: sempre que possível, controles de segurança automáticos deverão ser utilizados;

IV - resiliência: os sistemas e processos deverão ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

V - defesa em profundidade: controles deverão 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;

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

VII - exceção aprovada: exceções à POSIC deverão sempre ter aprovação superior; e

VIII - substituição da segurança em situações de emergência: deverão existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

CAPÍTULO VII

DAS DIRETRIZES GERAIS

Art. 8º De forma a promover a gestão e fomentar os aspectos de segurança da informação, a Sudam deverá instituir normativos operacionais que estabeleçam processos e procedimentos que garantam o controle de acesso às informações, instalações e sistemas de informação.

Art. 9º O gerenciamento dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

Art. 10. Os usuários deverão ser treinados e conscientizados nos procedimentos de segurança da informação.

Art. 11. É condição para acesso aos recursos de Tecnologia da Informação e Comunicação - TIC da Sudam a assinatura de Termo de Responsabilidade, contendo ciência aos termos desta Política, as responsabilidades e compromissos em decorrência deste acesso e penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da autarquia;

Art. 12. Quando do afastamento, da mudança de responsabilidade, de lotação ou de atribuições do usuário dentro da organização, far-se-á necessária a revisão imediata dos direitos de acesso e uso dos ativos de TIC.

§ 1º Os direitos de acesso e uso dos ativos atribuídos ao usuário deverão ser extintos quando da efetivação de seu desligamento.

§ 2º Todo ativo produzido pelo usuário desligado será de propriedade da Sudam, observadas as disposições da legislação aplicável.

Seção I

Do Tratamento da Informação

Art. 13. O processo de classificação da informação tem por objetivo assegurar que a informação receba o nível adequado de proteção de acordo com a sua importância para a Sudam.

Art. 14. As informações são classificadas em termo do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

Art. 15. Todo ativo de informação sob a responsabilidade da Sudam é considerado um bem e deve ser protegido pela instituição, de acordo com as diretrizes descritas nesta POSIC, na Lei Geral de Proteção de Dados Pessoais - LGPD e demais regulamentações em vigor, com o objetivo de minimizar os riscos aos serviços e atividades, bem como preservar a imagem institucional.

Art. 16. A classificação da informação será descrita em norma complementar e obedecerá às diretrizes estabelecidas pela Lei de Acesso à Informação - LAI, regulamentada pelo Decreto nº 7.724, de 16 de maio de 2012, do Governo Federal, ou documento correspondente que venha a substituí-lo.

Parágrafo único. O tratamento da informação em relação às questões decorrentes da Lei Geral de Proteção de Dados Pessoais deverá ser objeto de normativo próprio e segundo a legislação aplicável e competente para tal.

Seção II

Da Segurança Física e do Ambiente

Art. 17. As normas aplicáveis à segurança física e do ambiente de TIC da Sudam deverão contemplar procedimentos de acesso físico às áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.

§ 1º Os procedimentos de que trata o caput deverão constar em norma complementar específica.

§ 2º O planejamento da segurança de equipamentos e instalações de processamento de informações críticas ou sensíveis deverá prever a proteção contra ameaças físicas e ambientais.

Seção III

Da Gestão de Incidentes em Segurança da Informação

Art. 18. Deverão ser estabelecidos procedimentos formais para prevenção, auditoria, detecção, notificação e tratamento de incidentes de segurança.

§ 1º Os incidentes de segurança deverão ser registrados e analisados periodicamente, servindo de subsídio para o aperfeiçoamento dos procedimentos e controles de segurança vigentes.

§ 2º O Comitê de Segurança da Informação e Comunicações - CSIC e a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR da Sudam deverão, dentro de suas competências, adotar medidas de tratamento de incidentes de segurança ocorridos na autarquia.

Seção IV

Da Gestão de Ativos de Informação

Art. 19. Medidas de segurança deverão garantir a proteção lógica e física dos ativos de informação da Sudam em níveis compatíveis ao seu grau de relevância.

Art. 20. Os ativos de informação, de acordo com sua criticidade, devem ser identificados, inventariados e mantidos atualizados, possuir um responsável e ser protegidos contra acessos indevidos.

Parágrafo único. Ativos de informação não inventariados, não gerenciados ou de uso particular não poderão acessar a rede local da instituição, exceto em condições excepcionais, tratadas em norma complementar específica.

Art. 21. Apenas software homologado poderá ser instalado e utilizado nas estações de trabalho, em servidores de rede e demais dispositivos institucionais.

Art. 22. A informação armazenada em estações de trabalho, dispositivos móveis ou mídias externas é de responsabilidade do usuário, cabendo a este adotar as medidas necessárias para evitar a perda de dados.

Seção V

Dos Controles de Acesso e da Gestão do Uso dos Recursos Computacionais e de Comunicações

Art. 23. Os procedimentos e controles de acesso à rede deverão ser estabelecidos para proteger a troca de informações em todos os tipos de recursos de comunicação.

Art. 24. O acesso à Internet no ambiente de trabalho da Sudam está condicionado às necessidades dos agentes públicos no exercício de suas atribuições e será regido por norma específica, em conformidade com esta POSIC e demais orientações governamentais e legislação em vigor.

Art. 25. Os procedimentos para controles de acesso, como a criação de perfis com permissões de acesso às instalações e às informações, deverão ser formalizados e comunicados para que sistemas, informações e demais recursos de TIC tenham a sua confiabilidade, integridade e disponibilidade asseguradas.

Parágrafo único. O tratamento às concessões de perfis de acesso delegadas a empresas e profissionais contratados deverá ser objeto de supervisão e monitoramento continuado, de forma a garantir o propósito de sua utilização.

Art. 26. Os procedimentos para utilização do e-mail corporativo deverão ser estabelecidos de forma a assegurar o uso do correio eletrônico somente na execução do trabalho da Sudam ou em benefício desta, não sendo admitidas, sob condições normais, o emprego de e-mails pessoais para atividades do trabalho.

Art. 27. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito da Sudam deverá ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, observando o disposto nesta seção.

Art. 28. As ações de segurança da informação para a implementação ou contratação de tecnologias de computação em nuvem, no âmbito da Sudam, deverão estar em conformidade com as orientações definidas em normas regulatórias específicas em vigência.

Art. 29. A cifração e a decifração de informações classificadas em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado, conforme procedimentos definidos em normas e legislações específicas em vigor.

Art. 30. O uso institucional das redes sociais deverá ser norteado por diretrizes, critérios, limitações e responsabilidades estabelecidas, visando ao uso seguro das redes sociais, conforme procedimentos definidos em normas e legislações específicas em vigência.

Seção VI

Da Gestão de Risco

Art. 31. Os procedimentos de segurança da informação deverão ser planejados, documentados, testados, implementados e periodicamente avaliados segundo os objetivos institucionais e os riscos inerentes às atividades da Sudam.

Art. 32. Os riscos, ameaças, vulnerabilidades e controles deverão ser reavaliados periodicamente para garantir que a organização esteja efetivamente protegida.

Seção VII

Da Gestão de Continuidade

Art. 33. A gestão de continuidade é um processo abrangente que contempla normativos específicos que serão estabelecidos de modo a minimizar, em nível aceitável, os impactos sobre a Sudam em caso de ocorrência de falhas ou desastres significativos, por meio da combinação de ações de prevenção e recuperação.

§ 1º O processo de Gestão de Continuidade deve se basear em um Plano de Continuidade de Negócios, estruturado a partir da análise e avaliação dos riscos identificados e da prioridade de recuperação dos processos de negócio.

§ 2º O Gestor de Segurança da Informação coordenará o processo da Gestão de Continuidade.

Seção VIII

Da Auditoria e Conformidade

Art. 34. Os mecanismos de auditoria e conformidade deverão ser elaborados e implementados, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de segurança da informação em vigor.

Art. 35. Deverão ser adotadas medidas de proteção para que administradores de sistemas não tenham permissão de exclusão ou desativação de registros de log de suas próprias atividades.

Art. 36. Os recursos e informações de registro de log deverão ser protegidos contra falsificação e acesso não autorizado.

CAPÍTULO VIII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 37. Compete à Diretoria Colegiada da Sudam - DICOL, em seu âmbito de atuação, além das obrigações já dispostas na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

I - designar um Gestor de Segurança da Informação interno;

II - instituir o Comitê de Segurança da Informação - CSIC;

III - instituir e implementar Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR; e

IV - aplicar as ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

Art. 38. Compete ao Gestor de Segurança da Informação da Sudam:

I - coordenar o Comitê de Segurança da Informação e Comunicações – CSIC;

II - coordenar a elaboração da Política de Segurança da Informação e Comunicações e das normas complementares, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a alta administração na implementação da POSIC;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da POSIC e das normas complementares a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor os recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Parágrafo único. O Gestor de Segurança da Informação da Sudam será designado pela alta administração dentre os servidores ocupantes de cargo efetivo na autarquia, com capacitação técnica compatível às suas atribuições.

Art. 39. Compete ao Comitê de Segurança da Informação e Comunicações - CSIC:

I - assessorar a implementação das ações de segurança da informação no âmbito da autarquia;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV - propor alterações à POSIC e às normas complementares, em conformidade com a legislação vigente; e

V - deliberar sobre normas internas de segurança da informação.

Parágrafo único. O Comitê de Segurança da Informação e Comunicações terá a seguinte composição:

a) o Gestor de Segurança da Informação da Sudam, que o coordenará;

b) um representante do Gabinete;

c) um representante de cada diretoria finalística; e

d) o Coordenador-Geral de Tecnologia da Informação e Comunicações.

Art. 40. Compete à Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR da Sudam:

I - receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação e comunicações na rede e em sistemas computacionais da Sudam;

II - apurar tecnicamente os incidentes críticos de segurança da informação, originados pelo descumprimento desta política, consolidando informações e reportando ao Comitê de Segurança da Informação e Comunicações;

III - atuar de forma preventiva, sempre que possível, e reativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio da organização, implementando controles de segurança aplicáveis; e

IV - atuar conforme os padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede, orientados pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República - CTIR GOV.

Parágrafo único. A ETIR será composta, preferencialmente, por servidores ocupantes de cargo efetivo e lotados na Coordenação-Geral de Tecnologia da Informação e Comunicações da Sudam, com capacitação técnica compatível com as atividades dessa equipe, e será coordenada pelo Agente Responsável.

Art. 41. Compete ao Agente Responsável pela ETIR da Sudam:

I - propor a criação de procedimentos internos;

II - gerenciar as atividades e distribuir tarefas para os membros que compõem a Equipe; e

III - coordenar as atividades de tratamento e resposta a incidentes em redes computacionais.

Art. 42. Compete à Coordenação-Geral de Tecnologia da Informação e Comunicações - CGTIC, no que se refere à segurança da informação, sem prejuízo das competências regimentais:

I - conscientizar, sensibilizar e treinar os usuários dos sistemas de informação e comunicações em relação aos conceitos e às práticas de segurança da informação;

II - adotar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários dos sistemas de informação;

III - monitorar, analisar e implementar mecanismos que permitam identificar, avaliar e mitigar os danos ocasionados por incidentes de segurança;

IV - providenciar cópias de segurança e procedimentos de recuperação das informações, conforme prazos e padrões compatíveis com as normas públicas;

V - promover inspeções periódicas em sistemas de informação e recursos computacionais verificando a integridade do próprio ambiente informatizado, com vistas a garantir a integridade dos dados manipulados;

VI - propor, implantar e operacionalizar rotinas e procedimentos que visam garantir o cumprimento dos princípios e diretrizes estabelecidos na Política de Segurança da Informação e Comunicações da Sudam;

VII - estimular a adoção de práticas que promovam a segurança da informação de TIC na autarquia;

VIII - propor normativos operacionais aplicáveis à segurança da informação de TIC, em observância às normas exaradas pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR;

IX - supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas de informação e dispositivos de tecnologia da informação voltados para segurança da informação; e

X - elaborar os Planos de Gerenciamento de Incidentes, Continuidade de Negócios e Recuperação de Negócios, com vistas à garantia de continuidade na disponibilização de recursos e serviços afetos à Tecnologia da Informação.

Art. 43. Compete à Coordenação-Geral de Pessoal - CGPES, no que se refere à segurança da informação, sem prejuízo das competências regimentais:

I - garantir a assinatura e a guarda do Termo de Responsabilidade, de que trata o Anexo II desta Resolução, dos servidores e estagiários; e

II - comunicar à CGTIC os ingressos, desligamentos, afastamentos e as movimentações de servidores e estagiários, com vistas a regularizar o acesso aos ativos da informação.

Art. 44. Compete aos Gestores de Contratos de Prestação de Serviços, no que se refere à segurança da informação, sem prejuízo das suas atividades:

I - garantir a assinatura e a guarda do Termo de Compromisso, de que trata o Anexo III desta Resolução, do representante legal da empresa;

II - garantir ao representante legal da empresa ou seu preposto o acesso ao conjunto de documentos que compõem a POSIC e suas normas complementares;

III - garantir que o representante legal da empresa ou seu preposto dê ciência a todos os respectivos funcionários sobre a POSIC e suas normas complementares, por ocasião de seu ingresso nas dependências da Sudam;

IV - garantir que o representante legal da empresa ou seu preposto encaminhe a cientificação disposta no subitem acima para a devida guarda; e

V - comunicar à CGTIC os ingressos, desligamentos, substituições de postos de serviço e as movimentações dos funcionários das empresas, com vistas a regularizar o acesso aos ativos da informação.

Art. 45. Compete às Instituições que atuam no complexo predial da Sudam e utilizam seus recursos de tecnologia da informação, no que se refere à segurança da informação, sem prejuízo das suas atividades:

I - garantir a todos os seus usuários o conhecimento do conjunto de documentos atualizados que compõem a POSIC e suas normas complementares;

II - garantir a assinatura e a guarda do Termo de Responsabilidade, de que trata o Anexo II desta Resolução, dos usuários, disponibilizando à Sudam quando solicitado; e

III - comunicar à CGTIC, através do Gabinete da Sudam, sobre os ingressos, desligamentos, afastamentos e as movimentações dos usuários, com vistas a regularizar o acesso aos ativos da informação.

CAPÍTULO IX

DAS PENALIDADES

Art. 46. Todos os responsáveis descritos no artigo 3º desta Política estão sujeitos às penalidades previstas na legislação, em caso de descumprimento ao disposto nesse instrumento.

Parágrafo único. O descumprimento ao disposto nesta POSIC poderá ser apurado mediante processo administrativo interno pelas instâncias competentes.

CAPÍTULO X

DA ATUALIZAÇÃO

Art. 47. Esta Política poderá ter suas diretrizes revisadas sempre que se fizer necessário, não excedendo ao período máximo de 03 (três) anos, a contar da data de sua publicação.

CAPÍTULO XI

DAS DISPOSIÇÕES FINAIS

Art. 48. A Política de Segurança da Informação e Comunicações – POSIC e suas alterações serão aprovadas pela Diretoria Colegiada da Sudam – DICOL.

Art. 49. Esta Política, quando necessário, poderá ser complementada por instrumentos, além dos já citados, aprovados pela Diretoria Colegiada da Sudam – DICOL.

Art. 50. As dúvidas de interpretação desta POSIC serão dirimidas pelo Gestor de Segurança da Informação quanto ao mérito técnico e operacional.

Art. 51. Os casos omissos desta POSIC serão decididos pelo Comitê de Segurança da Informação e Comunicações - CSIC.

ANEXO II

TERMO DE RESPONSABILIDADE - POSIC

MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA

TERMO DE RESPONSABILIDADE - POSIC

Pelo presente instrumento, eu, _____, CPF nº _____, 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 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, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal; Instrução Normativa nº 02, de 24 de julho de 2020 que altera a Instrução Normativa nº 1, de 27 de maio de 2020; e na Instrução Normativa nº 03, de 28 de maio de 2021, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

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.

Belém, _____ de _____ _____.

_____

Assinatura

ANEXO III

TERMO DE COMPROMISSO

MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA

TERMO DE COMPROMISSO

Pelo presente instrumento, eu, _____, CPF n° _____, RG n° _____, representante legal da empresa _____, CNPJ n° _____, em razão do CONTRATO n° ____/_____, 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, dos princípios e diretrizes estabelecidos na Política de Segurança da Informação e Comunicações - POSIC da Sudam e suas normas complementares, por ocasião do ingresso destes colaboradores 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, substituições de postos 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;

Belém, _____ de _____ de _____.

_____
Assinatura