Publicação no D O E
n. 32677 p. 06
de: 08 / 11 / 13
7. DIVERSAS

GOVERNO DO ESTADO DO AMAZONAS

CONSELHO DIRETOR
RESOLUÇÃO 079/2013

INSTITUI a Política de Segurança da Informação e Comunicações – PSIC da FAPEAM e dá outras providências.

A **DIRETORA-PRESIDENTA** da **FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DO AMAZONAS** e **PRESIDENTA DO CONSELHO DIRETOR**, no uso de suas atribuições estatutárias, e tendo em vista a decisão deste Conselho, em reunião realizada nesta data,

CONSIDERANDO o que dispõe o Art. 17, inciso IV, alínea "*a*" do Decreto 23.420, de 21 de maio de 2003, que aprova o Estatuto da Fundação de Amparo à Pesquisa do Estado do Amazonas – FAPEAM e dá outras providências;

CONSIDERANDO a necessidade de instituir a Política de Segurança da Informação e Comunicações da FAPEAM, cujo objetivo é garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações geradas e/ou processadas na FAPEAM,

RESOLVE:

I INSTITUIR as "Políticas da Informação e Comunicações", de aplicações no âmbito da Fundação de Amparo à Pesquisa do Estado do Amazonas – FAPEAM, que estabelecem os princípios, diretrizes gerais e específicas, atribuições, competências, responsabilidades e penalidades que regulamentam um Sistema de Gestão de Segurança da Informação (SGSI) aos usuários desta Fundação.

II DETERMINAR que a norma em questão seja disponibilizada, para consulta e conhecimento, no sítio eletrônico interno: http://10.10.1.33/ifapeam/psic.

III DELEGAR à competência da Gerência de Informática – GEINF, por meio do Comitê de Segurança da Informação e Comunicações, a atualização das Normas referidas nesta Resolução, em caso de haver alguma modificação da legislação, dos critérios e procedimentos.

IV REVOGAR as disposições em contrário.

V VIGORAR os efeitos desta Resolução, a partir da data de sua publicação.

SALA DE REUNIÕES DO CONSELHO DIRETOR DA FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DO AMAZONAS, em Manaus, 31 de outubro de 2013.

Profa. Dra. **Maria Olívia de Albuquerque Ribeiro Simão**
Presidenta do Conselho Diretor

CONSELHO DIRETOR – RESOLUÇÃO 079/2013 – ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA FUNDAÇÃO DE AMPARO À PESQUISA – FAPEAM

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 1º Os conceitos e definições:

I. **Ameaça**: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

II. **Ativos**: Qualquer coisa que tenha valor para a organização;

a. **Ativos primários**: Processos e atividades do negócio e a informação;

b. **Ativos secundários**: Hardware, software, rede, recursos humanos, instalações físicas e a estrutura da organização;

III. **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;

IV. **Comitê de Segurança da Informação e Comunicações – CSIC**: colegiado de caráter deliberativo responsável pela normatização e supervisão da segurança da informação e comunicações no âmbito da FAPEAM;

V. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VI. **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

VII. **Correio Eletrônico**: É uma ferramenta de comunicação interna e externa, fornecida pela Organização aos usuários, como meio auxiliar para realização de suas atividades funcionais.

VIII. **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

IX. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;

X. **Download**: Entende-se por download a ação de baixar softwares disponíveis na rede mundial de computadores, a Internet.

XI. **Estação de trabalho**: Computador, seja desktop ou notebook, utilizado pelos usuários da FAPEAM.

XII. **GEINF**: Gerência de Informática da FAPEAM, setor responsável pelo gerenciamento, controle e monitoramento dos recursos tecnológicos disponíveis na FAPEAM.

XIII. **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XIV. **Gestão de continuidade dos negócios**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da Organização e suas atividades de valor agregado;

XV. **Gestão de riscos de segurança da informação e comunicações – GRSIC**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;

XVI. **Gestão de segurança da informação e comunicações – GSIC**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

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;

XVII. **Gestor de SIC**: servidor nomeado pela Presidência da FAPEAM para exercer a função de Presidente do CSIC;

XVIII. **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;

XIX. **Integridade**: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental;

XX. **Licença de software**: É a concessão de direito ao uso de software.

XXI. **Login/Logon**: Define o processo no qual o acesso a um sistema informático é controlado através da identificação e autenticação do usuário por meio de credenciais fornecidas por este mesmo usuário;

XXII. **Logout/ Logoff:** Ação de sair da sessão autenticada no Servidor de Arquivos e/ou Sistemas.

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

XXIV. **Segurança física e do ambiente**: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXV. **Sessão**: Tempo de utilização de um sistema iniciado a partir da efetivação do login e do encerramento através do logoff.

XXVI. **Segurança da Informação e Comunicações – SIC:** conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXVII. **Software**: Todo o programa executável em computadores (por ex., aplicativo de automação de escritório, de desenvolvimento, navegador, etc.);

XXVIII. **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos a FAPEAM;

XXIX. **Tecnologia da Informação e Comunicações – TIC**: todas as tecnologias que interferem e mediam os processos informacionais e comunicativos dos seres. Ainda, podem ser entendidas como um conjunto de recursos tecnológicos integrados entre si, que proporcionam por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica e de ensino e aprendizagem;

XXX. **Tratamento de incidentes**: é o processo 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;

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

XXXII. **Usuário**: Todo e qualquer funcionário, seja efetivo, comissionado, bolsista, estagiário ou prestador de serviços terceirizados, que utilize uma estação de trabalho, para o exercício de sua função ou para prestação de seus serviços, identificável através de nome único e palavra-chave.

XXXIII. **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO II
DOS PRINCÍPIOS E DIRETRIZES GERAIS

Art. 2º Esta PSIC deve obedecer aos princípios constitucionais, administrativos e do arcabouçou legislativo vigente que regem a Administração Pública.

Art. 3º O cumprimento desta PSIC deverá ser avaliado periodicamente por meio de verificações de conformidade,

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

realizadas pelo Comitê de Segurança da Informação e Comunicações - CSIC, buscando a certificação do cumprimento dos requisitos de segurança da informação e a garantia de cláusula de responsabilidade e sigilo.

Art. 4º Cabe ao CSIC instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em SIC, buscando parcerias com outros órgãos e entidades.

Art. 5º Fica instituído que o CSIC e a GEINF serão responsáveis pelas seguintes atividades:

I. Zelar pela execução dos processos de segurança da informação e comunicações;

II. Desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos e metas da FAPEAM.

III. Avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação e desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;

IV. Fornecer subsídios visando a verificação de conformidade de segurança da informação e comunicações;

V. Promover a melhoria contínua nos processos e controles de Gestão da Segurança da Informação e Comunicações.

Art. 6º Os membros do CSIC devem receber periodicamente capacitação especializada nas disciplinas relacionadas à SIC de acordo com suas funções.

CAPÍTULO III
DAS DIRETRIZES ESPECÍFICAS

SEÇÃO I
Da Gestão dos ativos

Art. 7º Os ativos secundários (Hardware, software, rede) devem:

I. Ser inventariados e protegidos;

II. Ter identificados seus proprietários e custodiantes;

III. Ter mapeado as suas ameaças, vulnerabilidades e interdependências;

IV. Ter sua entrada e saída nas dependências da FAPEAM autorizadas e registradas por autoridade competente;

V. Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI. Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminativos e afins.

Art. 8º O acesso dos usuários aos ativos e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

SEÇÃO II
Do Tratamento da Informação

Art. 9º A FAPEAM deve: criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 10 Deverão ser realizados procedimentos de tratamento, armazenamento, identificação e classificação das informações da FAPEAM de tal forma a garantir a integridade, facilidade de localização e evitar o uso dessas informações por pessoas não autorizadas.

Art. 11 O descarte de documentos físicos deverá ser realizado através de trituração, incineração ou remoção dos dados de forma segurança.

Art. 12 Deverão ser realizadas cópias de segurança das informações tomando como base as normas de gerenciamento de cópias de segurança/backup da informação da FAPEAM.

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

SEÇÃO III
Da Gestão de Riscos e Tratamentos de Incidentes

Art. 13 Entende-se como gerenciamento de riscos o processo que visa à proteção dos serviços, informações geradas e/ou processadas pela FAPEAM, por meio da redução, retenção, ação de evitar ou transferência dos riscos. Para gestão de riscos deve-se:

I. Definir o escopo da gestão de riscos;

II. Analisar e avaliar os riscos (contra quem ou contra o quê deve ser protegido);

III. Definir o plano de tratamento do risco;

IV. Aceitar os riscos;

V. Implementar um plano de tratamento do risco;

VI. Realizar monitoramento contínuo e análise crítica de riscos;

VII. Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação.

Art. 14 As normas e procedimentos para implantação e gestão de riscos de informação serão definidos em documento específico elaborado pelo CSIC.

Art. 15 A FAPEAM deve prover os recursos necessários para conscientizar e capacitar todos os servidores em noções de segurança da informação visando à continuidade dos serviços e atividades seguindo os princípios da Segurança da Informação e Comunicação buscando agilidade na notificação de qualquer evento relacionado à segurança da informação que venha a ocorrer.

SEÇÃO IV
Da Gestão da Continuidade

Art. 16 Deve ser estabelecido o Plano de Continuidade de Negócios – PCN, que terá como objetivo manter em funcionamento os serviços e processos críticos da FAPEAM na possibilidade da ocorrência de desastres naturais, falhas de equipamento, furto, roubo, falhas humanas e qualquer outro tipo de incidente que venha a ocorrer;

Art. 17 O PCN da FAPEAM deve ser definido pela CSIC com base no plano de tratamento de riscos e terá aprovação do Conselho Diretor.

SEÇÃO V
Da Auditoria e Conformidade

Art. 18 Todos os usuários estão sujeitos à auditoria em se tratando da utilização dos recursos de TIC.

Art. 19 Os procedimentos de auditoria e de monitoramento de uso dos recursos de TIC serão realizados periodicamente pela GEINF ou CSIC, com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança.

Art. 20 Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja esta PSIC e normas complementares, será permitido ao CSIC auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário e à Alta Direção dependendo da gravidade. Sendo considerada gravidade baixa a atividade que comprometa apenas a máquina do usuário, gravidade média a atividade que comprometa o desempenho da rede e gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços.

Art. 21 A verificação da conformidade poderá também ser realizada de forma planejada, mediante calendário de ações estabelecido pelo CSIC.

Art. 22 Os resultados das verificações deverão ser documentados e encaminhados ao CSIC, para ciência e providências cabíveis.

SEÇÃO VI
Do Controle de Acesso e Utilização de Recursos de TIC

Art. 23 Todos os usuários da FAPEAM tem acesso ao uso dos recursos de TIC de acordo com perfil

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

preestabelecido, definidos através de requisitos técnicos ou por determinação específica de sua chefia imediata.

Art. 24 Os acessos aos recursos de rede autenticáveis deverão ser realizados através do cadastro do usuário com a criação de login e senhas.

Art. 25 Os usuários da FAPEAM são responsáveis por todos os atos praticados com suas identificações, tais como: login/senha, crachá, carimbo, correio eletrônico e certificado digital.

Art. 26 A identificação do usuário, qualquer que seja a forma e meios, dever ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 27 Todos os usuários deverão por meio do termo de sigilo e responsabilidade específica assumir o compromisso de:

I. declarar o conhecimento e aceitação dos termos desta PSIC e de suas políticas e normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

II. declarar estar ciente que os acessos realizados à Internet, assim como conteúdo das mensagens de correio eletrônico institucional são passíveis de auditoria; e

III. manter a confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da GEINF.

Art. 28 Todos os usuários ou qualquer pessoa que entre na instituição deverão possuir algum tipo de identificação visível e ter seu acesso registrado, onde possa ser visualizada a data e a hora de sua entrada.

Art. 29 Sempre que houver mudanças nas atribuições de determinado usuário, a chefia imediata deve comunicar imediatamente à GEINF através do formulário de acesso de usuário, que deve ter os seus privilégios de acesso às informações e aos recursos computacionais readequados, podendo ser cancelados em caso de desligamento da FAPEAM ou bloqueados em caso de afastamento.

Art. 30 Qualquer tipo de informação referente a conteúdo que dize respeito à FAPEAM deverá ser guardado em lugar seguro como, por exemplo, cofres, armários e mobílias que possuam algum tipo de segurança (trava, fechadura, etc.) quando não estiverem em uso.

Art. 31 É de total responsabilidade do usuário a proteção das informações institucionais que estejam sob sua responsabilidade, utilizadas no âmbito da FAPEAM ou fora de suas dependências.

Art. 32 A utilização indevida de recursos como impressoras, telefonia, internet e rede wireless da FAPEAM para atividades não inerentes à instituição, acarreta em penalidades de acordo com a gravidade do caso, que deverá ser analisado pelo CSIC e encaminhado ao Conselho Diretor para providências cabíveis.

SEÇÃO VII
Do Correio Eletrônico

Art. 33 Os serviços de correio eletrônico disponibilizados pela Secretaria de Estado de Administração – SEAD são oferecidos como um recurso profissional para apoiar os usuários cadastrados da FAPEAM no cumprimento dos objetivos institucionais e são passíveis de auditoria;

Art. 34 Faz-se necessário que a liberação deste recurso seja autorizada pela chefia imediata através do Formulário de Acesso de Usuário enviando-o à GEINF para realizar o cadastramento de seu e-mail institucional.

Art. 35 A conta do usuário é excluída automaticamente pela SEAD, após 30 dias de inatividade.

Art. 36 Deverão ser excluídas periodicamente as mensagens que não são necessárias, evitando a superlotação (*over-cota*) e consequentemente o não recebimento de e-mails.

Art. 37 O usuário deverá exportar e armazenar com auxílio da GEINF, se necessário, periodicamente as mensagens com conteúdo importante, visando aumentar o espaço livre da conta de e-mail.

Art. 38 É proibida a transferência de *login* e senha do correio eletrônico individual a terceiros, considerando que toda mensagem enviada é de responsabilidade do usuário cadastrado, salvo e-mails setoriais, os quais deverão ter a informação de quem envia a mensagem eletrônica.

Art. 39 É proibido o envio de anúncios publicitários, partidários, conteúdos pornográficos ou mensagens contendo

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

entretenimentos e correntes.

Art. 40 O usuário deve utilizar linguagem formal em respostas aos e-mails institucionais, evitando o uso de abreviações de palavras ou gírias.

Art. 41 É proibido o envio de mensagens que contenham declarações difamatórias e linguagem ofensiva, assim como as que possam prejudicar a imagem da FAPEAM, de outras empresas ou de outras pessoas;

Art. 42 É obrigatória a utilização de assinatura nos e-mails com o seguinte formato:

Nome do Funcionário;
Função;
Telefone Comercial – Telefone Corporativo Móvel
Departamento/Gerência/Núcleo – SIGLA
Fundação de Amparo à Pesquisa do Estado do Amazonas – FAPEAM
http://www.fapeam.am.gov.br

SEÇÃO VIII
Da Publicação e Acesso à Internet

Art. 43 Todos os usuários tem direito ao acesso à internet, conforme perfil aprovado por sua chefia imediata e estipulado nas normas de SIC. Esse acesso deverá ser feito exclusivamente para fins diretos e complementares às atividades da FAPEAM, para enriquecimento intelectual ou como ferramenta de busca de informações para contribuição na execução de suas atividades.

Art. 44 Toda informação postada no portal da FAPEAM ou mídia social institucional é de responsabilidade do usuário que a publicou, estando sujeito às penalidades cabíveis, caso necessário.

SEÇÃO IX
Da Segurança Física e do Ambiente

Art. 45 Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 46 O CSIC deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos ou interferências.

Art. 47 As proteções devem estar alinhadas aos riscos identificados.

SEÇÃO X
Da Segurança em Recursos Humanos

Art. 48 Os usuários devem ter ciência:

I. Das ameaças e preocupações relativas à SIC;

II. De suas responsabilidades e obrigações no âmbito desta PSIC.

III. Da colaboração para difundir o cumprimento desta PSIC e das normas de segurança e da legislação vigente a cerca do tema.

Art. 49 Devem ser estabelecidos processos permanentes de conscientização, capacitação em SIC, que alcancem todos os usuários da FAPEAM, de acordo com suas competências funcionais.

CAPÍTULO IV
ATRIBUIÇÕES, COMPETÊNCIAS E RESPONSABILIDADES

SEÇÃO I
Dos Funcionários

Art. 50 São atribuições dos funcionários:

I. Conhecer e cumprir esta PSIC;

II. Assinar o Termo de Responsabilidade, formalizando ciência, aceite e assumindo o compromisso de se enquadrar

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

às normas e regras desta PSIC.

III. Buscar sanar as dúvidas desta PSIC, diretamente com seu superior imediato ou com a CSIC, evitando penalidades posteriores.

IV. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela FAPEAM.

V. Assegurar que os recursos e serviços tecnológicos sob sua responsabilidade direta serão utilizados apenas para os fins cabíveis, aprovados e de interesse da FAPEAM.

VI. Comunicar os incidentes que afetem a SIC à GEINF.

SEÇÃO II
Do Gestor de SIC

Art. 51 São atribuições do Gestor de SIC:

I. Promover cultura de segurança da informação e comunicações;

II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Propor recursos necessários às ações de SIC;

IV. Coordenar o CSIC;

V. Comunicar ao CSIC os resultados e outras informações pertinentes;

VI. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC; e

VII. Propor normas relativas à SIC.

SEÇÃO III
Do Comitê de Segurança da Informação e Comunicações – CSIC

Art. 52 Compete ao Comitê de Segurança da Informação e Comunicações:

I. Normatizar e supervisionar a SIC no âmbito da FAPEAM.

II. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

III. Propor alterações na PSIC;

IV. Solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

V. Avaliar, revisar e analisar criticamente a PSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais da FAPEAM e às legislações vigentes;

VI. Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PSIC da FAPEAM;

VII. Constituir grupo de trabalho para realizar verificações de conformidade;

VIII. Aprovar o plano de investimentos em SIC da FAPEAM;

IX. Monitorar e avaliar periodicamente o plano de SIC, assim como determinar os ajustes cabíveis;

X. Propor projetos relacionados à melhoria da Segurança da Informação e Comunicações na FAPEAM;

XI. Promover campanhas de conscientização, palestras, treinamentos e outros meios de endomarketing sobre segurança, reciclagem, economia, uso consciente de recursos tecnológicos e outros assuntos relacionados a TIC;

XII. Definir e atualizar seu Regimento Interno; e

XIII. Baixar normas e procedimentos complementares a esta PSIC.

SEÇÃO IV
Da Gerência de Informática – GEINF

Art. 53 Compete a Gerência de Informática:

I. Facilitar e coordenar as atividades de tratamento e respostas a incidentes de segurança;

II. Promover a recuperação de sistemas;

III. Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

IV. Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V. Analisar ataques e intrusões na rede de computadores da FAPEAM;

VI. Executar as ações necessárias para tratar quebras de segurança;

VII. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

VIII. Executar o Plano de Continuidade de Negócios para o tratamento e resposta a incidentes;

IX. Participar em fóruns, redes nacionais e internacionais relativos à SIC.

X. Realizar a configuração dos equipamentos, ferramentas e sistemas concedidos para uso de seus custodiantes com todos os controles necessários para cumprir os requisitos de SIC propostos nesta PSIC;

XI. Garantir de forma ágil, através de solicitação formal, bloqueio de acesso de usuários à rede e seus serviços, quando por motivos de desligamento, férias, ou qualquer tipo de licença, incidente ou investigação com fins de salvaguarda de ativos da FAPEAM;

XII. Monitorar o ambiente de TIC, gerando indicadores, relatórios e históricos de:

a. uso de capacidade instalada de rede e dos recursos disponíveis;

b. tempo de resposta no acesso à internet e aos sistemas oferecidos pela FAPEAM ao público interno e externo;

c. períodos de indisponibilidade no acesso à internet e aos sistemas oferecidos pela FAPEAM ao público interno e externo;

d. incidentes de segurança (ataque de hackers, vírus, trojans, acessos indevidos, furtos e afins);

e. registro de atividades dos usuários ao navegar na rede interna e externa, sendo internet (sites, e-mails, upload/download de arquivos, e afins);

XIII. Prover a ampla divulgação desta PSIC para todos os usuários da FAPEAM.

XIV. Analisar riscos relacionados à SIC da FAPEAM e apresentar relatórios periódicos ao CSIC, acompanhados de propostas de aperfeiçoamento e melhorias para avaliação.

XV. Os funcionários da GEINF que possuírem perfil de administradores da rede poderão pela característica de seus privilégios, acessar os arquivos e dados de outros usuários. No entanto, somente quando necessário para que seja executada uma atividade operacional sob sua responsabilidade, como por exemplo, manutenção de computador, realizar cópias de segurança, auditoria ou testes.

SEÇÃO V
Do Gestor Setorial

Art. 54 São atribuições do Gestor Setorial:

I. Garantir a segurança dos ativos de informação sob sua responsabilidade;

II. Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PSIC;

III. Conceder e revogar acessos aos ativos de informação;

IV. Comunicar à GEINF a ocorrência de incidentes de SIC;

V. Designar custodiante dos ativos de informação, quando aplicável.

VI. Corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;

VII. Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

VIII. Incorporar aos processos de trabalho de seu setor, ou de sua área, práticas inerentes à SIC;

IX. Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793

X. Informar à Gerência de Pessoal (GEPE) a movimentação de pessoal de seu setor;

XI. Realizar o tratamento e a classificação da informação;

XII. Autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas no seu setor;

XIII. Comunicar à GEINF os casos de quebra de segurança;

XIV. Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos colaboradores.

XV. Ser exemplo na utilização dos recursos e serviços de TIC disponível na FAPEAM.

SEÇÃO VI
Da Diretoria Administrativa Financeira – DAF

Art. 55 São competências DAF:

I. Apoiar e determinar a utilização desta PSIC, como norma auxiliar na execução das atividades dos usuários.

II. Ter conhecimento e estabelecer as devidas punições aos usuários que burlarem ou se demonstrarem opostos ao seguimento das normas aqui estabelecidas.

III. Cobrar / Exigir da GEINF relatórios gerenciais periódicos a respeito da utilização dos recursos tecnológicos disponíveis aos funcionários.

SEÇÃO VII
Da Assessoria Jurídica

Art. 56 Compete à Assessoria Jurídica:

I. Apoiar juridicamente esta PSIC no que diz respeito a sua legalidade e como instrumento de embasamento para diversas situações de descumprimento desta.

II. Manter as áreas da FAPEAM informadas sobre alterações legais e/ou regulatórias que impliquem responsabilidades e/ou ações envolvendo a SIC.

III. Incluir, na análise e na elaboração de contratos, caso necessário, cláusulas específicas de SIC, com o objetivo de preservar informações referentes à FAPEAM.

CAPÍTULO VIII
Das Penalidades

Art. 57 Ações que violem esta PSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apurados e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

Art. 58 Esta Resolução ficará publicada no Portal Eletrônico Interno da FAPEAM, em caráter permanente, e entrará em vigor na data de sua publicação no Diário Oficial do Estado.

FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DO AMAZONAS, em Manaus, 31 de outubro de 2013.

Profa. Dra. **Maria Olívia de Albuquerque Ribeiro Simão**
DIretora-Presidenta da FAPEAM

Travessa do Dera, s/n - Flores
Tel.: (92) 3878-4000
gabinete@fapeam.am.gov.br
www.fapeam.am.gov.br
Manaus/Am - CEP.: 69058-793