SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DO AMAZONAS – CREA-AM

CREA-AM
Conselho Regional de Engenharia
e Agronomia do Amazonas

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PSI

CONTROLE DE REVISÕES:

REVISÃO		NATUREZA DA ALTERAÇÃO	FOLHA ALTERADA (s)
Nº	DATA		
00	26/05/2021	Elaboração	Todas
01	16/01/2024	Controle de Acesso via VPN (Virtual Private Network)	15 e 16

Revisado: Assessor Sênior de Desenvolvimento de Tecnologia da Informação 16/01/2024 Eduardo Frota	**Aprovado:**

1- DOCUMENTO DE DIRETRIZES E NORMAS ADMINISTRATIVAS

1.1 - INTRODUÇÃO/NORMATIVO

Todos os Empregados (Gestores, Colaboradores, Conselheiros, Estagiários, Menores Aprendizes, fornecedores ou prestadores de serviço) devem conhecer e cumprir as diretrizes de segurança da informação do Conselho Regional de engenharia e Agronomia do Amazonas – CREA-AM.

A Presidência e as Gerências devem cumprir e fazer cumprir a Política de Segurança da Informação.

Violações aos controles e regras da Política apresentadas neste mesmo, estarão sujeitas a punições ou penalidades, e deverão ser reportadas imediatamente a ADTI.

O acesso à internet, correio eletrônico (E-mail) de domínio @crea-am.org.br, e comunicador de mensagem instantânea (ex: Spark, Skype etc.) são utilizados somente para o cumprimento de atividades profissionais em cumprimento das atribuições de cada cargo no Crea-AM.

O acesso WI-FI (rede sem fio) é de uso exclusivo dos colaboradores ativos do Conselho e visitantes autorizados pela ADTI do Crea-AM.

Os usuários com problemas técnicos sejam no S.O (sistema operacional), hardware, software, rede ou outros devem solicitar o devido suporte técnico e especializado dos colaboradores da ADTI no ramal 7110, assim como solicitações/inclusões/permissões entre outros devem usar o sistema SITAC. Caso não seja possível a abertura do chamado o usuário deve telefonar para o ramal da ADTI para que a equipe técnica abra o chamado interno e possa atender sem prejuízo de continuidade dos serviços**.**

Todo usuário no âmbito corporativo terá em posse autorização de acesso a dados (Login e Senha) de acordo com suas atribuições, que deverão ser mantidas em sigilo.

Os acessos através dos sistemas corporativos serão efetuados com permissões de acesso especifica de acordo com níveis de permissão, designados a cada usuário conforme os níveis de acesso propostos nessa política de segurança da informação.

É expressamente proibido o desenvolvimento de atividades particulares, bem como a utilização indevida das estações de trabalho corporativa, como aplicações pessoais ou contraditórias aos serviços corporativos. - Ex: Efetuar ações caracterizadas como violação da segurança computacional, desenvolver vírus ou outros códigos maliciosos, manipular, sabotar, usar sniffers, permitir, motivar, efetuar ou fazer varreduras na rede, quebrar a senha de outras contas, ataques, fraudar, burlar os recursos disponíveis.

Telefones fixos, celulares, comunicadores de mensagens instantâneas fornecidas pelo CREA-AM assim como comunicadores instantâneos, devem ser usados apenas para o cumprimento de atividades profissionais.

Usuários de ativos tecnológicos como Notebooks, Netbooks, Caneta Digital, Modem 4G, Smartphones, Tablets, Celulares, Pen drive, Modem Móvel, DVD, ou qualquer outra forma eletrônica, magnética ou óptica de propriedade do CREA-AM, devem utilizar travas de segurança e autorização de acesso (Login e Senha) ou criptografia para vedar a utilização por parte de terceiros em caso de perda, furto ou roubo.

Somente será permitida a utilização de notebooks, netbooks, tablets, smartphones (ou outro tipo de ativo tecnológico) “Pessoais” mediante a emissão de documento comprobatório das referidas necessidades de utilização, além

de assumir a responsabilidade pelo objeto, e eventuais danos causados à rede corporativa ou segurança da informação do Conselho.

A informação é um ativo importante do CREA-AM e nunca deverá ser divulgada a pessoas não autorizadas.

Os documentos confidenciais não devem permanecer esquecidos em impressoras, sobre as mesas ou quaisquer locais acessíveis a pessoas não autorizadas. Os impressos não utilizados devem ser descartados nos locais de coleta seletiva. O Conselho poderá também implementar os serviços de cota de impressão destinada a cada usuário.

O uso do crachá de identificação é obrigatório. É pessoal e intransferível e deve ser usado por todos em local visível.

Propriedade Intelectual: É de propriedade do CREA-AM, todos os "designs", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício.

Para ter maior segurança na internet, recomendamos o acesso a cartilha de segurança para Internet desenvolvida pela CERT.br (*Centro de Estudos, Repostas e Tratamento de Incidentes de Segurança no Brasil*) que contém recomendações sobre como o usuário pode aumentar a sua segurança na internet. Acesso à cartilha: http://cartilha.cert.br.

Todos devem conhecer e cumprir a Política de Segurança da Informação, ao firmar seu compromisso através da assinatura do Termo de Responsabilidade, Confidencialidade e Sigilo de Informações em anexo a esse documento.

2- SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 – MISSÃO

Garantir a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização das atividades deste Conselho.

2.2 – OBJETIVO

A Política de Segurança da Informação é uma declaração formal do Crea-Amazonas acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários. Este documento estabelece regras de Segurança da Informação para prevenir o uso incorreto, indevido ou irregular de informações e recursos corporativos do CREA-AM, e estabelece as punições e penalidades aplicáveis.

2.3 – ABRANGÊNCIA

Presidente, Conselheiros, Diretores, Executivos, Gerentes, Prestadores de Serviços, Consultores, Auditores todos os demais empregados, Assessores do CREA-AM, temporários ou não, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam ativos corporativos do Crea-AM, e suas Inspetorias.

2.4 – BOAS PRÁTICAS

Cuidado ao tratar de assuntos do Conselho dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor. Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora do Conselho ou próximos a pessoas desconhecidas. Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento às pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem do CREA AMAZONAS.

2.5 – TERMOS E DEFINIÇÕES

Política de Segurança é a implementação de regras e normas fundamentadas diretamente às regras do negócio do Conselho através de análise de risco, ameaças e vulnerabilidades, para a continuidade corporativa.

2.6 – NOMENCLATURAS UTILIZADAS

TI: Tecnologia da Informação.

Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de *softwares*.

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Mídias Removíveis*:* Dispositivos que permitem a leitura e gravação de dados tais como: DVD, *Pen Drive*, cartão de memória entre outros.

USB*:* É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

VPN *(Virtual Private Network):* Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

Softwares de Mensagens: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Firewall*:* É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma serie de políticas de segurança a determinados pontos da rede.

Modem **4G**: É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como *Tablets* (com suporte 4G), *notebooks*, *netbooks*, *desktops*, etc. objetivando conexão com a internet. O modem 4G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, *smartphones* e *notebooks*) compatíveis com a tecnologia 4G.

Segurança da Informação*:* É o conjunto de rotinas e procedimentos que tem como principal foco a proteção de dados, ativos, e infraestrutura, reduz consideravelmente a probabilidade da presença de riscos e ameaças à imagem do Conselho.

***Diretrizes**:* São documentos relacionados à segurança da informação que apresentam o correto comportamento funcional, e que deve ser adotado por todos os profissionais da organização, de maneira que os objetivos estabelecidos sejam alcançados.

***Termo de Responsabilidade, Confidencialidade e Sigilo de Informações**:* É um documento integrante da Política de Segurança da Informação que estabelece as responsabilidades do efetivado, comissionado, conselheiros, estagiários e menores aprendizes ou empresas subcontratadas, sobre o uso de recursos e informações disponibilizadas pelo CREA-AM para a execução de suas funções.

***Confidencialidade**:* Significa assegurar que a informação esteja acessível apenas para quem tenha permissão de acesso.

***Integridade**:* Significa garantir a exatidão da informação em suas possíveis formas de processamento.

***Disponibilidade**:* É assegurar que a informação esteja disponível, sempre que necessário, aos usuários autorizados que tenham acesso a mesma e aos seus ativos.

***Ativos de informação ou ativos tecnológicos**:* São ativos considerados importantes para a organização e, se não protegidos adequadamente, podem causar impacto ao Conselho e respectiva infraestrutura. São considerados ativos de informação: documentos, informações sobre pessoal, ações internas, imagem do CREA-AM, informações sobre cadastramento de empresas e profissionais, parceiros, pesquisas competitivas, pessoas, licenciamento de software ou outros, documentação de sistemas, programas e códigos fontes, sistemas, aplicativos, computadores, servidores de rede, DVD, pen drive, access point, notebooks, netbooks, caneta digital, smartphones, tablets, celulares, modem móvel ou qualquer outra forma eletrônica, magnética ou óptica.

***Plano de Continuidade de Negócio**:* São atividades que têm por finalidade evitar a interrupção do "negócio" do CREA-AM, proteger seus processos críticos contra falhas e desastres e garantir que a retomada do "negócio", em caso de falha ou desastre, seja executada no menor tempo possível.

3 - O CONSELHO

O Conselho Regional de Engenharia e Agronomia do Estado do Amazonas (CREA-AM) é entidade autárquica de fiscalização do exercício e das atividades profissionais, da Engenharia, Agronomia, Geologia, Geografia e Meteorologia e seus cursos Técnicos e Tecnológicos, dotada de personalidade jurídica de direito público, instituída pela Resolução nº 223, de 30 de agosto de 1974 , na forma estabelecida pelo Decreto Federal nº 23.569, de 11 de dezembro de 1933, e mantida pela Lei nº 5.194, de 24 de dezembro de 1966, com sede e foro na cidade de Manaus e jurisdição no Estado do Amazonas, constituindo serviço público federal do Conselho Federal de Engenharia e Agronomia (Confea), para exercer papel institucional de primeira e segunda instâncias no âmbito de sua jurisdição.

Presidente é a autoridade de poder executivo, cabendo a ele as tarefas organizacional e institucional por finalidade de cumprir e fazer cumprir a legislação federal, as resoluções, as decisões normativas, as decisões plenárias baixadas pelo Confea, os atos normativos, os atos administrativos de acordo com a Lei n.º 5.194, de 1996 e do regimento interno do Conselho.

Conselheiro regional é o profissional habilitado de acordo com a Legislação em vigor, registrado no Crea, representante de entidades de classe ou de instituições de ensino superior dos grupos profissionais da Engenharia, da Arquitetura e da Agronomia de acordo com o Art. 34 Seção V.

Gestor é a pessoa a quem compete à interpretação dos objetivos propostos pela organização e atua, através do planejamento, da organização, da liderança, da direção de controle, a fim de atingir os referidos objetivos para organização. Conforme o Art. 189 do regimento interno do CREA-AM, A Superintendência é dirigida por um superintendente para exercer a função de gestor da estrutura auxiliar do CREA-AM.

Usuário Corporativo é todo aquele que tem acesso aos ativos tecnológicos.

Estagiário é todo estudante que frequenta o ensino regular em instituições de educação superior, de educação profissional, de ensino médio, da educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, vinculado junto ao Conselho nos termos da Lei N° 11.788, de setembro de 2008.

Menor Aprendiz é o contratado de trabalho especial, ajustado por escrito e por prazo determinado, em que o empregador se compromete a assegurar os jovens maiores de quatorze e menor de vinte e quatro anos, inscrito em programa de aprendizagem, formação técnico-profissional metódica, compatível com o seu desenvolvimento físico, moral e psicológico, e o aprendiz, a executar com zelo e diligência, as tarefas necessárias a essa formação, nos termos da Lei n° 10.097, de 19 de dezembro 2000.

Fornecedores são pessoas físicas ou jurídicas contratadas pela organização para fornecerem bens, produtos e serviços, nos termos dos pedidos de compras ou contratos pactuados consensualmente entre as partes.

Consultores e Prestadores de Serviços são pessoas físicas ou jurídicas que possuem conhecimentos específicos necessários para assessorar o Conselho na criação ou desenvolvimento de determinados projetos, análise de assuntos estratégicos e na elaboração de pareceres e opiniões que nortearão as decisões a serem tomadas pela Presidência ou Gestores (gerente de departamentos).

4 - POLÍTICAS

Esta Política contém as Diretrizes de Segurança da Informação necessárias para a proteção das informações e recursos corporativos, visando evitar ou minimizar os riscos de fraudes, vazamento e manipulação de informações e riscos de comprometimento dos dados corporativos por agentes internos ou externos. As informações e recursos corporativos do Conselho devem estar protegidos corretamente, e todos devem zelar pela proteção destas informações, e cumprir as diretrizes da política.

5 - RESPONSABILIDADES

5.1 – Comitê Gestor da Tecnologia da Informação – CGTI tem como missão:

- Colaborar com a elaboração da Política de Segurança da Informação junto a ADTI;
- Aprovar a Política de Segurança da Informação juntamente com a ADTI;
- Definir o Plano Estratégico para implantação da Política de Segurança da Informação;
- Definir e aprovar junto a ADTI e GESTOR os procedimentos e penalidades para se fazer cumprir a Política de Segurança;
- Aprovar e propor medidas e contramedidas para correção de problemas causados por quebra ou fragilidade da Política de Segurança;

- Alterações, revisões e ajustes da política de segurança de informação, serão previamente discutidos e informados aos interessados;

5.2 – Gestão de Tecnologia da Informação – GTI tem como missão:

- Coordenar todos os aspectos e atividades relacionadas à implementação da Política de Segurança da Informação e demais soluções;
- Monitorar o cumprimento das Diretrizes e Normas;
- Planejar e divulgar campanhas de conscientização da segurança da informação;
- Identificar vulnerabilidades e ameaças;
- Gerir incidentes de segurança da informação ou violações da política de segurança da informação;
- Aprovar e solicitar um planejamento anual de segurança da informação;
- Analisar e obter as aprovações necessárias para adotar quaisquer procedimentos divergentes aos estabelecidos na política de segurança da informação;
- Relatar as infrações e repassar a superintendência e a gerência competente sobre a adoção de punições ou penalidades aplicáveis na hipótese de descumprimento da política de segurança da informação;
- Acompanhar os indicadores internos e externos de segurança da informação;
- Alterações, revisões e ajustes da política de segurança de informação, serão previamente discutidos e informados aos interessados;
- Prover fundamentos para aprovação de procedimentos e regras estabelecidas;
- Monitorar a utilização das políticas implementadas;
- Elaborar e emitir parecer técnico acerca de assuntos relacionados à segurança da informação ou algum tema no âmbito do Conselho que seja competência da Gestão da ADTI;
- Propor novos procedimentos a ser seguido pelos departamentos para melhor adequação das regras do CREA-AM;
- Planejar e dimensionar junto aos departamentos ativos de informações e tecnológicos que melhor se adequam a estrutura do Conselho;

Atenção: A Gestão da ADTI terá autonomia, quando autorizada pelo superior imediato, para atuar sobre os equipamentos e ativos tecnológicos desta Autarquia, o que concerne aos seguintes tópicos: Realização de auditoria (*local ou remota*), definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como nocivas aos sistemas, ou à rede corporativa, acessos internos e externos, instalação/desinstalação de softwares, instalação de softwares de monitoramento, desinstalação de quaisquer softwares considerados nocivos à integridade dos ativos, credenciamento/descredenciamento de usuários, analisar e emitir parecer referente a solicitações ADTI, remover arquivos que não são pertinentes às regras de negócio do CREA-AM, remover arquivos temporários tanto de sistemas quanto de pastas compartilhadas nos servidores, remover arquivos que comprometam à segurança da informação do Crea-AM.

6 - MISSÃO DA GESTÃO

6.1 - Conselheiros, Presidência, Diretores e Gestores tem como missão:

- Assegurar e cobrar de seus subordinados o cumprimento da política de segurança da informação;
- Exigir da ADTI os relatórios gerenciais de acordo com suas atribuições;
- Coordenar todos os aspectos e atividades relacionadas à implementação e demais soluções de Segurança da Informação;
- Monitorar o cumprimento das Diretrizes;
- Planejar e divulgar campanhas de conscientização da Segurança da Informação;
- Identificar vulnerabilidades e ameaças internas e externas relacionadas ao seu setor e reportar a ADTI, mesmo que seja apenas uma simples desconfiança;
- Gerir incidentes de Segurança da Informação;
- Cuidar do credenciamento/descredenciamento de usuários lotados no departamento;
- Detectar problemas relativos à política de segurança da informação e comunicar imediatamente à Gestão de TI para providências;

6.2 - Empregados:

Todos os Empregados (gestores, estagiários e menores aprendizes ou fornecedores e prestadores de serviço do CREA-AM) devem conhecer e cumprir a política de segurança da informação, e formalizar ato através da assinatura do "Termo de Responsabilidades, Confiabilidade e Sigilo de Informações". Estão obrigados a zelar e cumprir as diretrizes da política de segurança da informação no exercício de suas atribuições em nível operacional ou gerencial. Devem, ainda, comunicar imediatamente ao comitê gestor de tecnologia da segurança da informação a existência de qualquer descumprimento, incidente ou violação da política de segurança da informação, bem como qualquer atividade suspeita.

6.3 - Área de Governança de TI e Superintendência geral do Crea-AM:

Cabe a estas duas áreas propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas pelos Gestores.

7 - PUNIÇÕES

O não cumprimento e/ou violação das diretrizes apresentadas nesta política de segurança da informação estão sujeitas as possíveis aplicações de advertências e/ou penalidades conforme grau de gravidade (leve, media e grave) definido no anexo "A" que terão punições na ordem descritas a seguir: Para Empregados (Colaboradores - Efetivo) / Menor Aprendiz e Estagiários / Terceiros (Terceirização de Serviços) / Conselheiros / Diretores do Conselho

a) Leve:

Perda de acesso privilegiado a determinados recursos;

Advertência formal e comunicação do ocorrido ao superior imediato.

b) Média:

Suspensão até 30 dias com supressão da remuneração mensal.

c) Grave

Processo administrativo disciplinar;

Aplicação de punições trabalhistas previstas no artigo 482 da CLT;

Ressarcimento dos prejuízos causados, conforme previsto em contrato ou Lei;

Processo civil ou criminal de acordo com a gravidade dos atos;

Rescisão imediata da relação contratual, acarretando o ressarcimento das perdas e danos causados ao CREA-AM e terceiros, conforme previsto em contrato ou Lei;

Rescisão do contrato de estágio;

7.1 - Conformidade

Demais esclarecimentos referentes às diretrizes implementadas nesta política de segurança da informação poderão ser fundamentados em normas específicas de autoria da presidência do CREA-AM;

Fica estabelecido que todo colaborador da organização, independentemente do grau de hierarquia, deve se submeter à implementação e utilização das políticas de segurança da informação implementadas nesse Conselho.

O principal foco da implementação da política de segurança da informação é impedir a violação de qualquer lei criminal, civil, estatutos ou regulamentações que podem comprometer diretamente ou indiretamente os ativos da informação.

8 - INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todo efetivo deve reportar imediatamente à gerência de tecnologia da informação os incidentes de segurança ou violações da política de segurança da informação de que tenham conhecimento. São exemplos de incidentes de segurança da informação: falhas de segurança em aplicativos (web ou desktops), divulgação não autorizada de informações, existência de vírus, pirataria de programas de computador, ataques internos e externos pela rede de dados, sabotagem, fraudes e violações de acesso.

9 - PESSOAS

Todo o efetivo do CREA-AM deve conhecer e cumprir a política de segurança da informação, bem como conhecer e assinar o Termo de Responsabilidade, Confidencialidade e Sigilo De Informações do CREA-AM.

As informações trocadas pela infraestrutura do CREA-AM são consideradas como de uso profissional e não pessoal, reservando-se o CREA-AM o direito de verificar todas as informações transacionadas.

10 - NIVEIS DE ACESSO

Todo e qualquer usuário do âmbito corporativo terá em sua posse autorizações de acesso (Login e Senha) de acordo com suas atribuições, sendo a senha mantida em sigilo e sob a responsabilidade exclusiva do usuário.

Os níveis de acesso serão regidos conforme a seguir:

a) Nível 5: Colegiado;

b) Nível 4: Presidente;

c) Nível 3: Gestores;

d) Nível 2: Usuários;

e) Nível 1: Estagiário;

f) Nível 0: Menor aprendiz.

11 - SEGURANÇA DO AMBIENTE FÍSICO

As máquinas (servidores) que armazenam sistemas do CREA AMAZONAS estão em área protegida – Data Center localizado na Rua Costa Azevedo, Centro – Manaus/AM.

A entrada ao *Data Center* tem acesso devidamente controlado e monitorado.

A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

O acesso às dependências deste Conselho com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da área responsável pela visita e mediante supervisão. Exceto para eventos e treinamentos organizados pelo CREA-AM.

Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

12 - MÁQUINAS – ESTAÇÃO DE TRABALHO

As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

Estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário/usuário ou prestador de serviços que utilizar os equipamentos deste Conselho e podem ser auditados a qualquer tempo pelo Departamento de Tecnologia da Informação.

O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.

Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.

Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades ligadas ao sistema CONFEA/CREA/MUTUA, só devem ser utilizadas em equipamentos com controles adequados.

13 - UTILIZAÇÃO DA REDE CORPORATIVA

Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa do Crea-AM.

Somente os empregados que estão devidamente autorizados a falar em nome do Conselho para os meios de comunicação podem escrever em nome do mesmo em sites de Bate Papo (Chat Room) ou Grupos de Discussão (fóruns, newsgroups). Em caso de dúvidas, procurar a área de Comunicação DO Conselho Regional de Engenharia e Agronomia do Amazonas.

Cada setor possui uma pasta compartilhada no servidor de arquivos para armazenar seus arquivos e todos conteúdo gerado nas estações de trabalho deve ser armazenado neste servidor de rede devidamente configurado em cada estação de trabalho e com acesso a nível de usuário com senha pessoal, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos.

O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante esclarecer que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

Arquivos que estão na rede com mais de 12 meses sem acesso serão copiados em mídia de armazenamento externo via Backup específico e excluídos após. Para ter acesso a esses arquivos, é necessário solicitar a TI.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc.) nos sistemas de armazenamento de dados em rede, pois ocupam espaço comum limitado do departamento.

14 - CONTROLE DE ACESSO

Os acessos às informações e aos recursos de informação do CREA-AM são restritos aqueles que precisam destes recursos para uso profissional no exercício de suas funções. As credencias de acesso aos sistemas (login e senhas) devem ser liberadas somente após a prévia aprovação de seu superior imediato e envio formal de solicitação do RH ou Gerência competente para o departamento que irá fazer a autorização de acesso. **As credenciais de acesso são pessoais e intransferíveis e deverá ser mantida em sigilo.**

O Gestor do departamento e o RH devem comunicar imediatamente a gestão de tecnologia da informação todas as transferências, afastamentos e desligamentos de usuários para que as credenciais de acessos aos sistemas operacionais, aplicativos, e-mails, software corporativo, intranet e rede sejam bloqueadas e/ou removidas.

Os usuários devem trocar suas senhas de acessos periodicamente, para garantir maior nível de segurança em suas contas de login e senha. Não é permitido o acesso à rede interna por equipamentos móveis não pertencentes ao CREA-AM.

15 - EXCEÇÕES

Eventuais exceções devem ser analisadas pela Gestão de TI, gerências competentes, Superintendência Geral e ou Presidência.

16 - PROTEÇÃO CONTRA PRAGAS VIRTUAIS

Os antivírus dos servidores e estações são atualizados automaticamente.

A varredura por vírus é feita diariamente nas estações e nos servidores.

As manutenções programadas serão comunicadas com antecedência, no período agendado o pessoal da ADTI poderá ter acesso completo a todo e qualquer computador de propriedade do Crea Amazonas para verificação.

É expressamente proibido remover ou modificar sistemas de detecção, prevenção e eliminação de vírus dos computadores, assim como é expressamente proibido desenvolver vírus ou outros códigos maliciosos com recursos de tecnologia do CREA-AM.

17 - INSTALAÇÃO DE SOFTWARE

O Crea Amazonas respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores do Conselho ou em suas Inspetorias. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) em todos os setores sejam internos ou externos do Crea Amazonas.

A área de Infraestrutura de TI deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

Qualquer instalação de software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico – Infraestrutura TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente. A Gerência de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

18 - SEGURANÇA NO ACESSO A INTERNET

O acesso à Internet deve ser realizado para fins de atividades profissionais e para exercício das funções contratadas pelo CREA-AM. Engloba nesta política desde a navegação a sites, downloads e uploads de arquivos. É terminantemente proibido o uso da Internet para acesso à sites ou endereços eletrônicos vinculados a atividades de pornografia, pedofilia, atividades ilícitas ou não éticas e preconceituosas, que incitem violência ou de violência explícita ou que não está homologada devidamente para uso, ou material que esteja em desacordo com a legislação vigente no país ou que não estejam diretamente relacionados às atividades funcionais contratadas pelo CREA-AM.

Acessos a outros sites que não estejam homologados deverão ser solicitados para a Gestão de TI, mediante justificativa e ciência dos gestores da área solicitante, quando não houver nenhum risco à organização. Todas as ações ou transações efetuadas na internet são de inteira responsabilidade do detentor da credencial de acesso e serão monitoradas. É vedado qualquer tipo de download. Como também o upload de qualquer software licenciado ao Conselho ou de dados de propriedade deste Conselho ou de suas Inspetorias, sem expressa autorização do gerente responsável pelo software ou pelos dados. Os acessos à internet poderão ser monitorados através de identificação e autenticação do usuário ou de qualquer outra forma que a gestão do Crea Amazonas ache necessária para preservar a segurança.

Para ter maior segurança na internet, recomendamos o acesso à cartilha de segurança para Internet desenvolvida pela CERT.br (Centro de Estudos, Repostas e Tratamento de Incidentes de Segurança no Brasil) que contém recomendações sobre como o usuário pode aumentar a sua segurança na internet. Acesso à cartilha: http://cartilha.cert.br

19 - ACESSO WI-FI (Rede Sem Fio)

O acesso à infraestrutura de rede sem fio deve ser realizado para a execução das atividades profissionais e exercício das funções contratadas pelo CREA-AM.

A infraestrutura de rede sem fio está disponível em todo âmbito do Conselho sendo assim possível conectar-se à rede corporativa que é de uso exclusivo dos ativos tecnológicos deste Conselho.

A rede sem fio possui senha de autenticação criptografada em padrões de segurança WIFI e demais controles criptográficos que podem ser implementados pelo Departamento de Tecnologia da Informação para monitoramento do comportamento do usuário quando estiver utilizando os recursos do Conselho.

É obrigatório o uso de um antivírus nos ativos tecnológicos conectados à rede sem fio, o mesmo deverá ser mantido sempre atualizado.

Qualquer ativo tecnológico, que não seja de patrimônio do Conselho poderá ser bloqueado sem aviso prévio, de forma a preservar a integridade e a disponibilidade da rede corporativa, garantindo assim a segurança da informação.

Este CONSELHO disponibilizará ao público rede WIFI chamada “WIFI SOCIAL” com regras de segurança especifica garantindo a segurança da informação.

Efetuar ação s que possam ser caracterizadas como violação da segurança da rede sem fio, como interferir no sinal WIFI, manipular, sabotar, usar sniffers, efetuar ou fazer varreduras na rede, quebrar a senha de acesso, ataques, fraudar, burlar, desenvolver vírus ou outros códigos maliciosos, o usuário estará sujeito às punições previstas nessa política de segurança de informação sem prejuízo das demais medidas cabíveis de acordo com as leis vigentes no Brasil.

20 - REGRAS PARA UTILIZAÇÃO DO CORREIO ELETRÔNICO (E-Mail)

É proibido o uso do Correio Eletrônico (domino @crea-am.org.br) para envio de mensagens que possam comprometer a imagem deste Conselho perante os profissionais e a comunidade em geral e que possam causar prejuízo moral e ou financeiro, evite utilizar o e-mail do Conselho (domino @crea-am.org.br) para assuntos pessoais.

O Crea-AM é proprietário de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação do conselho e define o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de interesse do Crea Amazonas e podendo ser monitorado por ser propriedade deste Conselho e até mesmo vistoriado por direitos de verificação e auditoria.

Não execute ou abra arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas, mas não se limitando a: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

Não utilize o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft, Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, nem opiniões sexuais ou de raça etc. (Sua opinião é somente sua e nem sempre reflete a opinião deste Conselho). Os recursos tecnológicos do Crea-AM devem ser utilizados apenas no cumprimento de sua missão institucional.

Utilize o e-mail para comunicações oficiais internos, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

A utilização do e-mail/webmail do Crea Amazonas fora do horário de trabalho para posições que possuam controle/reporte de jornada deve ser aprovado pelo chefe do setor.

É expressamente proibido o envio de mensagens relacionadas a atividades ilícitas, não éticas, preconceituosas, de solicitação de ajuda financeira, ou relativa a atividades profissionais não ligadas a ATIVIDADES DESENVOLVIDAS PELO Crea-AM, pessoais, disseminação de correntes, pornografia, pedofilia, que incitem violência ou de violência explícita, distribuição de materiais protegidos por leis de direitos autorais, como por exemplo: software, música e vídeos, divulgação de documentos restritos e não autorizados, dentre outros.

Toda comunicação eletrônica através do e-mail corporativo é considerada de posse, custódia e controle deste Conselho e será monitorada através de ferramentas especializadas.

21 - USO DE SOFTWARES DE MENSAGENS

A instalação de software de mensagens e a liberação do acesso são restritas e sua utilização deve ser justificada à Gerência de TI.

O uso de sistemas de mensagens é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação online, no exercício de sua função. Enquanto o uso responsável dos sistemas de mensagens é estimulado, o seu abuso deve ser evitado.

Sistemas de mensagens possuem histórico de riscos associados à malwares (p.ex. Vírus, worms etc), de forma que deve ser utilizado com zelo e cuidado.

O uso de sistemas de mensagens em redes de relacionamento pessoais deve ser evitado no ambiente corporativo. Podendo a ADTI bloqueá-las por não haver finalidades laborais, o que usualmente torna-se contraproducente.

O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos para se instalarem e iniciarem os processos danosos, não só para aquele dispositivo, mas para todos os que a ele estiverem conectados ou que estiverem em rede. Exemplos de softwares de Mensagens: mIRC, Scoop Script, Avalanche, Full Throttle, MSN Messenger, Yahoo Messenger, Skype, etc.

22 - CONTROLE DE ACESSO VIA VPN

O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com o seu trabalho devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

É vedado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações deste Conselho.

Nunca deixar sessões VPN abertas. Cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar logoff ou bloquear seu equipamento. Mantenha-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

23 - CONTROLE DE ACESSO LÓGICO (Baseado em Senhas)

Os usuários poderão ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal. Utilize senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não utilize informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha. Utilize um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma. Não inclua senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função. A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso. A troca de uma senha bloqueada só será liberada por solicitação do próprio usuário.

24 - COMPARTILHAMENTOS DE ARQUIVOS (Ponto a Ponto (P2P))

Este tipo de software promove um compartilhamento universal de arquivos, permite vulnerabilidades que são exploradas pelos vírus e/ou por “hackers” que vasculham por redes passíveis de invasão de todos os formatos, permitindo ainda ao usuário executar o referido arquivo on-line ou baixá-lo em seu computador onde não será permitida a utilização do mesmo, pois o impacto causado a organização é muito grande, traz assim a descontinuidade das atividades faz com que o Conselho fique indisponível por tempo indeterminado. O usuário estará sujeito as punições previstas na legislação e nessa política de segurança de informação. Exemplos de Compartilhadores de Arquivos P2P: Torrent, uTorrent, Kademlia, Gnutela, Kad Network e SoulSeek. eMule, LimeWire, Ares Galaxy, Shareaza, DreaMule, iMesh e Morpheus, UFull, Throttle, Kazaa, Napster, Mp3X dentro outros com relação a P2P e suas variáveis.

O processo de realização de downloads exige boa parte da banda de navegação do servidor e, quando realizado em demasia congestiona o tráfego do link da organização do CREA-AM, assim congestiona o fluxo de tráfego do link corporativo e compromete sistemas que funcionam on-line, deixando extremamente lento ou inacessível. Todo tráfego de download exercível não será permitido, exceto para fins profissionais da organização, não havendo o cumprimento dessas diretrizes resultará em penalidades de acordo com as punições prevista nesta política de segurança de informação.

Uma vez que não existe qualquer pertinência com as finalidades institucionais propostas por esta organização, é terminantemente proibida a execução de jogos, streaming, músicas, vídeos ou rádios on-line ou localmente em seu ativo tecnológico proposto pelo CREA-AM, visto que esta prática congestiona o fluxo de tráfego do link corporativo e compromete sistemas que funcionam on-line. Toda e qualquer execução de jogos, rádios, ou qualquer tipo de streaming on-line não será permitido, exceto para fins das atividades da organização, o não cumprimento destas diretrizes, implica o usuário em infrações e punições de acordo com o previsto nessa política de segurança de informação.

25 - CONTROLE DE ATIVOS DE INFORMAÇÃO

Ativos da Informação são Ativos importantes para o CREA-AM e se não forem protegidos adequadamente, podem causar impacto negativo ao negócio ou à infraestrutura deste Conselho. São considerados ativos de informação, dentre outros: Documentos, Documentação de sistemas, Arquivos digitalizados, Informações sobre pessoas, profissionais, clientes, parceiros, empresas, terceiros ou pesquisas competitivas, Sistemas, Programas e código fontes, Aplicativos, Licenciamento de software ou outros, Computadores de mesa, notebooks, netbooks, caneta digital, smartphones, tablets, gps, celulares, pen drive, access point, modem móvel, DVD, ou qualquer outra forma eletrônica, magnética ou óptica, Servidores de rede, Senhas de acesso, Crachás, Imagem do CREA-AM.

Cada ativo deve possuir um proprietário responsável pela sua manutenção, proteção e autenticidade.

Os ativos devem ser classificados de acordo com critérios de confidencialidade, integridade e disponibilidade e protegidos de acordo com a importância que cada um representa.

26 - CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada setor estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por seu setor de acordo com os critérios a seguir:

Pública: É uma informação do CREA-AM ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

Interna: É uma informação do CREA-AM que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem do Conselho, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços.

Confidencial: É uma informação crítica para os negócios do CREA-AM ou de seus profissionais. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais o CREA-AM ou aos seus colaboradores. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, profissionais e/ou fornecedores.

Restrita: É toda informação que pode ser acessada somente por usuários do CREA-AM explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao Conselho.

27 - ARMAZENAMENTO DE ARQUIVOS

Todo departamento tem um espaço no servidor de armazenamento de dados para guardar arquivos. Durante o processo de autenticação do usuário, o sistema mapeia automaticamente uma letra associada ao espaço correspondente ao seu setor. Esse espaço é exclusivo para alocar arquivos pertinentes ao negócio CREA-AM.

Não se deve armazenar, nesse local, arquivos de cunho particular ou arquivos do tipo, imagem, vídeos ou áudio e etc que não estejam relacionadas as atividades laborais, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem aviso prévio.

É proibido o acúmulo de arquivos inúteis no diretório pessoal, seja no servidor ou na estação. E extremamente proibido copiar e mover para os drives de rede arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, etc...). Necessidades específicas de armazenamento devem ser solicitadas junto à gestão de TI, que será analisada a possibilidade do deferimento fazendo.

Todo usuário ao acessar a rede terá um atalho automaticamente da pasta chamada PUBLICA ou similar que seja comum a todos os usuários, aonde poderá utilizar da mesma para transferência de arquivos com outros departamentos, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível. Este compartilhamento de pasta PUBLICA e para diminuir o uso de “pen drives” dentro do Conselho, diminuindo assim riscos com vírus, worm, spyware, malware, etc. A pasta PUBLICA é simplesmente para arquivos temporários para troca de informações com outros departamentos, sendo assim os arquivos armazenados poderão ser apagados ao final do expediente sem aviso prévio.

Dica ao usuário – Caso esteja trabalhando em arquivos muito complexos com bastante informações, aconselhamos que o usuário faça primeiro em sua estação de trabalho e depois envie para o servidor de arquivo. Se o arquivo já está no servidor de armazenamento copie/mova para sua estação de trabalho, e depois reenvie para o servidor de arquivos.

Dica ao usuário – Arquivo é o ativo de informação do usuário, caso veja que um arquivo especifico seja de suma importância, faça cópias do mesmo em sua estação de trabalho, pen drive ou outro local de sua confiança.

28 - DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Todos os procedimentos e controles para desenvolvimento e manutenção de sistemas devem estar documentados e ser executados pelos responsáveis.

Requisitos de segurança devem ser analisados e implementados no desenvolvimento e manutenção dos sistemas. Entende-se como requisitos de segurança as atividades de análise do sistema, o planejamento de capacidade, a validação dos dados de entrada, processamento e saída, a proteção dos dados de teste, o controle de acesso à biblioteca de objetos fonte, o controle de mudanças no sistema, à verificação de controles internos, o controle do sistema em produção, especificações para contingência do sistema e a habilitação de trilhas de auditoria. O ambiente tecnológico de desenvolvimento dos sistemas, testes, homologação ambientes de produção devem ser segregados, bem como todos seus acessos. Em casos de desenvolvimento de software por terceiros, deve ser elaborado contrato especificando os controles e requisitos mínimos aceitáveis de segurança da informação e qualidade que o sistema deverá conter.

29 - SEGURANÇA FISICA DO AMBIENTE

O crachá de identificação é obrigatório, de uso pessoal e intransferível, e deve ser usado por todos em local visível.

O detalhamento dos itens relacionados a procedimentos e controles, contendo as regras a serem cumpridas, será complementado por normas específicas em desenvolvimento para: Registrar e verificar a entrada e saída de equipamentos nas dependências do CREA-AM, definir responsabilidades aos empregados, gestores, conselheiros, estagiários e menores aprendizes e terceiros quanto ao acompanhamento de visitantes nas dependências do CREA-AM, Câmeras de monitoramento e vigilância no âmbito do Conselho. Os recursos e instalações ligadas aos sistemas de informações críticas para o CREA-AM devem ser mantidos em áreas seguras, protegidas por recursos de controle de acesso, monitoramento e controle constantes do ambiente (detecção e aviso imediato de situações de emergência), climatização adequada, identificação e combate a incêndio, fornecimento ininterrupto de energia e conectividade (segurança no cabeamento).

Fica a critério da gestão de TI, delegar quem pode ou não ter acesso à sala dos servidores e fazer utilização de qualquer equipamento que estiver no ambiente ou fazer manutenção no ambiente.

É terminantemente proibido o acesso de qualquer pessoa que não tenha sido previamente autorizada pela Gestão de TI na sala de servidores, seja qual for o motivo.

Todos no CREA-AM devem adotar o padrão de mesa limpa e tela limpa no seu dia-a-dia, para impedir acessos não autorizados as informações do CREA-AM, não deixando documentos confidenciais em impressoras, sobre as mesas ou em locais acessíveis a pessoas não autorizadas.

Computadores e ativos tecnológicos do CREA-AM não devem ser deixados ligados ou desprotegidos de senha quando não estiverem em uso, ao ausentar do ativo tecnológico bloqueie a seção do ativo para usuários não autorizados.

Papéis ou mídias em geral não devem ser deixados sobre as mesas, especialmente fora do horário normal de expediente ou em horário de almoço.

Documentos impressos ou copiados em máquinas de fotocópias devem ser recolhidos logo após sua geração, os mesmos poderão possuir controle de cota de impressão por usuários no Conselho, podendo ter marcação de folha com nome data e hora do documento impresso.

Usuários de notebooks/netbooks assim como ativos tecnológicos, de propriedade do CREA-AM ou de terceiros, devem utilizar travas de segurança e senhas para evitar roubo e acesso não autorizado do equipamento. Os mesmos não devem ser deixados sobre as mesas durante a noite, exceto se estiverem em sala que seja trancada à chave.

A Assessoria de Tecnologia da Informação do CREA-AM deverá criar mecanismos de segurança para proteção dos dados em dispositivos móveis pertencentes ao Conselho.

A utilização de equipamentos de computação móvel fora das dependências do CREA-AM, como por exemplo: notebooks, netbooks, caneta digital, smartphones, tablets, celulares, modem, deve estar autorizada. Esses equipamentos não devem ser deixados em locais públicos e de fácil acesso (dentro de carros, por exemplo), sem a presença do responsável pelos mesmos. Além disso, devem ser adotados os mesmos controles de segurança utilizados dentro das dependências do CREA-AM.

Em viagens, esses equipamentos devem ser levados como bagagem de mão. O uso de notebooks, netbooks, caneta digital, smartphones, tablets, celulares, modem devem seguir os procedimentos especificados nas normas de uso e zelo do equipamento.

30 - BOAS PRÁTICAS DE SEGURANÇA PARA TRANSPORTE DE NOTEBOOK

Quando em deslocamentos de carro, coloque o mesmo no porta-malas ou em local não visível.

Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas.

Não coloque o notebook em carrinhos de aeroportos nem despache junto à bagagem.

Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.

Evite utilizar o notebook em locais públicos, nos hotéis, preferencialmente, guarde o notebook no cofre do seu apartamento sempre que for se ausentar. Avalie se em pequenas viagens é realmente necessário levar o notebook.

Utilização de equipamentos particulares / terceiros dentro do CREA-AM

Notebooks particulares para serem usadas dentro do CREA AMAZONAS E INSPETORIAS abrangidas neste documento, precisam ser avaliados pelo pessoal responsável de TI. Equipamentos de terceiros devem ser levados ao suporte para serem verificadas a atualização do antivírus e existência de vírus. É responsabilidade da área contratante encaminhar os terceiros sob sua responsabilidade para esta verificação.

31 - UTILIZAÇÃO DE MÍDIAS REMOVIVEIS E DA PORTA USB

A ADTI poderá bloquear as portas USB se necessário para preservar a segurança dos dados, mas poderá liberar por solicitação do encarregado pelo setor através de solicitação por escrito, devendo ser tratado como exceção à regra.

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modens 4G e os pen drives merecem a atenção. Tal vulnerabilidade não pode ser contida com firewalls ou com programas antivírus já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários do Conselho.

Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação da chefia do departamento do solicitante. Para notebooks de gerentes, chefes de setores e cargos acima esta liberação é efetuada por padrão.

Dentro do Crea-AM dê preferência à utilização da rede evitando a utilizando de modem 4G conectado à porta USB do computador, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o funcionário abre a porta para acesso sem qualquer controle. (Nesses casos os sistemas internos de segurança poderão detectar anomalias, isso poderá ser comunicado ao chefe do setor a ao Superintendente para providências administrativas).

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados. (Deve-se evitar a utilização de pen drives utilizados em computadores públicos, faculdades e lan houses nos equipamentos deste Conselho, caso seja inevitável a utilização deve-se fazer verificação com sistema antivírus).

É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

32 - GESTÃO DAS OPERAÇÕES E COMUNICAÇÕES DOS SISTEMAS DE INFORMAÇÃO

Todos os procedimentos de gestão das operações e comunicações dos sistemas de informação devem ser documentados e seguidos.

São considerados procedimentos de gestão das operações e comunicações dos sistemas de informação, dentre outros: Controle de mudanças operacionais, Proteção contra software malicioso, Instalação de programas de computador, Cópias de segurança de dados, Geração e análise de trilha de auditoria, Gerenciamento e controles da rede, Descarte de mídias, Níveis hierárquicos da informação, Documentação de sistemas e, Troca de informação por correio eletrônico, Internet, telefonia ou algum tipo de ativo de informação, ou ativo tecnológico.

33 - GESTÃO DE BACKUPS

Todos os backups serão programados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

O backup de armazenamento do servidor de arquivos é feito diariamente, acompanhado por cópias de sombras e sincronização em outro servidor espelho.

Existem três tipos de rotina de backup de sistemas que podem ser optados de acordo com a necessidade do Conselho, sendo backup completo, backup incremental e backup diferencial.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros. As mídias de backup devem ser acondicionadas de forma adequada segundo as normas da ABNT).

34 - GESTÃO DE CONTINUIDADE DE NEGÓCIOS NO ÂMBITO DO ADTI

Um Plano de Continuidade de Negócios no âmbito do DTI será criado e estará alinhado com a estratégia de negócios do CREA-AM, identificando os possíveis eventos que possam causar interrupções nos processos de negócio, como falhas em equipamentos, erros humanos, catástrofes e incidentes. Este plano deverá estar documentado, ser revisado, atualizado e testado periodicamente.

Todos os envolvidos em atividades de contingência e de continuidade serão devidamente treinados e serão atualizados em relação à política de segurança da informação.

35 - EXCEÇÕES à POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CREA-AM

As exceções à política de segurança da informação devem ser justificadas, por escrito, pelos solicitantes e serão analisadas previamente pelo Gestor de Tecnologia da Informação, podendo solicitar autorização de alçada superior (Gestor, Superintendente Geral ou Presidente do Conselho). As eventuais exceções, aprovados pela gestão, continuam reguladas pela política de segurança da informação e estão passíveis das penalidades aplicáveis.

36 - OUVIDORIA

Ouvidoria do CREA-AM pode ser contatada através dos seguintes canais: pelo e-mail – ouvidoria@crea-am.org.br; pelo telefone (92) 2125-7171 ou pessoalmente, no horário de 9h às 17h, na sede do CREA-AM localizada à Rua Costa Azevedo – 174 – Centro. No site – crea-am.org.br

37 - VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

38 - ATUALIZAÇÃO

Esta política será revisada a cada 12 meses ou a qualquer momento ato do Presidente do CREA-AM.

39 - DOCUMENTOS DE REFERÊNCIA

NBR ISO/IEC 17799:2005, ABNT 21:204.01-010, Lei 9.609/98 – Lei do Software, A *Lei 12.737*, de 30 de novembro de 2012, Lei nº 11.829, de 25.11.2008 CPPB em seus artigos 240 e 241 e 482 da CLT, Lei Federal n. 13.709/2018.