01	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO			
	NÚMERO	ACESSO	REVISÃO	PÁGINA
	GTI – 001	Restrito	01	1/31

CAMPO DE APLICAÇÃO

DIREÇÃO	GERÊNCIA	ASSESSORIAS
☒ GAB. PRESIDÊNCIA ☒SUPERINTENDÊNCIA	☒ INFRA-ESTRUTURA ☒ OPERACIONAL ☒ TECNOLOGIA DA INFORMAÇÃO ☒ GESTÃO COM PESSOAS ☒ FINANCEIRA/CONTABIL	☒ TÉCNICA ☒ COMUNICAÇÃO ☒ JURÍDICA

CONTROLE DE REVISÃO

REVISÃO: 01	PÁGINAS: Todas	DATA
MODIFICAÇÕES: Atualização ambiente de rede		06/01/2012
REVISÃO:	PÁGINAS:	DATA
MODIFICAÇÕES:		
REVISÃO:	PÁGINAS:	DATA
MODIFICAÇÕES:		

REAPROVAÇÃO DO DOCUMENTO

SITUAÇÃO:

NOME	ASSINATURA	SETOR	DATA

REGISTRO DE TREINAMENTO

NOME	ASSINATURA	SETOR	DATA

APROVAÇÃO

	ELABORAÇÃO	VERIFICAÇÃO	APROVAÇÃO
RESPONSAVEL	Tecnologia da Informação	Controladoria	Presidência
NOME/ASSINATURA			

1. OBJETIVO

Fornecer diretrizes e normas para a proteção e segurança dos ativos de informação da empresa, garantindo sua confidencialidade, integridade, disponibilidade, legalidade e auditabilidade.

1.1 OBJETIVOS ESPECÍFICOS

- Orientar aos usuários através das normas e procedimentos desta política, todas as ações de segurança dos ativos da informação.

- Instituir procedimentos para prevenir, responder e gerenciar os incidentes de segurança da informação da instituição, através da ação do Comitê de Segurança da Informação (Comitê SI).

- Colocar o CREA - AL em conformidade com a Norma Técnica ABNT NBR ISO/IEC 17799.

2. DOCUMENTOS COMPLEMENTARES / REFERÊNCIAS

ABNT NBR ISO / IEC 17799
ABNT NBR ISO / IEC 27001

3. DEFINIÇÕES

Segurança da Informação

É a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento

Ativos de Informação

Qualquer elemento que tenha valor para o CREA - AL e forneça suporte aos processos de negócios da empresa.

Categorias:
- Informações
- Software
- Hardware
- Ambiente Físico
- Pessoas
- Serviços

Dados

Qualquer elemento identificado em sua forma bruta, que em determinado contexto não conduz, por si só, à compreensão de determinado fato ou situação

Informação

Dados organizados e inseridos em um contexto, de maneira a propiciar determinado retorno ao manipulador, permitindo a escolha entre os vários caminhos que possam levar a um resultado.

Sistema de Informação

Conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção.

Sistema de Segurança da Informação

Sistema destinado à proteção contra a quebra de confidencialidade, de integridade ou de disponibilidade de dados ou informações, armazenados, em processamento ou em trânsito, podendo abranger a segurança dos recursos humanos, da documentação e do material das áreas e instalações de comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Princípios de Segurança da Informação

Responsabilidade - As responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.

Conhecimento - Para garantir a confiança no sistema, os administradores, os fornecedores e os usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários.

Ética - Todos os direitos e interesses legítimos de usuários, intervenientes e colaboradores devem ser respeitados ao prover um sistema de informação e ao estabelecer um sistema de segurança.

Legalidade - Processos de segurança devem levar em consideração os Objetivos, Princípios e Missão do CREA - AL; bem como as leis, normas e políticas organizacionais, administrativas, comerciais, técnicas e operacionais;

Proporcionalidade - O nível, a complexidade e os custos dos processos de segurança devem ser apropriados e proporcionais ao valor e à necessidade de confiança nos sistemas de informação considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual.

Integração - Os processos de segurança devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de criar um sistema de segurança da informação coerente.

Celeridade - As ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível.

Revisão - Os sistemas de segurança devem ser reavaliados periodicamente, uma vez que os sistemas de informação e os requisitos de segurança variam com o tempo.

Liberdade - Um sistema de segurança da informação deve ser compatível com o legítimo uso e fluxo de informações/dados devendo ser observadas as normas de privacidade e de direito de realização de auditorias.

Propriedades da Segurança da Informação

Confidencialidade – Certeza do que foi dito, escrito ou falado será acessado somente por pessoas autorizadas (Confidencialidade requer Integridade).

Integridade – Garantia de que a informação não foi alterada (de forma indevida ou não autorizada), a quebra da Integridade ocorre quando a informação é corrompida, falsificada ou roubada.

Disponibilidade – Garantia de que a informação será acessada pelos usuários autorizados sempre que necessário.

Legalidade – O uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos.

Auditabilidade – O acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.

Não repúdio – O usuário que gerou ou alterou a informação não pode negar o fato, pois existem mecanismos que garantem a sua autoria.

Vulnerabilidades

Fragilidade de um ativo ou grupo de ativos que possam ser exploradas por uma ou mais ameaças, devem ser identificadas e corrigidas.

Tipos:
- Físicas
- Naturais
- Hardware e Software
- Comunicações
- Humanas

Ameaças

Agente de um incidente indesejado que pode resultar em dano para a empresa. A Segurança da Informação precisa prover mecanismos para impedir que as Ameaças explorem as Vulnerabilidades.

Tipo:
- Naturais
- Intencionais
- Involuntárias

Responsabilidade

Obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de ativos de informação.

Usuário

Indivíduo com acesso autorizado a dados e informações de acordo com os controles de acesso definidos.

Colaborador

Todos os funcionários do CREA - AL.

Terceiros

Pessoas envolvidas com o desenvolvimento de atividades na organização, de caráter permanente, continuado ou eventual, dentre os quais prestadores de serviço, consultores e estagiários.

Acesso

Possibilidade ou permissão para se obter ou utilizar dados ou informações.

Controles de Acesso

Restrições ou permissões de acesso concedidas ao usuário.

Direito de acesso

Faculdade de adentrar em um sistema de informação, respeitada a necessidade de conhecer.

Necessidade de Conhecer

Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou informações internas e/ou confidenciais.

Proprietário

É o responsável pelo ativo de informação da sua área.

Custódia

Consiste na responsabilidade de se guardar um ativo, entretanto a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder o acesso a terceiros.

Incidente de segurança de informação

Conjunto de atividades ou eventos correlacionados entre si, abrangentes à confidencialidade, integridade ou disponibilidade da informação.

4. SIGLAS

CREA - AL – Conselho Regional de Engenharia e Agronomia de Alagoas
GTI – Gerência de Tecnologia da Informação
GINF – Gerência de Infraestrutura
RH – Gerência de Gestão com Pessoas (Ouvidoria)
CEQ – Coordenação do Escritório da Qualidade
SI – Segurança da Informação
SGSI – Sistema de Gestão da Segurança da Informação
CSI – Comitê de Segurança da Informação
ABNT – Associação Brasileira de Normas Técnicas
NBR – Norma Brasileira

5. DIRETRIZES

5.1 INTRODUÇÃO

O Conselho Regional de Engenharia e Agronomia de Alagoas através de sua Direção determina a implantação da Política de Segurança da Informação da Instituição objetivando proteger seus ativos de informações.

5.2 APLICAÇÃO

- Todos os ambientes e colaboradores da instituição que utilizam os ativos de informação.
- Referência para o Comitê SI prevenir, responder e gerenciar todas as situações de violação da segurança da informação, tais como roubo, fraude, acessos não autorizados de clientes/terceiros, tentativas de engenharia social, ameaças físicas, naturais, etc.

5.3 AGENTES ENVOLVIDOS

5.3.1 Comitês

Comitê de Segurança da Informação – Comitê SI

Têm como principal função estabelecer junto com os Proprietários da Informação os procedimentos de segurança, além de gerenciar incidentes, divulgar e pôr em vigor a Política de Segurança da Instituição.

5.3.2 Gerências

Gerência de Tecnologia da Informação – GTI

A Gerência de Tecnologia da Informação é a gestora dos ativos de informação, preside o Comitê de Segurança da Informação e é responsável pela elaboração e atualização da Política de Segurança da Informação.

Estão sob sua responsabilidade direta os Bancos de Dados, toda a infra-estrutura de Software e Hardware além dos serviços de manutenção e backup relacionados aos mesmos, desta forma a GTI gerencia e controla todas as informações da rede de computadores e seus sistemas e/ou informações oriundas destes recursos.

Os procedimentos de Segurança da Informação sob controle da GTI encontram-se nos capítulos 5.6, 5.7 e 5.10.

Gerência de Infra-Estrutura – GINF

Tem como principal função dentro da Política de Segurança a aplicação das medidas de segurança e de continuidade para os ativos de informação relacionados ao ambiente físico além de serviços para manutenção e operacionalidade destes ambientes.

Os procedimentos de Segurança da Informação sob responsabilidade da GINF encontram-se no capitulo 5.8 e 5.10.

Gerência de Pessoas

Participa da Política de Segurança através da divulgação e treinamento da mesma, delibera sobre os relatórios do Comitê SI no que se refere ao estabelecimento de sanções e penalidades nas situações avaliadas em que a política for desrespeitada.

Os procedimentos de Segurança da Informação gerenciados pelo RH encontram-se no capitulo 5.9.

5.3.3 Colaboradores

Gestor da Informação: Afrânio Bastos (Gerente de Tecnologia da Informação)
Responsabilidade: Segurança da Informação do CREA - AL

Custodiantes GTI:, Guilherme Correia (CREA - AL),
Responsabilidade: responsável pelos ativos de Hardware, Software, Serviços de Backup e Manutenção de Computadores e Sistemas.

Custodiante GINF: Petrucio Lima (Gerente de Infraestrutura)
Responsabilidade: Prover ambiente físico e manutenção adequada à proteção dos ativos.

Custodiante Gerencia de Pessoas: Fernanda Fernandes (Gerente de Pessoas)
Responsabilidade: Gerenciar os procedimentos de Segurança da Informação envolvendo os colaboradores.

Comitê de Segurança da Informação: Afrânio Bastos (GTI), Guilherme Correia (GTI), Fernanda Fernandes (Gerente de Pessoas), Petrucio Lima (GINF)
Responsabilidade: São responsáveis pela garantia de que a segurança das informações estão de acordo com a política implementada.

Usuários da GTI:

CREA - AL – Afrânio Bastos de M. Neto, Guilherme Correia
Responsabilidade: Auxiliam os Custodiantes e o Comitê SI no controle e monitoramento da política.

Proprietário da Informação: Gerentes, Coordenadores e Supervisores da instituição.
Responsabilidade: São responsáveis pelos ativos de informação de seu setor e classificam junto com o Comitê SI e Custodiantes os níveis de acesso das mesmas.

Usuários da Informação: Todos os colaboradores da instituição ou terceiros que venham utilizar informação da mesma.
Responsabilidade: São responsáveis pelo cumprimento da Política de Segurança da Informação. Seus níveis de acesso aos ativos de informação são determinados pelos proprietários da informação de acordo com suas funções.

5.4 CLASSIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO

Os ativos de informação são o patrimônio composto por todos os dados e informações gerados e manipulados nos processos operacionais da CREA - AL, bem como todos os elementos de infraestrutura, tecnologia, hardware, software, pessoas e serviços necessários à execução destes processos.

Classificação dos Ativos de Informação no CREA - AL	
Natureza do Ativo	Descrição
1- Informações	- Banco de dados e arquivos magnéticos. - Manuais de rotinas e procedimentos - Documentos em papel - Documentos operacionais da empresa - Documentos e relatórios confidenciais - Relatórios e impressos dos sistemas
2- Software	- Sistemas operacionais - Aplicativos - Utilitários
3- Hardware	- Servidores, desktops e notebooks. - Impressoras e copiadoras. - Equipamentos eletrônicos digitais. - Equipamentos e instalações de comunicação de dados (roteadores, switchs, cabeamento, etc.) - Mídias magnéticas e ópticas.
4- Ambiente Físico	- Móveis, prédios, salas, acomodações, mobílias, etc. - Geradores, no-break e ar-condicionado.
5- Pessoas	- Empregados, estagiários, terceiros e fornecedores.
6- Serviços	- Comunicação (ligações telefônicas, videoconferências, etc.) - Serviços de backup, manutenções e atualizações de sistemas. - Manutenção de hardware, elétrica, refrigeração, telefônica, etc.

Tabela 1

Gerências Responsáveis pelos Ativos de Informação	
Natureza do Ativo	Gerências
1- Informações	*Todas as Gerências*
2- Software	GTI – Tecnologia da Informação
3- Hardware	GTI – Tecnologia da Informação
4- Ambiente Físico	GINF – Infraestrutura e Patrimônio
5- Pessoas	GP – Gestão com Pessoas
6- Serviços	GTI – Tecnologia da Informação GINF – Infraestrutura e Patrimônio

Tabela 2

5.5 ATIVO - INFORMAÇÃO

Os ativos de informação classificados como Informações (*ver tabela 1*) são compostos por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos operacionais do CREA - AL, como conseqüência utilizam-se do ativo “Software” no processamento dos dados os quais dão origem a maior parte das informações.

5.5.1 Política de Classificação e Descarte da Informação

Ver NQ/GTI-CSI-002

5.5.2 Normas e Procedimentos de Segurança

5.5.2.1 Política de Acesso Físico

A política de acesso físico tem como objetivo prevenir a controlar o acesso as informações e instalações físicas do CREA - AL, evitar perda, dano ou comprometimento dos ativos além de prevenir e evitar a exposição e/ou roubo dos ativos de informação e equipamentos.

1- É obrigatório o uso do crachá para acesso e circulação de funcionários às dependências do CREA-AL.

2- Todo acesso às salas e dependências do CREA por outrem que não seja funcionário do setor é expressamente proibido a menos que seja formalmente permitido.

2.1- É obrigatório o uso de crachá de identificação para os terceirizados e visitantes.

2.2- É dever de todo o colaborador informar ao setor de segurança sobre a presença de qualquer pessoa não identificada (sem o crachá de visitante) acompanhada ou não, dentro das dependências do CREA.

3- Salas abertas somente enquanto houver pessoas autorizadas pelo gerente ou responsável a ficarem.

4.1- Clientes, visitantes e terceiros não podem ter acesso às salas e departamentos, salvo autorizados expressamente pelo responsável.

5- Visitante e pessoal terceirizado deve ser supervisionado na portaria. Suas horas de entrada e saída e o local de destino devem ser registrados e sua entrada previamente autorizada pelo responsável.

6- Não permitido filmagem e fotografias através de câmeras fotográficas, filmadoras, aparelhos celulares e outros sem autorização do responsável pelo setor.

7- A salas dos servidores GTI têm acesso restrito apenas ao Gestor da Informação e Custodiantes da GTI.

- Serviços de manutenção na sala dos servidores deve ser acompanhado presencialmente por um dos Custodiantes da GTI.

8- O usuário não pode permitir acesso e uso de pessoas sem autorização aos seus computadores.

9- Perdas de chaves deve ser informada imediatamente para que possa providenciar a troca da fechadura e de outras cópias das chaves perdidas.

10- As áreas consideradas estratégicas devem possuir circuito fechado de TV, havendo registro por meio de câmeras de vídeo, que deverão estar armazenadas em mídia magnética e/ou óptica, de forma a poderem ser resgatadas em caso de alguma ocorrência ou auditoria.

11- Deve-se haver alarmes em áreas estratégicas com gerenciamento remoto caso ocorra acessos não autorizados.

12- Áreas estratégicas devem ter perímetros de segurança (barreiras como: paredes, portões de entrada controlada por cartão ou balcões de recepção com recepcionistas)

13- Serviços de terceiros devem ser agendados previamente, deve ser fornecido o nome das pessoas que executarão o serviço, assim como o detalhamento da atividade a ser desenvolvida e aprovada pelo gerente da área.

14- Trabalhos feitos fora da instituição devem ter seu conteúdo aprovado previamente pelo gerente do setor.

15- Pontos de entrega e de carregamento de materiais pelos fornecedores devem ser controlados, para evitar que pessoas não autorizadas entrem nas instalações do CREA.

5.5.2.2 Política de Mesa Limpa e Tela Limpa

Visando evitar acessos não autorizados a Política de Mesa Limpa e Tela Limpa considera que quando o usuário não estiver usando a informação, a mesma não deve ficar exposta.

1- Papéis e mídias removíveis quando não usados devem ser imediatamente armazenados.

2- Quando não utilizar a tela do computador será iniciado automaticamente à proteção de tela com senha.

3- Antes de ausentar-se de seu local de trabalho, o usuário deverá fechar todos os programas em uso e efetuar *logoff* da rede. Caso a ausência seja definitiva deve-se desligar o equipamento, inclusive o estabilizador.

4- É proibido o consumo de alimentos, bebidas e fumo nos setores.

5.5.2.3 Política de Manuseio e Armazenamento Físico

1- Documentos e mídias removíveis devem ser armazenados em salas e/ou armários com chave e acessados apenas pelos funcionários do setor.

2- Documentos e mídias removíveis devem estar identificados conforme o nível de proteção: Interna(2) ou Confidencial(3), sob forma de carimbos ou etiquetas. (ver NQ/GTI-CSI-002 Política de Classificação e Descarte da Informação)

3- Chaves de gavetas, armários e portas devem ser guardadas em local de acesso controlado e restrito.

5.5.2.4 Política de Acesso Externo

Recursos de processamento da informação e informações do CREA - AL que são acessados, processados, comunicados ou gerenciados por partes externas devem ser identificados e controlados pelos seus respectivos proprietários da informação.

Deve-se identificar / avaliar: - Riscos relacionados com as partes externas
- Avaliação da informação a ser concedida a clientes
- Avaliação da informação a ser concedida a terceiros

5.5.2.5 Documentação dos Procedimentos Operacionais

Os procedimentos operacionais devem ser documentados, mantidos atualizados, armazenados adequadamente e disponíveis a todos os usuários que deles necessitem.

5.6 ATIVO – SOFTWARE

5.6.1 Classificação e Controles de Acesso ->

Inventário e Classificação dos Softwares Utilizados

Sistemas Operacionais	Versão	Qtde.
Windows 2007		
Windows Vista Bussines		
Windows XP Professional		
Windows 2003 Server Standard		

Windows 2008 Server Standard		
Linux		
Mikrotik		
Aplicativos		
Banco de Dados Firebird		
Sistema Implanta (Financeiro/Contabil/Patrimonio/Compras)		
Sistemas Gerenciais		
MV 2000i		
Ronda/Rubi (folha de pagamento)		
Pacote Office [Editor/Planilha/Apresentação/Correio]		
MS Office 2003		
BrOffice + Thunderbird		
Navegadores		
Internet Explorer		
Firefox		
Utilitários		
Ferramentas de Desenvolvimento		
PLSQL Developer		
SQL Navigator		
Ferramentas de Conexão e Comunicação		
Symantec PC Anywhere		
Anti-Vírus		
Outros		

Tabela 11

Formas de Acesso aos Sistemas

Serviços Disponíveis	Controle de Acesso
Rede	Perfil de usuário
Rede + Minerva	Perfil de usuário
Rede + Minerva + Folha de pagamento	Perfil de usuário
Rede + Minerva + Implanta	Perfil de usuário

Tabela 12

Classificação Geral de Acesso aos Sistemas

Serviços	Perfil	Acessos
Rede	Administrativo Geral 1 Administrativo Geral 2 GTI Administrador da Rede GTI Suporte GTI Técnico	*Ver tabela 14*
Sistema Folha	Administrativo Operador	Todos os Módulos, Tabelas e Config.
Sistema Implanta	Administrador	Tabelas e Configuração

	Operador	Operacionalização e Relatórios.

Tabela 13

Classificação Detalhada de Acesso a Rede

Servidores			
Perfil	Acessos	Restrições	Pastas Disponíveis
Básico	Minerva Impressão OpenOffice Acrobat Reader	Internet Menu Iniciar Mídia Magnética Dispositivos USB Área de Trabalho Unidade C / Explorer Instalação de Programas	S:\Setores \Meus Documentos U:\Usuario
Gerentes	Sistema Sitac Internet Impressão OpenOffice Mídia Óptica Acrobat Reader Mídia Magnética Internet Explorer Área de Trabalho Dispositivos USB Unidade C / Explorer Compactador de Arquivos	Mídia Magnética Área de Trabalho Instalação de Programas	S:\Setores \Meus Documentos U:\Usuario
Financeiro	Sistema Implanta Sistema Minerva Internet Impressão OpenOffice Mídia Óptica Acrobat Reader Mídia Magnética Internet Explorer Área de Trabalho Dispositivos USB Unidade C / Explorer Compactador de Arquivos	Menu Iniciar Instalação de Programas Área de Trabalho	S:\Setores S:\Setores \Meus Documentos U:\Usuario
Pessoal	Sistema Minerva Sistema Folha Impressão OpenOffice Acrobat Reader Impressão	Internet Menu Iniciar Mídia Magnética Dispositivos USB Área de Trabalho Unidade C / Explorer Instalação de Programas	S:\Setores \Meus Documentos U:\Usuario
GTI			
Adm. Rede			
Programador			*Códigos fonte*

			Ambiente simulação *Ambiente desenvolvimento*
Suporte Folha			
Técnico			

Tabela 14

5.6.2 Normas e Procedimentos de Segurança

5.6.2.1 Política de Acesso Lógico

1- Cada usuário terá sua conta de acesso que é única, exclusiva e intransferível.

2- Tipos de conta:
- Colaboradores
  [Primeiro nome]+[matrícula]
- Terceirizados
  [Nome da empresa]+[primeiro nome]
- Outros
  [Função]+[primeiro nome]

3- As contas de usuário possuem acesso limitado nas estações de trabalho, os quais variam de acordo com o perfil do mesmo.

4- As contas e perfis de acesso dos usuários serão revisados periodicamente, cabendo à GTI o direito de retirar acessos sem comunicação prévia caso se verifique incidentes suspeitos ou outra situação de maior relevância.

4.1- Contas que estejam sem utilização por mais de 90 dias serão suspensas, a não ser em casos justificados;

5- Todo o colaborador poderá ter uma conta para acesso aos recursos da rede, mas para acesso a sistemas específicos deverá ter uma conta e senha pessoal e intransferível.

6- A criação de contas se fará mediante o preenchimento pelo setor solicitante do documento DOC-TI Cadastro de Usuário, cabe a GTI após análise a aprovação ou não deste cadastro.

7- As contas de acesso a rede e sistemas e seus respectivos *logs* podem ser monitoradas pela GTI com o objetivo de se verificar possíveis irregularidades.

8- Sessões inoperantes nos sistemas serão inativadas após tempo pré-definido.

9- Acesso a servidores para serviços críticos devem ter horário de conexão agendado e autorizado pela GTI.

5.6.2.2 Política de Uso da Intranet

1- Instalação e/ou utilização de equipamentos de informática pertencentes ou não a CREA - AL só poderão ser usados após liberação da GTI.

2- Todas as instalações de programas estão bloqueadas e só serão permitidas após autorização da GTI.

2.1- Jogos ou qualquer tipo de software/aplicativo não pode ser gravado ou instalado no diretório pessoal do usuário, no computador local e em qualquer outro diretório da rede, somente será permitido o uso de softwares previamente instalados no computador.

2.2- Material de natureza pornográfica, pedófila, racista, páginas de animação, vídeo, filmes, ou outra atividade que comprometa a imagem do CREA - AL ou que não se relacione com o trabalho do setor não pode ser exposto, executado, impresso, armazenado, distribuído, editado, ou gravado através do uso dos recursos computacionais.

3- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas.

4- Cada usuário apenas poderá utilizar a pasta \Meus Documentos ,S:\Setores a qual contém as sub-pastas da gerência onde trabalha e U:\Usuarios para uso restrito de documentos com limite de xx MB .

5- Acessos a dispositivos USB, mídias ópticas e magnéticas, pastas e sub-pastas não cobertas pelo perfil do usuário só serão permitidas após a liberação formal da GTI.

6- O usuário deve fazer manutenção periódica na sua pasta \Meus Documentos, pois a mesma tem espaço limitado e evita-se acúmulo de arquivos desnecessários.

7- O limite de espaço para a pasta \Meus Documentos é de 500 MB, caso o usuário ultrapasse o limite, o mesmo deverá salvar o excedente em DVD e ficará responsável pelo mesmo.

8- O CREA - AL não se responsabiliza pela utilização de equipamentos de informática particulares e não fornecerá assessórios, software ou suporte técnico. Danos físicos, roubo, perda de dados decorrentes de falha humana, ou pelo mau funcionamento do equipamento e/ou software dentro da instituição são responsabilidade do proprietário do equipamento.

9- Os equipamentos devem ser configurados, conforme a função a ser exercida, funcionalidades, serviços e protocolos desnecessários devem ser desativados.

5.6.2.3 Política de Uso de Senhas

1- As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.

2- Procedimentos para a criação de senhas
- Não utilize palavras que estão no dicionário (nacionais ou estrangeiros).
- Não utilize informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc.
- Não utilize senhas somente com dígitos ou com letras.
- O comprimento mínimo deve ser de oito caracteres.
- Misture caracteres maiúsculos e minúsculos.
- Misture números, letras e caracteres especiais.
- Inclua, pelo menos, um caractere especial.
- Utilize um método próprio para lembrar a senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma.
- Não anote sua senha em papel ou em outros meios de registro de fácil acesso.
- Não utilize o nome do usuário.
- Não utilize o primeiro nome, o nome do meio ou o sobrenome.
- Não utilize nomes de pessoas próximas, como da esposa (o), dos filhos, de amigos.
- Não utilize senhas com repetição do mesmo dígito ou da mesma letra.
- Não forneça sua senha para ninguém, por razão alguma.
- Utilize senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.
- Não use a mesma senha para finalidades profissionais e pessoais.
- Não inclua senha em nenhum processo automático de acesso.

3- Tempo de validade máxima de 42 dias, expirando em seguida.

4- As senhas serão bloqueadas após 5 tentativas sem sucesso, devendo o usuário contatar a administração da rede notificando-a sobre estas tentativas.

5.6.2.4 Política de Uso da Internet

1- É proibida a utilização dos recursos da internet para fins que não seja de trabalho para o CREA - AL.

1.1- É considerável falta grave acesso a conteúdos pornográficos, serviços de bate-papo, relacionamentos, programas de compartilhamento de arquivos, hacker, etc.

2- Somente navegação de sites é permitida. Casos específicos que exijam outros tipos de serviços de internet, tais como; FTP, IRC, VPN, etc., deverão ser solicitados diretamente à Gerência de Tecnologia da Informação.

3- Caso a Gerência Tecnologia da Informação julgue necessário poderá bloquear imediatamente arquivos ou domínios que comprometam o uso da banda ou perturbe o bom andamento dos trabalhos.

4- Evitar o fornecimento de dados pessoais ou da empresa em sites WWW, pois essas informações podem ser utilizadas para finalidades indevidas, como o envio de propaganda indesejada ou spam.

5- Haverá geração de relatórios dos sites acessados por usuário e caso necessário a prestação de contas sobre estes acessos.

6- É obrigatório o uso de antivírus, antispywere e firewall em todos os servidores, desktops e notebooks do CREA - AL, inclusive os de terceiros caso venham utilizar nossa rede, estes devem ter aprovação prévia da GTI antes do uso.

7- O uso de serviços de comércio eletrônico devem ter atenção especial para evitar atividades fraudulentas, os gerentes devem informar à GTI quais computadores irão utilizar este serviço para serem tomadas as devidas providências de controle.

5.6.2.5 Política de Uso de E-Mail

1- Os colaboradores só poderão usar a conta de e-mail *nome*@crea-al.org.br com o propósito de uso para empresa.

2- O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, freqüência ou tamanho das mensagens.

2.2- É proibido encaminhar ou repassar mensagens em cadeia tipos: propagandas, correntes religiosas, de ajuda, para ganhar dinheiro, apelativos para dar sorte, anúncios, informativos, propaganda política, etc.

2.2- O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los, se for solicitada a interrupção do envio a solicitação deve ser acatada e o envio não deve acontecer;

3- Caso a GTI julgue necessário haverá bloqueios do e-mail com arquivos anexos, destinatários e/ou domínios que comprometa o uso da banda ou perturbe o bom andamento dos trabalhos.

4- É obrigatória a manutenção da caixa de e-mail evitando o acúmulo de e-mails e arquivos inúteis.

- A cota máxima é de 10GB por conta.
- O tamanho máximo para anexos é de 25MB.

5- É obrigatória a utilização de assinatura nos e-mails, seguindo padrão do CREA - AL.

6- Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos.

6.1- Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não houver certeza absoluta que solicitou este e-mail.

6.2- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês.

7- Não é permitida má utilização da linguagem em respostas aos e-mails comerciais, tais como; abreviações e uso de gírias.

8- É proibido o tráfego através de e-mail de informações classificadas como nível 3 (Confidencial).

5.6.2.6 Política de Aquisição de Software

1- As aquisições de software devem ser analisadas e autorizadas previamente pela GTI.

2- A instalação e configuração dos softwares devem ser feitas pelos técnicos da GTI.

3- A guarda dos manuais e CDs dos softwares deve ficar na GTI.

5.6.2.7 Política de Computação Móvel e Trabalho Remoto

1- A permissão para acesso remoto deve ser fornecida mediante solicitação formal, a aprovação deve ser concedida pelo gerente da GTI. Deve-se verificar se o usuário deste serviço já assinou o DOC-GTI Termo de Confidencialidade e entregar uma Declaração de que está ciente das condições de segurança para uso de computação móvel e trabalho remoto.

2- Conexões de acessos remotos na rede interna serão efetuadas após confirmação do usuário.

5.6.2.8 Política de Recursos para Desenvolvimento, Testes e Produção

- Recursos de desenvolvimento, teste e produção devem ser separados a fim de reduzir os riscos de acessos e modificações não autorizadas aos sistemas.

5.6.2.9 Política de Desenvolvimento de Sistemas

- O desenvolvimento, manutenção e implantação de sistemas devem ser analisados, testados e autorizados previamente pela gerência da GTI.

- Deve-se prevenir a ocorrência de erros, perdas, modificações não autorizadas ou o mau uso de informações nos sistemas.

- Os sistemas devem ter formas de controle para validar as entradas e saídas de dados para desta forma garantir que os dados estão corretos e apropriados.

- O processamento interno deve ter checagens para detectar qualquer corrupção de informações por erros ou ações deliberadas.

5.6.2.10 Proteção Criptográfica

Deve ser utilizado o uso de criptografia e controles de chaves para garantir a confidencialidade, autenticidade e integridade dos arquivos.

5.6.2.11 Política de Monitoramento

- A utilização dos recursos de produção deve ser monitoradas e analisadas criticamente de forma regular a fim de sincronizar com as demandas de infra-estrutura necessárias para o desempenho requerido dos sistemas.

- Logs de todos os usuários, administradores de rede e operadores da GTI devem ser arquivados e analisados regularmente.

- O registro dos logs das falhas nos sistemas devem ser monitorados e analisados regularmente.

- As sincronizações dos relógios devem estar de acordo com o horário oficial de Maceió.

5.7 ATIVO – HARDWARE

5.7.1 Classificação

Hardware
Servidores
Desktops / Notebooks
Impressoras
Copiadoras
Scanners
Switchs

Tabela 15

5.7.2 Normas e Procedimentos de Segurança

5.7.2.1 Política de Utilização

1- Qualquer saída de equipamentos do CREA - AL será mediante a autorização da GTI.

2- O colaborador em hipótese alguma poderá usar os equipamentos dentro ou fora da instituição para uso particular

3- A responsabilidade pelos danos físicos aos equipamentos e periféricos fica a cargo do usuário do mesmo.

3.1- Não são permitidas tentativas de reparo dos equipamentos ou remoção de componentes, nem mesmo a alteração da disposição dos equipamentos;

3.2- Ao perceber qualquer problema com o equipamento comunicar à GTI.

5.7.2.2 Política de Manutenção

1- Só é permitida a abertura de equipamentos pelos técnicos da GTI, exceto nos casos para troca de cartuchos de impressoras.

2- Hardware enviado para manutenção externa deve ser inspecionado para que, caso haja informações internas ou confidenciais estas sejam removidas antes de o equipamento ser levado para assistência externa.

3- Itens de hardware danificados de forma permanente devem ser avaliados para se verificar se devem ser destruídos ou vendidos como sucata.

4- Hardware sobressalente deve estar disponível caso o equipamento e/ou serviços relacionados a ele sejam de criticidade alta.

- As demais regras e procedimentos aplicados a manutenção de hardware encontram-se no item 5.8.2.2.

5.7.2.3 Política de Uso de Impressoras

1- Ao enviar impressão certifique-se se já foi solicitada à impressão, para evitar re-envio e desta forma desperdício de papel e exposição desnecessária de informações.

2- Não é permitido deixar impressões erradas no ambiente de trabalho.

3- Se ocorreu erro na impressão:

3.1- E o papel pode ser reaproveitado (em branco) deve-se colocá-lo de volta na bandeja de impressão.

3.2- Caso houve impressão desnecessária e a informação for classificada como Pública, deve-se reaproveitar papel para rascunho ou enviá-lo para o setor gráfico.

3.3- Caso a Informação seja interna ou confidencial, descartá-lo seguindo os procedimentos da NQ/GTI-CSI-002.

4- As impressões devem ser feitas em formato rascunho, exceto os documentos formais e comercias.

5- Nunca deixar a bandeja esvaziar, desta forma evita-se acúmulo na fila de impressão, que causam impressões e exposições de informações desnecessárias e desperdício de papel, energia e tinta.

6- Os recursos de impressão e fotocópia são de uso exclusivo dos trabalhos relacionados ao setor ou atividades previamente autorizadas, não é permitido impressão de desenhos, cartazes ou cartões.

5.7.2.4 Política de Aquisição de Hardware

1- As aquisições de hardware devem ser analisadas e autorizadas previamente pela GTI.

2- A instalação e configuração dos equipamentos devem ser feitas pelos técnicos da GTI.

3- A guarda dos manuais e CDs dos equipamentos deve ficar na GTI.

4- O inventario de todo o conjunto de ativos de processamento deve ser registrado e mantido.

5.7.2.4 Política de Segurança para Notebooks e PDAs.

- A senha deve ser diferente da senha do sistema operacional ou aplicativos.

- Os equipamentos devem ser guardados em locais restritos dentro de armários ou gavetas com chave.

5.7.2.5 Política de Identificação do Hardware

- Todo hardware do CREA - AL deverá ter as seguintes identificações:
  - Física: Plaqueta do Patrimônio e Número de Série
  - Lógica: Nomenclatura padrão para identificação na rede de acordo com procedimentos das ROT/GTI-RED

5.8 ATIVO – AMBIENTE FÍSICO

5.8.1 Classificação

Ambiente	Descrição
Equipamentos de Comunicação	Centrais telefônicas, aparelhos de fax, etc.
Equipamentos Técnicos	Geradores, ar-condicionado, no-break.
Ambiente Físico	Mobília, acomodações, cofres, instalações elétricas, hidráulicas e telefônicas, salas, prédios, etc.

Tabela 16

5.8.2 Normas e Procedimentos de Segurança

5.8.2.1 Política de Acesso Físico

Ver item 5.5.2.1

5.8.2.2 Política de Segurança e Manutenção dos Equipamentos

1- Toda e qualquer instalação deve ser feita seguindo os procedimentos recomendados pelo fabricante e/ou normas específicas existentes.

2- Equipamentos instalados em áreas de acesso pouco restrito deverão dispor de segurança física, como armário, gaiola, ou equivalente, com trava mecânica e/ou eletrônica, chave ou outro dispositivo que permita barrar o acesso de pessoas não autorizadas.

3- Equipamentos instalados em áreas de acesso comum deverão estar presos a dispositivos de alarme antifurto e cabos com travas.

4- As instalações devem ser feitas de modo que permita o fácil acesso às equipes de manutenção.

5- As instalações devem garantir boa ventilação a seus componentes.

6- Não colocar material sobre os equipamentos de maneira que prejudique seu sistema de ventilação.

7- A manutenção dos equipamentos deverá ser feita de acordo com intervalos específicos do fabricante, se essas recomendações não forem conhecidas, procedimentos de manutenção devem ser elaborados e aplicados.

8- Somente profissionais autorizados poderão fazer manutenção nos equipamentos, ou seja, o próprio fabricante, empresas autorizadas por ele e/ou a equipe de manutenção do CREA.

9- Devem ser mantidos todos os registros de falhas suspeitas ou ocorridas em toda as manutenções preventivas e corretivas.

10- Equipamentos sobressalentes devem estar disponíveis para o caso de a criticidade do equipamento seja alta.

5.8.2.3 Política de Segurança Física das Instalações de Processamento

A segurança física das instalações de processamento tem como objetivo proteger edificações e equipamentos, prevenir perda, dano ou comprometimento dos ativos, manter a continuidade das atividades dos negócios e reduzir as ameaças que coloquem em risco o bom funcionamento dos sistemas. Desta forma as instalações de processamento devem ser em locais isolados, sem identificação e com acesso restrito.

1- A temperatura, umidade e ventilação das instalações que abrigam os servidores devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

2- As instalações elétricas devem seguir a norma NBR-5410 Instalações Elétricas de Baixa Tensão.

3- Os sistemas de proteção contra descargas atmosféricas e aterramento devem receber manutenção preventiva anual.

- O projeto, instalação e manutenção do sistema devem estar em conformidade com a norma NBR-5419-2000.

4- Todas as instalações centrais de processamento bem como qualquer área estratégica do CREA - AL devem estar ligadas a geradores.

- Todos os equipamentos que suportam atividades críticas devem usar no-break com autonomia considerável.
- Tanto os no-break como os geradores devem ter contrato de manutenção firmado para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante.

5- Todos os servidores e equipamentos de rede críticos devem ter fontes redundantes no modo *load sharing* tornando um *failover* imperceptível.

6- As salas de processamento devem possuir iluminação e interruptor elétrico de emergência.

7- A alimentação elétrica das salas deve ser independente, conectada diretamente a rede elétrica primária.

8- Devem-se tomar medidas de segurança ambiental para detectar:

- Incêndio
- Fumaça
- Poeira
- Vibração
- Umidade
- Água

Sensores destes fatores devem estar interligados e de forma que permitam ser monitorados remotamente e possuir disparo de alarmes.

5.8.2.4 Política de Cabeamento da Rede Computacional

1- O cabeamento deve ser preferencialmente subterrâneo e através de sistema de dutos exclusivos.

2- Os dutos de cabeamento devem possuir proteção anti-roedor (ver NBR 14773).

3- As rotas de cabeamento devem receber sinalização específica para evitar acidentes ou danos de terceiros.

4- As caixas de passagens devem ser mantidas adequadas ao uso e possuir identificação.

5- Todos os pontos de rede e switchs relacionados aos mesmos devem ser identificados, catalogados e atualizados sempre que necessário.

6- A instalação de cabeamento, tanto de cobre como de fibra ótica, deve seguir as recomendações das normas NBR 14565 e TIA/EIA 568-B.2-1.

5.8.2.5 Política de Segurança Física das Instalações de Telefonia

Da mesma forma que as instalações de processamentos os sistemas de telefonia requerem cuidados para garantir a continuidade de suas operações.

1- O acesso físico ao hardware do sistema de telefonia e aos terminais de configuração de sistema é restritivo aos técnicos da telefonia e ao pessoal da companhia provedora do serviço.

2- O sistema de telefonia deve estar em uma área segura com acesso altamente restrito.

3- A instalação de novos modems ou qualquer equipamento relacionado á central telefônica deve ser supervisionada pelo responsável pela telefonia.

4- O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos são de responsabilidade exclusiva da GINF

-Seguir demais condições compatíveis nos itens 5.8.2.3 e 5.8.2.4.

5.8.2.6 Política de Segurança dos Escritórios, Salas e Instalações

1- Os projetos de construção, de reforma e mobília devem garantir a prevenção do acesso físico não autorizado, danos, interferências e quaisquer outras ameaças as instalações e informações do CREA - AL, bem como garantir segurança dos pacientes, colaboradores e terceiros.

- Deve-se aplicar proteção adequada contra ameaças externas e do meio ambiente, como por exemplo: enchentes, terremotos, explosões, perturbações da ordem pública entre outras formas de desastres naturais ou causados pelo homem.

5.9 ATIVO - PESSOAS

5.9.1 Regra Geral dos Níveis de Acessos por Função

Bloco Administrativo	
Cargo	Nível de Acesso
Direção	Confidencial
Gerência	Confidencial
Coordenação	Interna
Supervisão	Interna
Assistentes, Auxiliares, e demais funções.	Interna

Tabela 18

5.9.2 Infrações, Penalidades e Responsabilidades

Os colaboradores são responsáveis pela guarda, zelo e bom uso dos ativos da instituição, dentro dos ativos de informação cabe a todos os colaboradores a proteção dos recursos tecnológicos e informações oriundas ou não destes recursos.

Todos os funcionários devem colaborar com o trabalho do Comitê SI. Supervisores, Coordenadores e Gerentes devem gerenciar o cumprimento da PSI por parte de seus subordinados, identificando os desvios praticados, adotando as medidas necessárias e registrando os incidentes junto ao Comitê SI

Todo e qualquer descumprimento das normas e procedimentos da Política de Segurança da Informação do CREA - AL é considerada falta disciplinar. As penalidades serão determinadas pela Ouvidoria de acordo com o capítulo X do PCCS, tendo como base o parecer de incidentes de segurança do Comitê SI o qual avalia a gravidade das infrações e atesta que houve a violação da política diante situações e atividades cometidas pelo colaborador, tais como: conduta em desacordo com a política, atividade ou falha no cumprimento da política que possa causar ou gerar riscos aos ativos da empresa e sua imagem perante aos clientes, atividades com finalidade de tirar proveito próprio dos ativos da empresa, negligência na proteção dos ativos sob sua responsabilidade, etc.

5.9.4 Normas e Procedimentos de Segurança

5.9.4.1 Política de Pré-admissão

Para todos os candidatos selecionados são pré-requisitos para sua admissão a análise de idoneidade pessoal e profissional, conforme parecer favorável nas pesquisas abaixo:

1- Verificação financeira junto a órgãos fiscalizadores (SERASA / SPC).

2- Verificação de registros criminais.

3- Verificação da exatidão do curriculum vitae.
- Confirmação das atividades acadêmicas e profissionais.
- Verificação das referências profissionais e pessoais.

5.9.4.2 Política de Admissão e Demissão de Funcionários, Temporários e Estagiários

1- O setor de RH deverá informar à GTI toda e qualquer movimentação de temporários e/ou estagiários e admissão/demissão de colaboradores, para que possam ter seus privilégios de acessos aos sistemas, informações e recursos devidamente liberados, revistos, modificados ou revogados.
- Transferência de colaboradores entre setores e mudança de função deve ser informada à GTI para adequar os sistemas ao novo perfil.

2- Cabe ao setor solicitante da contratação a comunicação à GTI sobre as rotinas que o novo contratado terá direito a acesso (DOC-GTI Cadastro de Usuários), no caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço à CREA - AL.

3- Nos casos de demissão ou término/cancelamento de serviços temporários ou estagiários o setor de RH deverá comunicar o fato o mais rapidamente possível à GTI para que os usuários sejam inativados dos sistemas e possíveis contas de usuários usados pelos mesmos que não podem ser excluídas tenham suas senhas redefinidas.

4- Cabe ao setor de RH dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação do CREA-AL (DOC-GTI Termo de Confidencialidade / DOC-GTI Cartilha de Segurança). Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

5- As descrições dos cargos devem conter as responsabilidades e papéis pela segurança da informação pertinentes a cada cargo, tais como:
- As características de responsabilidade, decisão e iniciativa.
- Detalhamento das qualificações técnicas necessárias.
- Descrição sumária das tarefas inerentes à função.
- As necessidades de acesso a informações internas e confidenciais.
- O nível de segurança do setor onde a função é exercida

6- Dependendo do cargo, após o término do contrato de trabalho, as responsabilidades sobre a segurança das informações devem continuar por um tempo definido.

7- Após o término dos contratos, funcionários, fornecedores e terceiros devem devolver todos os ativos que estejam em sua posse (documentos, crachás, chaves, ferramentas, etc.) bem como documentar e transferir para a organização qualquer procedimento ou detalhe técnico essencial para a continuidade dos serviços.

- O colaborador firmará antes do desligamento, declaração de que não possui qualquer tipo de pendência junto a CREA - AL, devendo ao RH checar junto às gerências a veracidade das informações.
- Deverá ser realizada entrevista de desligamento para orientar o colaborador sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência na CREA - AL.
- Os colaboradores demitidos ou demissionários não poderão ter acesso aos ativos de informação.

5.9.4.3 Política de Acompanhamento de Desempenho

- Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos colaboradores, a ser realizado pela chefia imediata dos mesmos.
- Os comportamentos incompatíveis, ou que possam gerar comprometimentos a segurança, deverão ser averiguados e comunicados a chefia imediata e/ou Comitê SI.
- Deverão ser motivo de registro os atos, atitudes e comportamentos positivos ou negativos relevantes.

5.9.4.4 Política de Contratação de Fornecedores

- No contrato deve estar claramente especificado a responsabilidade e deveres de ambas as partes para a segurança da informação.

- Em anexo ao contrato deve estar assinado o Termo de Responsabilidade para Fornecedores, a ser redigido pela Gerência envolvida com o serviço/produto fornecido.

5.9.3.4 Política de Conscientização, educação e treinamento

O principal agente da segurança da informação são as pessoas, desta forma é fundamental para o sucesso da política o treinamento e atualizações constantes.

- Todos os colaboradores devem receber treinamento sobre a Política de Segurança da Informação e suas posteriores atualizações.
- Todo novo colaborador admitido, antes do início de suas funções deve passar pelo treinamento de segurança da informação e assinar o DOC/GTI-CSI Termo de Confidencialidade.

- As formação das turmas para treinamento deve ser de acordo com as funções.

- Após o treinamento o colaborador deve estar apto a reconhecer todas as ameaças possíveis à segurança dos ativos de informação no decorrer de suas funções, bem como estar ciente da obrigatoriedade e dos meios para relatar estes incidentes ao CSI.

- As chefias imediatas são co-atuantes no treinamento e conscientização, devem assegurar que todos os colaboradores tenham conhecimento e compreensão das normas e procedimentos de segurança.

5.10 ATIVOS - SERVIÇOS

5.10.1 Classificação dos Serviços

Gerência	Serviços
Infraestrutura	Manutenção Predial, Elétrica, Hidráulica, Telefônica e Eletrônica.
	Serviços Terceirizados
Tecnologia da Informação	Suporte Técnico e Manutenção de Sistemas
	Manutenção de Hardware e Rede
	Procedimentos de Backup
	Serviços Terceirizados

Tabela 19

5.10.2 Requisitos para execução de serviços

- Abertura de Ordem de Serviço.

- Avaliação prévia da OS para identificar e gerenciar os impactos do serviço nos processos operacionais do CREA e riscos de segurança aos ativos de informação e clientes.

- Estar em conformidade com as normas ABNT de segurança de cada serviço envolvido.

5.10.3 Normas e Procedimentos de Segurança

5.10.3.1 Política de Manutenção Predial, Elétrica, Hidráulica, Telefônica, Eletrônica

Os procedimentos de segurança na aplicação destes serviços devem estar de acordo com as Normas do SESMET (nr - 04 - sesmet - serviços especializados em engenharia de segurança e medicina do trabalho) e Rotinas Operacionais da GINF.

(Ver também item 5.8.2.3, 5.8.2.5 e 5.8.2.6)

5.10.3.2 Suporte Técnico e Manutenção de Sistemas

- Modificações e mudanças de versões nos sistemas devem ser previamente analisadas e estritamente controladas.
- Qualquer implementação e atualização deve ser feita no ambiente de teste.

- As vulnerabilidades técnicas dos sistemas devem ser monitoradas, bem como deve-se tomar as medidas apropriadas para lidar com os riscos associados.

As atividades de Suporte e Manutenção devem estar de acordo com as rotinas operacionais da GTI (ROT/GTI-SUP, ROT/GTI-RED, ROT/GTI-DES e ROT/GTI-BCO)
(ver também item 5.6.2.9)

5.10.3.3 Política de Manutenção de Hardware e Rede

Seguir as ROT/GTI-SUP de manutenções de hardware.
Ver também itens os 5.7.2.2, 5.8.2.2 e 5.8.2.4 desta política.

5.10.3.4 Política de Cópias de Segurança (backup)

1- Backup

1.1- Abrangência

É de responsabilidade da Gerência da Tecnologia da Informação a realização de backup e armazenamento dos seguintes sistemas, arquivos e configurações:

- Sistemas
  - SITAC
  - Folha de Pagamento
  - Implanta
  - Almoxarifado
  - Agenda
- Compartilhamentos
  - \\srvfile-01\Desktops
  - \\ srvfile-01\Setores
  - \\ srvfile-01\Usuários
  - \\ srvfile-01\Logs
  - \\ srvfile-01\Instaladores
  - \\ srvfile-01\Suporte
  - \\ srvfile-01\Wallpaper
- Sistema Operacional [Estado de Sistema]
  - Windows 2003 Server
- Firewall/Proxy
  - Microsoft Forefront TMG

1.2- Freqüência

- Deve ser feito pelo menos um backup completo por semana.
- Os bancos de dados dos sistemas e os aplicativos dos mesmos devem ter backup on line nas réplicas dos seus servidores (standby).

1.3- Validação

- O backup completo deve ser validado semanalmente em ambiente e rede física separados do ambiente de produção.

1.4 Mídias

- Deverá haver duas cópias do backup em mídias de formato diferentes.

2- Backups sob responsabilidade do usuário

- Qualquer outro programa, arquivo ou configuração que não se enquadre no item 1 tem o seu backup, guarda e armazenamento sob responsabilidade do setor onde é executado, ou seja, devem ser feito pelos usuários.
- Consultar a GTI no caso de dúvidas para a execução destes backups.

3- Segurança física dos backups

- As mídias contendo os backups devem ser armazenadas em cofres especiais resistentes a incêndio, umidade, interferências eletromagnéticas, poeira, fumaça e vandalismo.
- Apenas pessoal autorizado poderá ter acesso às mídias de backup e aos aplicativos que efetuam os backups.

5.10.3.5 Serviços Terceirizados

1- A gerência responsável pelo contrato de serviço deve garantir que os controles de segurança, as definições do serviço e os níveis de entrega incluídos no contrato de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.

2- Os serviços, relatórios e registros fornecidos pelos terceirizados devem ser regularmente monitorados a analisados criticamente. Auditorias devem ser executadas regularmente.

3- As mudanças nos serviços terceirizados devem ser analisadas previamente para a manutenção e melhoria dos procedimentos e controles existentes levando-se me conta a criticidade dos sistemas e processos de negócio envolvidos na mudança.

4- O desenvolvimento terceirizado de software deve ser supervisionado pela Coordenação de Análise e Desenvolvimento, sendo que esta deve entregar a Gerência de TI relatório mensal sobre a supervisão.

5.11 GERENCIAMENTO DE INCIDENTES

O Comitê SI, gerencia e monitora os incidentes de segurança com colaboração dos proprietários de informação de cada setor.

Deve-se assegurar que as fragilidades e eventos de segurança dos ativos de informação sejam comunicados ao Comitê SI, permitindo desta forma a tomada de ação corretiva em tempo hábil.

- Os eventos de segurança da informação devem ser relatados o mais rapidamente possível.

- Os colaboradores, fornecedores e terceiros devem ser orientados a registrar e notificar qualquer observação ou suspeita de ameaças a segurança.

5.12 GESTÂO DE CONTINUIDADE

O Comitê SI, gerencia os aspectos da continuidade do negócio relativos à segurança da informação, tem como finalidade não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada, se for o caso.

5.12.1 Considerações Gerais

- Todos os aspectos de continuidade devem ser desenvolvidos e implementados.

- Todos os proprietários da informação devem avaliar regularmente seus processos operacionais referentes a segurança da informação, os processos devem atender aos requisitos de segurança desta política.

- Deve-se identificar e avaliar os eventos que podem causar interrupções aos processos operacionais, as probabilidades de ocorrências e as conseqüências para a segurança da informação.

- Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e continuidade.

5.12.2 Plano de Contingência

Ver NQ-GTI-CSI-003

5.13 CONSIDERAÇÕES FINAIS

As normas e procedimentos desta política devem ser interpretados de forma que todas as suas determinações sejam obrigatórias e cogentes.

Este documento deve ser revisado a cada 6 meses.

6. RESPONSABILIDADES / AUTORIDADES

Gerência de Tecnologia da Informação / Comitê de Segurança da Informação - CSI

7. IDENTIFICAÇÃO DE REGISTROS

REGISTRO	NQ/GTI-CSI-001 Política de Segurança da Informação
COLETA	GTI
INDEXAÇÃO	Por revisão.
ARQUIVAMENTO	Em pastas.
ACESSO	Restrito.
LOCAL DE GUARDA	GTI
TEMPO DE GUARDA	No mínimo 2 anos.

DISPOSIÇÃO	Descartar em máquina de fragmentação.