CONSIDERANDO a missão institucional desta Controladoria-Geral de Disciplina, no tocante à prevenção e à repressão aos desvios de conduta de integrantes dos órgãos de Segurança Pública e Sistema Penitenciário, contribuindo para a melhoria dos serviços prestados à sociedade;

CONSIDERANDO que um dos eixos estratégicos deste Órgão busca o atendimento, no campo da inteligência, daquelas demandas de maior potencial ofensivo (delitos ligados a grupos de extermínio/homicídios/corrupção/sequestro/extorsão etc), que exigirão investigações mais abrangentes e profundas a serem capitaneadas pela Delegacia de Assuntos Internos – DAI, em parceria com o Ministério Público, Polícia Federal e outras entidades, de forma a reprimir institucionalmente os desvios de conduta de maior complexidade;

CONSIDERANDO que a Delegacia de Assuntos Internos, conforme disposto no § 1º do art. 1º do Decreto n.º 30.841, de 07.03.2012, é vinculada funcionalmente à Controladoria-Geral de Disciplina;

CONSIDERANDO a existência de inquéritos policiais em trâmite na Delegacia de Assuntos Internos que também são objetos de investigações preliminares a cargo da Célula de Investigação Preliminar/GTAC; CONSIDERANDO ainda a necessidade de otimizar os trabalhos desenvolvidos pela Célula de Investigação Preliminar/GTAC, em homenagem aos princípios da celeridade e economia processual.

RESOLVE:

I - DETERMINAR que as investigações preliminares que também são objetos de inquéritos policiais em trâmite na Delegacia de Assuntos Internos sejam distribuídas aos delegados encarregados pelos respectivos inquéritos, para que após a conclusão do procedimento policial, seja anexada cópia integral do feito aos autos da investigação preliminar e emissão de parecer, visando a adoção de medidas no âmbito administrativo disciplinar;

II - DETERMINAR que a Delegacia de Assuntos Internos apresente, no prazo de 10 dias, a relação dos dados dos inquéritos policiais daquela Especializada (número, nomes de vítimas e indiciados) a este Gabinete, para que seja informado pela CEPROD o número/localização das investigações preliminares junto ao SISPROC, objetivando a redistribuição desses procedimentos pela CEINP aos delegados da DAI, caso ainda não tenha sido providenciada tal

redistribuição;

III - DETERMINAR ainda que a Delegacia de Assuntos Internos comunique à CGD qualquer instauração ou recebimento de inquérito policial para que seja procedido o registro junto ao SISPROC, visando a apuração no âmbito administrativo disciplinar. Os casos omissos serão analisados e decididos pelo Controlador-Geral de Disciplina.

REGISTRE-SE E PUBLIQUE-SE.

CONTROLADORIA GERAL DE DISCIPLINA DOS ÓRGÃOS DE SEGURANÇA PÚBLICA E SISTEMA PENITENCIÁRIO, em Fortaleza, 03 de julho de 2018.

Rodrigo Bona Carneiro

CONTROLADOR GERAL DE DISCIPLINA DOS ÓRGÃOS DE SEGURANÇA PÚBLICA E SISTEMA PENITENCIÁRIO, RESPONDENDO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

Este documento tem por finalidade estabelecer as diretrizes de segurança da Informação que deverão ser adotadas pela Controladoria Geral de Disciplina dos Órgãos de Segurança Pública e Sistema Penitenciário – CGD. Tais diretrizes fundamentarão as normas e procedimentos de segurança a serem elaborados e implementados por parte da CGD seguindo determinação do Decreto nº29.227 de 13 de março de 2008, que institui a Política de Segurança da Informação dos ambientes de Tecnologia da Informação e Comunicação – TIC do Governo do Estado do Ceará.

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da CGD para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da CGD.

A Política de Segurança da Informação – PSI da CGD tem os seguintes objetivos específicos:

a) Definir o escopo da Segurança da Informação;

b) Orientar as ações de segurança da Informação com a finalidade de reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação (físico e virtual) e recursos;

c) Permitir a adoção de soluções de segurança integradas;

d) Servir de referência para auditoria, apuração e avaliação de responsabilidades.

As regras estabelecidas neste documento estendem-se a todos os que fazem parte da CGD, tais como empregados, servidores, cargos em comissão, terceirizados, estagiários, prestadores de serviços e os que, de alguma forma, fazem uso dos recursos computacionais.

1.1 TERMINOLOGIA

As regras e diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes.

1.2 REFERÊNCIA

-Constituição Federal;

-Lei nº12.965 de 23 de abril de 2014;

-Decreto nº29.227 de 13 de março de 2008, do Governo do Estado do Ceará;

-Norma ABNT NBR ISO/IEC 27001: 2006;

-Norma ABNT NBR ISO/IEC 27002: 2005.

1.3 CONCEITOS E DEFINIÇÕES

Para efeitos desta Política, considera-se:

-**PSI:** Política de Segurança da Informação;

-**Sistema de Informação**: É um conjunto organizado de elementos, podendo ser pessoas, dados, atividades ou recursos materiais em geral. Estes elementos interagem entre si para processar informação e divulgá- la de forma adequada em função dos objetivos de uma organização;

-**Informação:** Agrupamento de dados que contenham algum significado;

-Internet: É o sistema constituído de conjunto de protocolos lógicos estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes (Lei Nº12.965 de 23 abril de 2014.);

-Ativo: Qualquer coisa que tenha valor para a organização [ISO/ IEC; 13335-1:2004];

-Usuário: Servidores ou colaboradores que tem acesso autorizado aos sistemas de informação;

-Códigos Maliciosos ou Agressivos: Qualquer código adicionado, modificado ou removido de um Sistema, com a intenção de causar dano ou modificar o funcionamento correto desse Sistema, como por exemplo, vírus eletrônico;

-Vulnerabilidade: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. [ABNT NBR ISO/IEC 27002:2005];

-Risco: É a chance (probabilidade) de uma ameaça se transformar em realidade, causando problema à organização (FONTES 2000);

-Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. [ISO/IEC 13335- 1:2004];

-Disponibilidade: Propriedade de estar acessível sob demanda por uma entidade autorizada;

-Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

-Integridade: É a "propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental" (IN01 GSIPR, 2008);

-Autenticidade: É a propriedade de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, Órgão, entidade ou sistema;

-Vírus: É um código malicioso;

-Byte: É a unidade de 08 Bits;

-Hardware: É a parte física do computador;

-Software: É uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de um dado/informação ou acontecimento, são os programas;

-SMTP: É um protocolo que permite transferir o correio de um servidor a outro em conexão ponto a ponto;

-Spam: É o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

-Hacker: um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores;

-Programas P2P: Programas que fazem troca de arquivos em uma rede ponto a ponto;

-**Download**: significa transferir (baixar) um ou mais arquivos de um servidor remoto para um computador local;

-Backup: Cópia de segurança;

-Dispositivo móvel: é qualquer equipamento que possa ser transportado e utilizado em ambiente externo aos limites físicos da organização.

DA CLASSIFICAÇÃO DAS INFORMAÇÕES

As classificações abaixo se enquadram como exceções garantidas pela Lei Estadual nº15.175, que institui o acesso à informação pública.

Tipo de Documento / Informação Classificada	Grau de Sigilo	Prazo de Sigilo	Fundamento Legal
Autos dos Procedimentos de Investigação Preliminar de Denúncias de Desvio de Conduta	RESERVADO	Investigações em andamento ou prazo legal de 5 (cinco) anos, na forma do Art. 23, §1º, III da Lei 15.175/2012	Art. 22, VIII da Lei 15.175/2012
Autos de Processos de Sindicância	RESERVADO	Sindicância em andamento ou prazo legal de 5 (cinco) anos, na forma do Art. 23, §1º, III da Lei 15.175/2012	Art. 22, VIII da Lei 15.175/2012
Autos de Processos Administrativos Disciplinares - PAD	RESERVADO	Processos Administrativos Disciplinares em andamento ou prazo legal de 5 (cinco) anos, na forma do Art. 23, §1º, III da Lei 15.175/2012	Art. 22, VIII da Lei 15.175/2012
Autos de Processos de Conselhos de Disciplina - CD	RESERVADO	Processo de Conselho de Disciplina em andamento ou prazo legal de 5 (cinco) anos, na forma do Art. 23, §1º, III da Lei 15.175/2012	Art. 22, VIII da Lei 15.175/2012
Autos de Processos de Conselho de Justificação - CJ	RESERVADO	Processo de Conselho de Justificação em andamento ou prazo legal de 5 (cinco) anos, na forma do Art. 23, §1º, III da Lei 15.175/2012	Art. 22, VIII da Lei 15.175/2012
Autos de Inquéritos Policiais - IP	RESERVADO	Inquéritos Policiais em andamento ou prazo legal de 5 (cinco) anos, na forma do Art. 23, §1º, III da Lei 15.175/2012	Art. 22, VIII da Lei 15.175/2012
Documentos produzidos pela Coordenadoria de Inteligência	SECRETO	Prazo legal de 15 (quinze) anos, na forma do Art. 23, §1º, II da Lei 15.715/2012	Art. 22, VIII da Lei 15.175/2012

DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO DA CGD

O Comitê de Segurança da Informação da CGD tem a atribuição de divulgar e estabelecer os procedimentos de segurança, assim como se reunir periodicamente, ou a qualquer momento, com o objetivo de manter a segurança da informação em todas as áreas da Organização. O Comitê será presidido pelo Controlador Geral de Disciplina e em seus afastamentos ou impedimentos legais pelo Controlador Geral Adjunto de Disciplina ou quem delegar.

Os demais membros do Comitê, em seus afastamentos ou impedimentos legais, serão representados pelos seus respectivos substitutos legais.

1.4 COMPOSIÇÃO DO COMITÊ

I – Controlador Geral de Disciplina;

II – Controlador Geral Adjunto de Disciplina;

III – Secretária Executiva de Disciplina;

IV – Coordenadora de Disciplina Civil

V – Coordenador de Disciplina Militar;

VI – Coordenador da Assessoria Jurídica;

VII – Coordenadora do Grupo Tático de Atividade Correcional;

VIII – Coordenador(a) de Inteligência;

IX – Coordenadora Administrativo-Financeira;

X – Coordenadora da Assessoria de Desenvolvimento Institucional;

XI – Orientador da Célula de Tecnologia da Informação e Comunicação;

XII – Orientadora da Célula de Gestão de Pessoas;

XIII – Orientador da Célula de Registro e Controle de Procedimentos Disciplinares.

1.5 DA COMPETÊNCIA DO COMITÊ

I – assessorar na implementação das ações de segurança da informação da Controladoria Geral Disciplina;

II – elaborar e submeter ao Controlador Geral de Disciplina, propostas de normas e políticas de uso dos recursos de informação, tais como:

- **a)** classificação das informações;
- **b)** gerenciamento de identidade e controle de acesso lógico;
- **c)** controle de acesso físico;
- **d)** controle de acesso à Internet;
- **e)** utilização do correio eletrônico;
- **f)** utilização de equipamentos de tecnologia da informação;
- **g)** utilização de programas e aplicativos;
- **h)** utilização de armazenamento lógico;
- **i)** monitoramento e auditoria de recursos tecnológicos;
- **j)** contingência e continuidade dos serviços de tecnologia da informação.

III – rever periodicamente a Política de Segurança da Informação (PSI);

IV – dirimir dúvidas e deliberar sobre questões não contempladas na PSI;

V – propor e acompanhar planos de ação para aplicação da PSI, assim como campanhas de conscientização dos usuários;

VI – receber e analisar as comunicações de descumprimento das normas referentes à PSI desta CGD, apresentando parecer à autoridade/ órgão competente a sua apreciação;

VII – constituir grupos de trabalho para tratar de temas específicos.

DAS CONTAS E SENHAS DE USUÁRIOS

As contas de usuários contêm as credenciais que identificam um usuário. Elas permitem que um usuário efetue logon em um domínio e tenha acesso aos recursos disponíveis nesse domínio. Permitem também que um usuário efetue logon localmente e tenha acesso aos recursos de um computador.

As senhas são de caráter sigiloso tendo como regra para a sua composição:

-Mínimo de caracteres maiúsculos;

-Mínimo de caracteres minúsculos;

-Mínimo de numéricos;

-Mínimo de caracteres especiais;

Exemplo: Rfef3454@

1.6 Após solicitação, por meio de formulário específico, assinado pelo chefe imediato do usuário e aprovado pelo Coordenador, ficará a cargo da CETIC a criação de contas de usuários com acesso aos sistemas da CGD;

1.7 É de responsabilidade de cada usuário o sigilo de sua senha, não compartilhada e que deverá ser trocada pelo usuário no primeiro acesso;

1.8 O usuário é responsável pelos acessos aos serviços realizados pela sua conta, o mau uso de uma conta de acesso aos serviços por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;

1.9 A CETIC bloqueará temporariamente as contas de servidores e colaboradores (exceto e-mail) de férias e licença, e excluirá todas as contas dos que perderem o vínculo funcional com a CGD, de acordo com informação prestada pela Célula de Gestão de Pessoas.

DO USO DO EMAIL ELETRÔNICO

1.10 O e-mail institucional, de uso restrito para as atividades relacionadas ao desempenho das funções dos servidores e colaboradores, é considerado o meio formal e obrigatório de comunicação eletrônica. para fins legais, a CGD se reserva ao direito de realizar auditoria nas caixas postais do email institucional;

1.11 É recomendado o acesso diário ao e-mail institucional sob pena de bloqueio por inatividade após decorrido o prazo de 08 (oito) dias, cujo desbloqueio só ocorrerá mediante justificativa ao chefe imediato;

1.12 O tamanho das caixas postais deverá ser no máximo 150 MBytes para secretários, coordenadores e orientadores, e para os demais usuários 50 MBytes;

1.13 O usuário não deverá enviar, armazenar e manusear material que caracterize a divulgação incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente norma, lesivos aos direitos e interesses do órgão ou de terceiros, ou que de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

1.14 O usuário não deverá enviar, armazenar e manusear mensagens que não sejam de conteúdo

1.15 O uso da conta de correio eletrônico institucional será de responsabilidade de seu titular, sujeitando-se às penalidades cabíveis em caso de desvio de finalidade.

DO ACESSO À INTERNET

Internet é um sistema global de redes de computadores interligadas que utilizam o conjunto de protocolos padrão da internet (TCP/IP) para servir vários bilhões de usuários no mundo inteiro. É uma rede de várias outras redes, que consiste de milhões de empresas privadas, públicas, acadêmicas e de governo, com alcance local e global e que está ligada por uma ampla variedade de tecnologias de rede eletrônica, sem fio e ópticas.

1.16 A internet provida pela CGD deve ser utilizada no estrito interesse institucional;

1.17 O acesso à internet deve ser monitorado por meio de ferramentas próprias, podendo ser auditados quando necessário;

1.18 É expressamente proibido o acesso à internet com o fim de violar leis e regras brasileiras ou de qualquer outro país;

1.19 Somente usuários autorizados a falar, analisar ou publicar documentos em nome da Controladoria Geral de Disciplina poderão fazê-los em comunicações eletrônicas;

1.20 Não é permitido o uso da internet provida pela CGD para acessar sites que contenham material de incentivo a violência, propaganda política partidária com o fim de divulgação ou autopromoção pessoal, racismo, terrorismo, hacker, pornografia, pedofilia, dentre outros do gênero, além dos sites de conversão (bate-

-papo), proxy; jogos, programas que implementam P2P, a exemplo do Kazaa, Emule, Net-Meeting, Napster, Groove, ICQ, Morpheus, facebook e afins, exceto quando necessário aos procedimentos investigatórios;

1.21 É expressamente proibido download de arquivos que não sejam de interesse institucional;

1.22 A disseminação de vírus ou qualquer outro tipo de código malicioso é inaceitável, cabendo à CETIC a identificação da máquina disseminadora e ao GTAC, com o auxílio da CETIC, a identificação do responsável por tal prática visando as medidas administrativas decorrentes.

1.23. É dever do usuário no acesso à Internet:

1.23.1 Observar a finalidade institucional e o que preceitua a presente norma de controle;

1.23.2 Certificar-se (de) que a conexão é segura quando tiver que preencher qualquer formulário ou enviar informações;

1.23.3 Desconectar-se imediatamente de um site que contenha acesso restrito, mesmo que tenha sido aceito pelos sistemas encarregados de barrá-lo;

1.24 É de responsabilidade do administrador da Internet:

1.24.1 Implantar apenas um ponto de acesso para monitoramento da internet;

1.24.2 Adotar mecanismos de criptografia/codificação para transferência de informações sensíveis pela internet;

1.24.3 Fornecer, quando solicitado pela direção, relatório de acessos dos usuários.

DO USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho abrangem todos os computadores, notebooks, tablets ou qualquer outro equipamento eletrônico, tombado como patrimônio público pertencente ao acervo desta CGD ou a serviço dela.

1.25 O papel de parede das estações de trabalho deve seguir uma(a) padronização do Governo do Estado do Ceará;

1.26 As estações de trabalho devem ser utilizadas estritamente dentro da CGD, salvo quando a necessidade do serviço público exigir o contrário.

1.27 As estações servidoras, computadores e notebooks devem estar protegidos com software de detecção e reparo contra software/código malicioso, com atualização sistemática;

1.28 O direito de administrar as estações de trabalho é privativo da CETIC;

1.29 O usuário é responsável por sua estação de trabalho, inclusive o backup de seus arquivos pessoais;

1.30 Não é permitida a instalação de software e arquivos que não sejam de interesse da CGD;

1.31 A CETIC, quando necessário, realizará auditorias nas estações de trabalho visando detectar instalação indevida de softwares;

1.32 Todas as estações de trabalho devem estar configuradas para ficar bloqueadas quando permanecerem inativas por 5 minutos, sendo necessário para o desbloqueio o login e senha do usuário;

1.33 O usuário não deve beber, comer ou fumar próximo as estações de trabalho;

1.34 Somente os técnicos (da) CETIC estão autorizados a realizar manutenções físicas e lógicas nas estações de trabalho;

1.35 Caso seja necessária a formatação do disco de uma estação de trabalho, o usuário deve assinar um termo autorizando a área de TI a realizar a referida formatação, responsabilizando-se pelo backup dos dados armazenados;

1.36 Os equipamentos devem estar instalados em áreas protegidas contra acessos indesejados;

1.37 Deverá ser instalado sistema de no-break com um gerador de energia próprio capaz de alimentar os equipamentos nos locais considerados sensíveis;

1.38 Arquivos com conteúdo importante, cuja perda represente prejuízo para a CGD devem ter cópia de segurança mantida em computador alternativo ou em um servidor, visando backup de rotina;

DO USO DE DISPOSITIVOS MÓVEIS

1.39 Os usuários de dispositivos móveis tais como: tablets, celulares e outros, fica proibido a gravação e reprodução de fotos e vídeos das informações contidas na tabela de classificação das informações da CGD. Se comprovada a infração, deverá ser retido o aparelho para que se proceda a exclusão dos arquivos e posteriormente entregue ao seu proprietário;

1.40 É proibida a gravação de som referentes a assuntos de caráter sigiloso, bem como outros expressos na tabela de classificação das informações da CGD, por qualquer dispositivo móvel que não seja corporativo;

1.41 Os Dispositivos móveis corporativos deverão ser configurados com senhas de bloqueio de acesso;

1.42 Deverão ser instalados nos dispositivos móveis corporativos, softwares de segurança para proteção de vírus, malware e outras pragas virtuais;

1.43 A perda, extravio, furto ou roubo de dispositivo corporativo, deve ser realizado um boletim de ocorrência e enviado cópia para a Secretaria Executiva, como forma de proceder os bloqueios necessários;

DO CONTROLE DE BACKUP

1.44 As mídias que fazem parte dos Processos Disciplinares devem ter cópia armazenada nos servidores da CGD;

1.45 O armazenamento das mídias de backup deve ser realizado em localidade diferente de onde estão armazenados os equipamentos geradores da informação;

1.46 Caberá a CETIC a responsabilidade pela integridade dos backups realizados no servidor destinado para esse fim;

1.47 A CETIC realizará BACKUP diariamente, armazenando-o em locais externos, se possível;

1.48 Os arquivos pessoais contidos nos computadores da CGD são de inteira responsabilidade do usuário que os armazenou;

1.49 As pastas compartilhadas armazenadas nos servidores serão de responsabilidade da CETIC.

DAS ATRIBUIÇÕES DA CÉLULA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CETIC)

1.50 Criar e manter as contas dos usuários, sistemas e serviços;

1.51 Adotar mecanismos para forçar o usuário a trocar a senha no primeiro acesso;

1.52 Instruir os usuários na criação de senhas e a sua importância na segurança da informação;

1.53 Adotar mecanismos de segurança de acesso de usuários, bloqueando a senha após 05 (cinco) tentativas inválidas;

1.54 Propor diretrizes, normas e Procedimentos de Segurança da Informação;

1.55 Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança da informação;

1.56 Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança da informação;

1.57 Comunicar ao Controlador Geral de Disciplina as ocorrências e incidentes de segurança da informação, na forma de relatório detalhado e circunstanciado;

1.58 Homologar e autorizar o uso de sistemas e dispositivos de processamento de informações nas dependências da CGD;

1.59 Verificar periodicamente a conta postmaster para detectar eventuais problemas que possam ocorrer no servidor e na entrega de e-mail dos usuários;

1.60 Criar contas "security" e "abuse" nos servidores de domínio;

1.61 Implementar o papel de moderador nas listas, como objetivo de evitar spans;

1.62 Configurar o servidor de correio para autorizar o recebimento do Email somente após a autenticação do Usuário, utilizando configurações do tipo "smtp auth", "smtp after pop", etc;

1.63 Implementar medidas para filtragem de spam, vírus e e-mails indesejados (correntes, mensagens pornográficas, propaganda, etc.) no sistema de correio eletrônico;

1.64 Monitorar o funcionamento do servidor de correio eletrônico quanto ao número de conexões, mensagens enviadas e recebidas, mensagens bloqueadas, banda consumida na rede, etc;

1.65 Suspender, a qualquer tempo, o acesso do usuário a recursos computacionais quando evidenciado riscos à segurança da informação, com anuência da Direção Superior.

DAS RESPONSABILIDADES DA CHEFIA IMEDIATA

1.66 Disseminar a Política de Segurança da Informação;

1.67 Solicitar a disponibilidade ou cancelamento dos recursos de informática necessários aos seus subordinados para o bom desempenho da função;

1.68 Estabelecer os procedimentos adequados para montagem do plano de contingência adequado para os elementos que impactam diretamente no ambiente de Tecnologia da Informação e Comunicação (TIC) da Controladoria Geral de Disciplina, garantindo a continuidade dos serviços quando houver algum tipo de interrupção nos ativos considerados críticos.

DAS MEDIDAS RESTRITIVAS

1.69 Bloqueio de acesso para averiguação;

1.70 Processos administrativos, criminais e cíveis, sem prejuízo das penalidades previstas em lei.

Fortaleza, 16 de dezembro de 2014.

Frederico Sérgio Lacerda Malta
CONTROLADOR GERAL DE DISCIPLINA DOS ÓRGÃOS DE SEGURANÇA PÚBLICA E SISTEMA PENITENCIÁRIO, RESPONDENDO