



ESTADO DE GOIÁS  
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA

Portaria 205/2018 - SSP

*Dispõe sobre os procedimentos de backup do software CODIS e as políticas de segurança do Banco de Perfis Genéticos da Superintendência de Polícia Técnico-Científica, no âmbito da Secretaria de Segurança Pública do Estado de Goiás.*

O Secretário de Estado da Segurança Pública de Goiás no uso de suas atribuições legais e usando da competência que lhe confere o Decreto nº 8.934, de 06 de abril de 2017 e o Decreto de 14 de fevereiro de 2018 e tendo em vista o que consta do Processo nº 201800016007758;

RESOLVE:

Art. 1º Definir o Campo de Aplicação dos Administradores do Banco de Perfis Genéticos da SPTC/GO, equipe de Tecnologia da Informação da Gerência de Informática e Telecomunicações da SSPGO (GIT/SSPGO) com permissão para dar suporte no servidor e no sistema CODIS.

Art. 2º Explanar sobre as Definições, Siglas e Abreviaturas:

§ 1º CODIS: software desenvolvido pelo FBI (*Federal Bureau of Investigation*) e significa *Combined DNA Index System* (Sistema de índice combinado de DNA). CODIS liga evidências de DNA obtidas a partir de cenas de crime, identificando criminosos em série e também compara a evidência da cena do crime com os perfis de DNA obtidos de criminosos condenados, fornecendo assim aos investigadores a identidade do autor do crime. Além disso, o CODIS contém perfis de parentes de pessoas desaparecidas, restos humanos não identificados. Existem três níveis do CODIS no Brasil: o sistema de índice de DNA local, usado por laboratórios individuais localizados nos estados, Distrito Federal e Polícia Federal e o sistema de índice de DNA nacional administrado pela Polícia Federal como o banco de dados de DNA do país, contendo todos os perfis de DNA carregados pelos laboratórios participantes da Rede Integrada de Banco de Perfis Genéticos (estados, Distrito Federal e Polícia Federal).

§ 2º Administrador do BPG/SPTC-GO: Perito Criminal que atenda aos requisitos estabelecidos pelo Comitê Gestor da RIBPG, nomeado por portaria, ponto central de contato para a RIBPG no Laboratório de Biologia e DNA Forense, responsável por garantir o cumprimento das normas estabelecidas no Manual de procedimentos operacionais da Rede Integrada de Bancos de Perfis Genéticos.

§ 3º Administrador local: é o Administrador do BPG/SPTC-GO e que possui acesso ilimitado e irrestrito a todas as funcionalidades do software CODIS, para monitorar e realizar atualizações e upgrades no *software*.

§ 4º Usuários do grupo *backup operators*: usuários que contém conta de acesso ao sistema operacional do Windows onde funciona o CODIS, para realização dos backups e manutenção do servidor.

§ 5º BNPG: Banco Nacional de Perfis Genéticos.

§ 6º BPG/SPTC-GO: Banco de Perfis Genéticos da Superintendência de Polícia Técnico-científica do Estado de Goiás.

§ 7º CODIS: *Combined DNA Index System*.

§ 8º FBI: *Federal Bureau of Investigation*.

§ 9º GIT: Gerência de Informática e Telecomunicações.

§ 10. ICLR: Instituto de Criminalística Leonardo Rodrigues.

§ 11. RIBPG: Rede Integrada de Banco de Perfis Genéticos.

§ 12. SEGPLAN: Secretaria de Estado de Gestão e Planejamento.

§ 13. SPTC: Superintendência de Polícia Técnico-científica.

§ 14. SSPGO: Secretaria de Segurança Pública do Estado de Goiás.

Art. 3º Definir os Recursos Necessários:

§ 1º Servidor com sistema CODIS;

§ 2º Ambiente climatizado e seguro para guarda do servidor.

Art. 4º Descrever os Procedimentos no Tocante as Considerações Iniciais

§ 1º O Banco de Perfis Genéticos da SPTC/GO foi criado pela Portaria n.º 1970/2014 datada de 29/12/2014 da SSPGO;

O software utilizado pelo BPG/SPTC foi cedido pelo FBI por acordo celebrado entre o Governo Brasileiro (Polícia Federal) e o Governo Americano (FBI).

§ 2º O Estado de Goiás, para receber o software CODIS, assinou acordo de cooperação técnica cujo extrato foi publicado no Diário Oficial da União n.º 227, na Seção 3, do dia 22/11/2013;

§ 3º A carta divulgada pelo FBI do Departamento de Justiça dos Estados Unidos (*Letter of Agreement* - LOA), em 05/01/2015, na Seção II.A.2 da Carta de Acordo, estabelece que uma das responsabilidades do FBI é preparar e distribuir diretrizes para a utilização do CODIS. Essas diretrizes devem estar disponíveis na língua inglesa. De acordo com essa cláusula, são consideradas ainda as seguintes diretrizes nos termos do acordo: não autoriza qualquer agência ou lei internacional a distribuir, publicar ou divulgar informações obtidas ou incluídas no software, incluindo, boletins, capturas de tela do software, materiais de reunião e instruções e/ou material de treinamento, sem a aprovação prévia por escrito do FBI;

§ 4º Todas as ações relacionadas ao sistema CODIS estão baseadas nos três princípios da segurança da informação e, portanto, norteadores das ações desenvolvidas por todos os operadores e usuários do sistema CODIS e demais sistemas que viabilizam a operacionalização do BPG/SPTC-GO:

I - Confidencialidade: a informação somente deve estar acessível a quem deva acessá-la e a ninguém mais;

II - Integridade: a informação deve estar íntegra, sem alterações não autorizadas, causadas dolosa ou culposamente, até mesmo de forma acidental;

III - Disponibilidade: a informação deve estar sempre disponível a quem deve ter acesso

a ela.

§ 3º O servidor que hospeda o BPG/SPTC e, conseqüentemente, o software CODIS está fisicamente instalado na Gerência de Informática e Telecomunicações da SSPGO (GIT/SSPGO);

§ 4º O cliente que acessa o servidor está fisicamente instalado no Laboratório de Biologia e DNA Forense do Instituto de Criminalística Leonardo Rodrigues;

§ 5º O Administrador Titular do BPG/SPTC-GO e, na sua ausência, seu adjunto, de acordo com o Manual de Procedimentos Operacionais da RIBPG, 3ª Versão, publicado pela Resolução n.º 02 de 24/10/2017, do Comitê Gestor, é o ponto central de contato para a RIBPG e é o responsável, executando ou supervisionando, por:

I - Garantir o cumprimento das normas estabelecidas no referido manual;

II - Exercer o controle de usuários que acessam o sistema CODIS;

III - Garantir o sigilo dos dados armazenados;

IV - Notificar o administrador do Banco Nacional de Perfis Genéticos, caso o Laboratório deixe de cumprir requisitos estabelecidos no Manual da RIBPG;

V - Garantir o funcionamento do BPG/SPTC-GO e a sua comunicação com o BNPG;

VI - Realizar cópias de segurança do BPG/SPTC-GO (*backup*); e

VII - Os procedimentos de inserção, uploads e análise dos resultados do BPG/SPTC-GO.

VIII - Considerando o grau de especialização exigidos para realização de cópias de segurança do sistema CODIS, bem como o nível de acesso necessário para garantir a segurança do servidor, tais atribuições devem ser realizadas pela Gerência de Informática e Telecomunicações da Secretaria de Segurança Pública do Estado de Goiás (GIT/SSPGO).

IX - É de responsabilidade do Administrador do BPG/SPTC-GO e, na sua ausência, seu adjunto, supervisionar as atividades desenvolvidas pela GIT/SSPGO relacionadas ao sistema CODIS. A GIT/SSPGO deve permitir visitas técnicas do Administrador do BPG/SPTC-GO e deve enviar relatórios, quando solicitado, para monitorar e acompanhar as ações decorrentes da manutenção do hardware e da realização das cópias de *backup* exigidas pelo Manual da RIBPG.

X - A GIT/SSPGO deve permitir auditorias internas e auditorias externas, agendadas previamente, como do Ministério da Justiça, conforme prevê o Art. 9º do Decreto Presidencial n.º 7.950/13, ou de órgãos acreditadores.

XI - O Gerente da GIT/SSPGO ou servidor por ele designado deve informar qualquer intercorrência do BPG/SPTC-GO que venha comprometer:

a) O sigilo dos dados armazenados;

b) A segurança do servidor que hospeda o sistema CODIS;

c) Qualquer problema que inviabilize a comunicação entre o cliente e o servidor e entre este e o BNPG;

d) Qualquer dano no hardware e/ou software;

e) Qualquer ocorrência que a equipe especializada julgar necessária comunicar ao Administrador do BPG/SPTC-GO.

Art. 5º Dispor sobre a segurança física do servidor CODIS:

§ 1º O servidor deve ficar em ambiente de acesso restrito e controlado. Não é permitido o livre acesso a usuários não autorizados previamente pelo Administrador do BPG/SPTC-GO;

§ 2º O servidor deve ser protegido de variações de picos na rede elétrica;

§ 3º O servidor deve ser protegido de variações de temperatura.

Art. 6º Descrever a Rotina de *backup*:

§ 1º O banco de dados do sistema CODIS é baseado no sistema Microsoft SQL Server. Dessa forma, toda instalação do CODIS contém um plano de manutenção (*Maintenance Plan*) que inclui a geração de cópias de segurança em todos os dias úteis (de segunda à sexta-feira). Esse plano de manutenção prevê a retenção de cópias de segurança das últimas quatro semanas, apagando as mais antigas. As cópias de segurança do BPG/SPTC-GO, devem obedecer as “Orientações gerais para backup dos bancos de perfis genéticos, Versão 1, de 16 de março de 2015” (documento interno da RIBPG);

§ 2º Os backups diários, armazenados no servidor, podem ser comprometidos em casos mais graves de dano ou falha no sistema. Dessa forma o servidor CODIS não pode ser o único local de guarda de cópias de segurança. Diariamente, devem ser feitos *backup* em outra unidade de armazenamento;

§ 3º As cópias de *backup* externas devem ser realizadas na SEGPLAN, em servidores remotos que são disponibilizados no *Data Center* do órgão para uso da SSP, conforme Decreto nº 8.463, de 29 de setembro de 2015, em ambiente com acesso restrito à equipe da GIT/SSPGO;

§ 4º O ambiente da SEGPLAN que hospeda as cópias de *backup* do sistema CODIS também está sujeito a auditorias internas e externas, conforme prevê o Decreto Presidencial n.º 7.950/13 e as normas estabelecidas pelo Comitê Gestor da RIBPG;

§ 5º Os arquivos e pastas críticas para backup estão descritos nas “Orientações gerais para backup dos bancos de perfis genéticos, Versão 1, de 16 de março de 2015” (documento interno da RIBPG);

§ 6º Deve ser realizado ainda backup da máquina virtual, que deve ser feito conforme as “Orientações gerais para backup dos bancos de perfis genéticos, Versão 1, de 16 de março de 2015” (documento interno da RIBPG). Cabe ao suporte de tecnologia da informação verificar o pleno funcionamento deste *backup*, sob a supervisão do Administrador do BPG/SPTC-GO. Recomenda-se realizar *backup* da máquina virtual a cada 3 meses.

Art. 7º Dispor sobre os Usuários que podem realizar *backup*:

§ 1º Os usuários com perfil de administrador do BPG/SPTC-GO tem privilégios para realizar *backups*;

§ 2º Os usuários com perfil de administrador local têm privilégios para realizar *backups*;

§ 3º Os usuários que estejam no grupo “*backup operators*” tem privilégios para realizar *backups*;

§ 4º Somente terá acesso ao servidor CODIS, para manutenções e realização das cópias de segurança, pessoas previamente autorizadas formalmente pelo Administrador do BPG/SPTC-GO;

§ 5º O usuário responsável pela manutenção do servidor e realização das cópias de segurança somente poderá utilizar seu usuário e senha. As contas de acesso devem ser criadas individualmente, uma para cada usuário, inclusive para o suporte de tecnologia da informação;

§ 6º Todos os usuários devem assinar termo de sigilo e confidencialidade.

Art. 8º Informar outras ações para proteção do sistema CODIS:

§ 1º É de competência da GIT/SSPGO designar servidor especializado, sob a supervisão do Administrador do BPG/SPTC-GO e, na sua ausência, seu adjunto, para realizar atualização mensal do sistema operacional do CODIS (*Windows update*);

§ 2º Os sistemas que hospedam o servidor e cliente devem ser protegidos com antivírus;

§ 3º Os sistemas operacionais (*Windows*) do CODIS devem estar em uma rede separada por firewall;

§ 4º O sistema CODIS funciona apenas com a liberação no Firewall do acesso ao sistema para os Peritos Criminais usuários do CODIS, através de IP específico da Estação de Trabalho informada;

§ 5º É liberado acesso remoto ao servidor para a Equipe de TI da GIT/SSPGO, para configuração de monitoramento e manutenção do servidor;

§ 6º Adicionalmente, é necessária a liberação do Windows Update, para a atualização do Windows, a liberação de atualização do sistema Antivírus e a liberação para monitoramento do servidor pelo Zabbix e PRTG;

§ 7º Não é necessário acesso externo algum ao servidor diretamente.

PUBLIQUE-SE.

Gabinete do Secretário de Estado da Segurança Pública de Goiás, Goiânia, aos 07 dias do mês de junho de 2018.

**IRAPUAN COSTA JÚNIOR**

Secretário



Documento assinado eletronicamente por **IRAPUAN COSTA JUNIOR, SECRETÁRIO DE ESTADO**, em 07/06/2018, às 14:57, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.



A autenticidade do documento pode ser conferida no site [http://sei.go.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=1](http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1) informando o código verificador **2794211** e o código CRC **DD14443D**.

Secretaria de Estado da Segurança Pública – [www.ssp.go.gov.br](http://www.ssp.go.gov.br)  
Av. Anhanguera, n. 7364 – Setor Aeroviário – CEP 74543-010 Goiânia - GO  
fone: 3201-1000



