



GRUPO DE TRABALHO:

RECURSOS CRIPTOGRÁFICOS

“Ampliar estudos sobre o uso, contratação de serviços e desenvolvimento de recursos criptográficos.”

Coordenador: Carlos Gustavo Cordeiro De Andrade (MRE)

Facilitador: Bruno Pereira Pontes (GSI/PR)



RECURSOS CRIPTOGRÁFICOS

INTEGRANTES

1. Carlos Gustavo Cordeiro De Andrade (MRE)
2. Bruno Pontes (GSI/DSIC)
3. Loriza Andrade Vaz de Melo (MP)
4. Rodrigo Fernandes França (MP)
5. Otávio Carlos Cunha da Silva (ABIN)



PROPOSTA DO GRUPO DE TRABALHO:

- Revisão da NC 09/IN01/DSIC/GSIPR (Uso Recurso Criptográfico);



PREMISSAS:

- Evitar o uso “indiscriminado” do algoritmo de estado (informação sigilosa não classificada);
- Contemplar o uso de criptografia na interligação das redes;
- Tratar do armazenamento da informação criptografada;
- Alterar o mínimo a estrutura da norma já existente;



REVISÃO DA NC 09:

- 2. CONCEITOS E DEFINIÇÕES:
 - 2.3 *Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e/ou método de processo sejam passíveis de controle e auditoria;*
 - 2.8 *Empresa Estratégica de Defesa (EED) do setor de Tecnologia de Informação e Comunicação (TIC): toda pessoa jurídica do setor de Tecnologia de Informação e Comunicação (TIC) devidamente credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das condições previstas no inciso IV do art. 2º da Lei nº 12.598, de 22 de março de 2012.*



REVISÃO DA NC 09:

- 5. ORIENTAÇÕES ESPECÍFICAS:
 - 5.1 Algoritmo de Estado:
 - 5.2 Algoritmo Registrado:



REVISÃO DA NC 09:

- 5. ORIENTAÇÕES ESPECÍFICAS:
 - 5.1 *Algoritmo de Estado:*
 - 5.1.3 *Toda informação classificada, mesmo quando criptografada, somente poderá ser armazenada em centro de processamento de dados fornecido por órgãos e entidades da Administração Pública Federal, conforme legislação em vigor.*
 - 5.1.5 *Recomenda-se o uso de recurso criptográfico baseado em algoritmo de Estado para a criação de um canal de comunicação seguro (Rede Privada Virtual - VPN) para interligar redes dos órgãos e entidades da APF, direta e indireta, objetivando a troca de informações sigilosas.*



REVISÃO DA NC 09:

- 5. ORIENTAÇÕES ESPECÍFICAS:
 - 5.1 *Algoritmo de Estado:*
 - 5.1.6 *Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, poderá ser utilizado recurso criptográfico baseado em algoritmo de Estado para a cifração e decifração das informações sigilosas não classificadas.*
 - 5.1.12 *Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no item 5.1.9 poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições:*
 - *a) a empresa seja preferencialmente uma Empresa Estratégica de Defesa do setor de Tecnologia de Informação e Comunicação e utilize tecnologia nacional, não sendo aceito empresas que apenas forneçam recursos criptográficos com tecnologia estrangeira;*



REVISÃO DA NC 09:

- 5. ORIENTAÇÕES ESPECÍFICAS:
 - 5.2 *Algoritmo Registrado:*
 - 5.2.1 *Recomenda-se a utilização de recurso criptográfico baseado em algoritmo registrado para cifração e decifração das informações sigilosas não classificadas, desde que atendidas obrigatoriamente as seguintes condições:*



REVISÃO DA NC 09:

- 5. ORIENTAÇÕES ESPECÍFICAS:
 - *a) O desenvolvimento ou obtenção do algoritmo registrado deverá ser realizado levando-se em consideração a necessidade de proteção da informação sigilosa, bem como as possíveis ameaças à sua exposição, cabendo tal responsabilidade a alta administração do órgão que o empregará; e*
 - *b) O algoritmo deverá ser registrado no GSI/PR, que manterá sob sua guarda e controle o banco de registros;*
 - *c) O órgão deverá manter sob sua guarda o código fonte e método de processos do algoritmo, bem como implementar os controles adequados, inclusive quanto à auditoria;*



REVISÃO DA NC 09:

- 5. ORIENTAÇÕES ESPECÍFICAS:
 - 5.2 *Algoritmo Registrado:*
 - 5.2.3 *Recomenda-se que a informação sigilosa não classificada, mesmo quando criptografada, seja armazenada em centro de processamento de dados fornecido por órgãos e entidades da Administração Pública Federal, conforme legislação em vigor.*
 - 5.2.4 *A critério do órgão, o recurso criptográfico baseado em algoritmo registrado poderá ser utilizado para a cifração e decifração das informações consideradas por ele de acesso restrito.*



REVISÃO DA NC 09:

- 7. DISPOSITIVOS TRANSITÓRIOS:
 - 7.4 O GSI/PR elaborará um guia técnico de recursos criptográficos com orientações de como proceder para cumprir o previsto no item 5.2.1.



CONTRIBUIÇÕES:

- A Proposta de Revisão da NC 09 foi submetida ao CGSI para apreciação em 27/11 do corrente;
- Foram recebidas contribuições do Banco Central, do MRE e do próprio DSIC;
- As sugestões do MRE não resultaram em mudanças na proposta do GT, foram apenas esclarecidas dúvidas;



CONTRIBUIÇÕES:

- As contribuições do Banco Central resultaram nas seguintes mudanças:
 - O depósito do código fonte e/ou método de processo será feito no próprio órgão, devendo ser feito apenas o registro no GSI/PR, que necessitará do mínimo de informações.
 - Foi incluído também, em disposições transitórias, que o GSI/PR elaborará um guia técnico de recursos criptográficos com orientações de como proceder para cumprir o previsto na norma.



CONTRIBUIÇÕES:

- As contribuições do DSIC resultaram nas seguintes mudanças:
 - Ajuste no conceito de Empresa Estratégica de Defesa.
 - Organização do item 5 com base nos recursos e não mais no tipo de informação.



CONCLUSÃO:

- Necessidade de revisão do artigo Art. 4º, 6º, 7º e 8º da IN GSI/PR nº 3:
 - Referências da NC09 e de seus itens;
- Necessidade de revisão do artigo Art. 5º da IN GSI/PR nº 3:
 - Inclusão do inciso que trata da Empresa Estratégica de Defesa;