PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL

COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

ATA DE REUNIÃO – SESSÃO POR VIDEOCONFERÊNCIA

Aos 15 dias do mês de setembro do ano de 2022, às 9 horas e 30 minutos, reuniram-se os membros titulares e suplentes do Comitê Gestor da ICP-Brasil - CG ICP-Brasil e servidores do ITI para participar da Reunião Ordinária deste Comitê. Estiveram presentes: Juliana Ribeiro Silveira (Coordenadora do CG ICP-Brasil) da Casa Civil da Presidência da República; Carlos Roberto Fortner (Secretário-Executivo do CG ICP-Brasil); Victor Hugo da Silva Rosa (Titular do Gabinete de Segurança Institucional da Presidência da República); Leonardo Garcia Greco (Titular do Ministério da Justiça e Segurança Pública); Luiz Carlos Miyadaira Ribeiro Junior (Titular do Ministério da Economia); Rubens Caetano Barbosa de Souza (Titular do Ministério da Ciência, Tecnologia e Inovação); Marcio Nunes da Silva (Suplente da Sociedade Civil); Edmar da Silva Araújo (Titular da Sociedade Civil); Sérgio Paulo Gomes Gallindo (Titular da Sociedade Civil); Célio de Siqueira Ribeiro (Titular da Sociedade Civil); Giselle Dias Rodrigues Oliveira de Barros (Titular da Sociedade Civil); Maurício Augusto Coelho (Diretor de Infraestrutura de Chaves Públicas – ITI); Pedro Pinheiro Cardoso (Diretor de Auditoria, Fiscalização e Normalização – ITI); Alexandre de Munia Machado (Procurador-Chefe do ITI); Jorge Carvalho de Oliveira (Coordenador-Geral de Normalização e Pesquisa -ITI); Alcimar Sanches Rangel (Chefe de Gabinete – ITI); José Rodrigues Gonçalves (Coordenador-Geral de Infraestrutura e Segurança da Informação); André Machado Caricatti (Coordenador-Geral de Operações); Brenda Rodrigues Mesquita Sampaio (Assessora de Comunicações – ITI). A Reunião foi realizada por videoconferência, usando o aplicativo Webex pelo link: https://iticonferencia.webex.com/iticonferencia/j.php?MTID=m3b86917a3b033a30c2fe51722295301f e transmitida em tempo real e aberta via canal do Youtube e permanece em seu inteiro teor à disposição na página: https://www.youtube.com/watch?v=bfG1IJScBlI.

Abertura e pronunciamento inicial: Após os cumprimentos formais, a Coordenadora do CG ICP-Brasil, Juliana Ribeiro Silveira, apresentou as boas-vindas aos membros do CG ICP-Brasil, convidados presentes e aos ouvintes que acompanharam a reunião pela internet. Em seguida, o Coordenadora informou que em decorrência do período de defeso eleitoral, o *chat* da reunião foi desativado, e ainda, solicitou que os participantes não poderão debater temas de cunho político que possa se caracterizar publicidade eleitoral, uma vez que a reunião será disponibilizada no canal do *Youtube*. Em seguida, informou sobre a recondução dos seguintes membros da sociedade civil no CG ICP-Brasil: Márcio Nunes da Silva, Sérgio Paulo Gomes Gallindo, Giselle Dias Rodrigues Oliveira de Barros, Eduardo Calais Pereira, informou também a nomeação dos novos membros do Ministério das Relações Exteriores: Túlio César Mourthé de Alvim Andrade e Graziela Rodrigues Caselli. Em seguida, declarou aberta a reunião, para tratar das seguintes pautas a serem deliberadas:

Pauta 1: Revogação da Resolução nº 160, de 17 de abril de 2020.
Pauta 2: Apresentação do Relatório do GTT Sala-Cofre.
Pauta 3: Aprovação dos Relatórios de Auditoria da AC Raiz (2021)
Pauta 4: Gerenciamento de PUK Mediante Validação Presencial.

Em seguida, a Coordenadora do CG ICP-Brasil passou a palavra ao Secretário-Executivo do Comitê Gestor, senhor Carlos Roberto Fortner, para a condução dos trabalhos que, de imediato, solicitou que o senhor Jorge Carvalho de Oliveira, Coordenador-Geral de Normalização e Pesquisa do ITI, apresentasse os aspectos técnicos relativos à Pauta 1.

Finalizada a apresentação do senhor Jorge Carvalho de Oliveira, o Secretário-Executivo do Comitê Gestor retomou a palavra e abriu a discussão com os membros do CG ICP-Brasil.

O senhor Sérgio Paulo Gomes Gallindo manifestou-se favorável à pauta, no entanto, solicitou que constasse em ata as sugestões referentes à Pauta 1 que estão anexadas na página 8 desta Ata.

O senhor Edmar da Silva Araújo manifestou-se de forma que as reuniões virtuais fossem priorizadas, uma vez que são mais eficientes, econômicas, práticas e demandam menos esforços logísticos para o ITI.

Em seguida, a Coordenadora iniciou a deliberação da Pauta 1

Pauta 1: Revogação da Resolução nº 160, de 17 de abril de 2020.

Síntese do problema ou da situação que reclama providências.

Considerando a Declaração de Emergência em Saúde Pública de Importância Internacional pela Organização Mundial da Saúde - OMS, em 30 de janeiro de 2020, o Ministério da Saúde publicou a Portaria nº 188, de 3 de fevereiro de 2020.

Com o objetivo de contribuir com os esforços de contenção da pandemia, considerado a decisão de governo de minimizar os efeitos da pandemia sobre a economia, o ITI editou a Instrução Normativa nº 04, de 07 de abril de 2020, para tratar a situação das assembleias de condomínios e o Comitê Gestor da ICP-Brasil publicou a Resolução nº 160, de 17 de abril de 2020, que estabeleceu diretrizes para as reuniões do Plenário do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (CG ICP-Brasil) durante o estado de emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19).

Os atos publicados em decorrência da pandemia em geral declaram a vigência incluindo algo como "permanecendo em vigor enquanto perdurar o estado de emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19)", ou seja, a vigência não está determinada.

Com a publicação da Portaria GM/MS nº 913, de 22 de abril de 2022, que declarou o encerramento da Emergência em Saúde Pública de Importância Nacional (ESPIN) em decorrência do coronavírus (2019-nCov), revogando a Portaria nº 188, de 3 de fevereiro de

2020, os diversos decretos e atos inferiores a decretos editados para normatizar as medidas necessárias ao enfrentamento da crise e regulamentar as relações oriundas do estado de emergência em saúde pública estariam com seus efeitos possivelmente prejudicados ou exauridos, em razão do término da situação de crise sanitária.

Esse entendimento foi apresentado pela Subchefia de Articulação e Monitoramento - SAM, que encaminhou à Casa Civil da Presidência da República, por meio do Ofício nº 216/2022/SAM/CC/PR, sugestões para a revogação de atos normativos em decorrência da publicação da Portaria GM/MS nº 913, de 22 de abril de 2022. Por meio do ofício nº 216/2022/SAM/CC/PR, a Casa Civil da Presidência da República encaminhou ao Instituto Nacional de Tecnologia da Informação as sugestões da SAM para conhecimento e as devidas providências.

Das sugestões apresentadas constam as Resoluções nº 167, de 17 de abril de 2020, e nº 170, de 23 de abril de 2020, já revogadas anteriormente, restando a revogação da Resolução nº 160, de 17 de abril de 2020.

Resultado da votação: **PAUTA 1 APROVADA POR UNANIMIDADE.**

Em seguida, o Secretário-Executivo do Comitê solicitou que o Wilson Roberto Hirata, Assessor do Diretor-Presidente do ITI, apresentasse os aspectos técnicos relativos à Pauta 2.

Finalizada a apresentação do senhor Jorge Carvalho de Oliveira, o Secretário-Executivo do Comitê Gestor retomou a palavra e abriu a discussão com os membros do CG ICP-Brasil.

O senhor Sérgio Paulo Gomes Gallindo apresentou suas considerações relativas à Pauta 2 que estão anexadas na página 9 desta Ata.

Logo após, o senhor Edmar da Silva Araújo apresentou suas considerações relativas à Pauta 2 que estão anexadas na página 11 e 12 desta Ata.

Pauta 2: Apresentar o Relatório do GTT Sala-Cofre.

Síntese do problema ou da situação que reclama providências.

O Grupo de Trabalho Técnico, denominado GTT Sala-cofre, foi instituído pela Resolução do Comitê Gestor da ICP-Brasil n° 198, destinado à elaboração de estudos e de propostas voltadas à dispensa da obrigatoriedade de manutenção de salas cofre para guarda de Módulo de Segurança Criptográfica (MSC).

A coordenação do GTT foi delegada ao assessor Wilson Roberto Hirata, conforme Portaria ITI nº 19, de 25 de novembro de 2021.

Para o levantamento de subsídios, realizaram-se fóruns de discussões a respeito do tema "segurança física" com representantes de entidades envolvidas direta ou indiretamente na operacionalização de infraestrutura de missão crítica.

Considerando que durante os meses de levantamento de subsídios o grupo concluiu não haver consenso sobre qualquer proposta para estudo viável que permita a dispensa da exigência de sala-cofre sem incorrer em rebaixamento de requisitos de segurança, chegou-se à conclusão pelo encerramento dos trabalhos.

Por fim, o objetivo da presente pauta é apresentar para avaliação do Comitê Gestor da ICP-Brasil o relatório produzido pelo GTT Sala-Cofre, contendo as conclusões e recomendações, atendendo ao disposto no art. 4º da Resolução CG ICP-Brasil n° 198, de 16 de novembro de 2021.

PAUTA 2 – NÃO DELIBERATIVA (RELATÓRIO APRESENTADO).

Em seguida, o Secretário-Executivo do Comitê solicitou que o senhor Mauricio Augusto Coelho, Diretor de Infraestruturas de Chaves Públicas, apresentasse os aspectos técnicos relativos à Pauta 3.

Finalizada a apresentação do senhor Mauricio Augusto Coelho, o Secretário-Executivo do Comitê Gestor retomou a palavra e abriu a discussão com os membros do CG ICP-Brasil.

Durante a discussão da Pauta, os membros do Comitê parabenizaram com louvor a equipe da Diretoria de Infraestruturas de Chaves Públicas pelos resultados alcançados por ocasião da Auditoria da AC Raiz realizada pela empresa *Ernest & Young.*

Encerrado o debate, a Coordenadora iniciou a deliberação da Pauta 3.

Pauta 3: Aprovação dos Relatórios de Auditoria da AC Raiz (2021).

Síntese do problema ou da situação que reclama providências.

O Comitê Gestor da ICP-Brasil aprovou, por meio da Resolução nº 159, de 07 de fevereiro de 2020, a contratação de empresa de auditoria independente para auditar o ambiente operacional da Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviço de suporte, segundo as normas e padrões estabelecidos para a ICP-Brasil e, ainda, segundo os normativos internacionais WebTrust, nos exercícios de 2020 a 2024.

Dessa forma, através do Contrato nº 14/2018, firmado entre o ITI e a empresa Ernst & Young Auditores Independentes S/S, foi realizada a auditoria baseada nos normativos vigentes, denominados DOC-ICP-01 e DOC-ICP-02, e documentos Webtrust, para o período de 09 de setembro de 2020 a 08 de setembro de 2021 (exercício 2021), cujos Relatórios de Conformidade da AC Raiz e de Asseguração, encontram-se à disposição dos membros do Comitê Gestor.

Resultado da votação: **PAUTA 3 APROVADA POR UNANIMIDADE.**

Em seguida, o Secretário-Executivo do Comitê solicitou que o senhor Wilson Roberto Hirata, Assessor do Diretor-Presidente do ITI, apresentasse os aspectos técnicos relativos à Pauta 4.

Finalizada a apresentação do senhor Wilson Roberto Hirata, o Secretário-Executivo do Comitê Gestor retomou a palavra e abriu a discussão com os membros do CG ICP-Brasil.

O senhor Sérgio Paulo Gomes Gallindo apresentou suas considerações relativas à Pauta 4 que estão anexadas nas páginas 9 e 10 desta Ata.

Logo após, o Edmar da Silva Araújo apresentou que suas manifestações como membro deste Comitê foram construídas coletivamente pelos associados da Associação de Autoridades de Registro do Brasil (AARB) e relatou que o tema desta Pauta dividiu as opiniões de seus associados, pois algumas Autoridades de Registro (AR) entenderam que tema discutido seria um fator positivo para o consumidor final da certificação digital, enquanto outras AR entenderam que estariam abraçando uma responsabilidade que hoje não estaria em sua missão enquanto AR, nesse sentido, partes de AR se sentiram desconfortáveis para o gerenciamento do PUK. Com isso, o senhor Edmar sugeriu, sem prejuízo à deliberação da Pauta, que fosse criado um fórum de discussão para debater o tema a fim de deixar as AR mais confortáveis e seguras.

Em seguida, o senhor Pedro Pinheiro Cardoso, Diretor de Auditoria, Fiscalização e Normalização do ITI, comentou que a Pauta não está relacionada como uma nova atribuição para as Autoridade de Certificação (AC) ou para as AR, isso porque possibilita o titular de certificado digital atribuir a um terceiro o gerenciamento do seu PUK, a exemplo de uma empresa ou órgão de governo que tenha adquirido certificados para todos seus colaboradores que pode designar um setor exclusivo para realizar o gerenciamento do PUK. Ademais, cabe a decisão do titular sobre o gerenciamento de seu PUK, não seria uma obrigação para a AR

Encerrada a apresentação e não havendo manifestações, a Coordenadora iniciou a deliberação da Pauta 4.

COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Pauta 4: Gerenciamento de PUK Mediante Validação Presencial.

Síntese do problema ou da situação que reclama providências.

O item 4.5.1.2, alínea “b”, do documento DOC-ICP-05, versão 6.2, dispõe sobre obrigações do titular, trazendo na alínea “b”:

> “...
>
> b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
>
> ...”

Importante ressaltar que a senha que protege diretamente a chave privada armazenada em cartão ou token criptográfico é denominada PIN (Personal Identification Number). O PUK (PIN Unlock Key), por sua vez, tem como função desbloquear ou possibilitar a troca do código PIN, ou seja, um código PUK possibilita acesso a uma chave privada somente de forma indireta pela possibilidade de substituição de um código PIN. Ademais, a implementação do PUK é opcional como papel de acesso de oficial de segurança para cartões criptográficos (Smartcard).

Nesse sentido, o gerenciamento do PUK só possibilita acesso à chave privada de um certificado quando a mídia criptográfica armazenadora da referida chave estiver ao alcance do gerenciador do PUK.

Assim, é possível implementação de gerenciamento do PUK por uma entidade confiável (AC ou AR) sem comprometimento da proteção da chave privada, desde que tal implementação adote procedimentos de segurança no processo de desbloqueio/troca do PIN e mediante autorização do usuário.

Uma das formas de procedimento seguro em gerenciamento de PUK por entes confiáveis e mediante a autorização do usuário poderia ser por meio de validação presencial do titular do certificado no processo de desbloqueio de PIN. Nessa situação, o procedimento de gerenciamento do PUK pode ser perfeitamente viável e seguro do ponto de vista de proteção da chave privada do titular do certificado, não comprometendo a conformidade com o disposto no item 4.5.1.2, alínea "b", do DOC-ICP-05, versão 6.2.

COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Resultado da votação: **PAUTA 4 APROVADA.**

- 9 (nove) votos favoráveis: Victor Hugo da Silva Rosa; Leonardo Garcia Greco; Luiz Carlos Miyadaira Ribeiro Junior; Rubens Caetano Barbosa de Souza; Marcio Nunes da Silva; Sérgio Paulo Gomes Gallindo; Célio de Siqueira Ribeiro; e Giselle Dias Rodrigues Oliveira de Barros.
- 1 (um) voto contrário: Edmar da Silva Araújo.

Por fim, a Coordenadora informou que a próxima reunião ordinária será realizada no período de 15 a 22 de março de 2023 e que, oportunamente, todos serão informados sobre a data e horário.

Nada mais havendo a registrar, considerou-se encerrada da qual, para constar, eu, Alcimar Sanches Rangel, Chefe de Gabinete do Instituto Nacional de Tecnologia da Informação – ITI, à luz do artigo 7º e do artigo 27 do anexo I da Resolução CG ICP-Brasil nº 190, 18 de maio de 2021, que aprova o regimento interno do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira – CG ICP-Brasil., lavrei a presente Ata que, lida e aprovada, encaminha-se assinada digitalmente para publicação no site do ITI, www.iti.gov.br.

ALCIMAR SANCHES RANGEL
Assinado de forma digital por ALCIMAR SANCHES RANGEL
Dados: 2022.11.10 14:15:39 -03'00'

ALCIMAR SANCHES RANGEL
Chefe de Gabinete do ITI

Aprovo a lavratura da presente Ata de Reunião. Publique-se.

CARLOS ROBERTO FORTNER
Assinado de forma digital por CARLOS ROBERTO FORTNER
Dados: 2022.11.10 19:04:24 -03'00'

CARLOS ROBERTO FORTNER
Secretário-Executivo do CG ICP-Brasil

Brasscom

São Paulo, 14 de setembro de 2022

Aos

Exma. Sra. **Juliana Ribeiro Silveira**, Coordenadora do CG ICP-Brasil
Exmo. Sr. **Carlos Roberto Fortner**, Secretário-Executivo do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil

C/C:

Sergio Sgobbi, Diretor de Relações Institucionais e Governamentais, Brasscom

Assunto: Voto referente à Plenária por Videoconferência do Comitê Gestor da ICP-Brasil.

Prezados Coordenadora do CG ICP-Brasil Sra. **Juliana Ribeiro Silveira**, e Secr. Ex. do CG ICP-Brasil Sr. **Carlos Roberto Fortner**

Saúdo-os, cordialmente, fazendo votos de estejam bem.

Este representante da **Brasscom**, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, e na qualidade de integrante do CG ICP-Brasil representando da sociedade civil, vem, respeitosamente, perante Sra. Coordenadora do Comitê Gestor e do Sr. Secretário Executivo do Comitê Gestor, e demais membros integrantes do colegiado, apresentar os votos referentes aos temas da Plenária por Videoconferência do Comitê Gestor da ICP-Brasil convocada em 31 de agosto de 2022 a ser realizada em **15 de setembro de 2022.**

Pauta 01: Revogar a Resolução nº 160, de 17 de abril de 2020.

DO VOTO

Pela aprovação, com comentários.

A resolução nº 160, de 17 de abril de 2020, estabeleceu diretrizes para realização das reuniões do Plenário do CG da ICP-Brasil, durante o estado de emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19). A resolução prevê que, todas as reuniões ordinárias ou extraordinárias do Plenário do CG ICP-Brasil sejam realizadas obrigatória e exclusivamente em sessão virtual.

Considerando a publicação da Portaria GM/MS nº 913, de 22 de abril de 2022, que declarou o encerramento da Emergência em Saúde Pública de Importância Nacional (ESPIN) em decorrência da Infecção Humana pelo novo Coronavírus (2019-nCov), a pauta 01, tem propósito de revogar a resolução nº 160, de 17 de abril de 2020, e consequentemente a obrigatoriedade de reuniões exclusivamente por sessão virtual. A **Brasscom** é favorável à pauta,

Entretanto, devemos considerar a opção prevista no Art. 9º parágrafo 1º do Regimento Interno do Comitê Gestor, o qual prevê, que as reuniões poderão ocorrer em **"sessão presencial ou eletrônica (sessão virtual ou sessão por videoconferência)"**, de forma que revogação da Resolução nº 160, de 17 de abril de 2020 não inviabilize o modelo "híbrido", a saber, a faculdade de realizar reuniões do Plenário do CG da ICP-Brasil, concomitantemente, de modo **presencial ou virtual**.

Brasscom - Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais
Rua: Gomes de Carvalho, nº 1629 – Vila Olímpia – SP – CEP: 04547-006 -Caixa Postal: 112147
SHN, Qd. 1, Bl. A, Edifício Le Quartier, Sala 1514 Brasília/DF

Brasscom

Pauta 02: Apresentação do Relatório Final do GTT Sala-Cofre.

DO VOTO

Pela aprovação, com ressalvas.

O relatório do GTT Sala-cofre, concluiu que:

> *[...] o grupo concluiu não haver consenso sobre qualquer proposta para estudo viável que permita a dispensa da exigência de sala-cofre sem incorrer em rebaixamento de requisitos de segurança;*

Todavia, não foram substanciadas, com lastro em evidências técnicas, a alegada inviabilidade do estudo acerca de opções alternativas às Sala-cofre com requisitos de segurança a altura do necessário. Ademais, nota-se que o objeto de estudo no que diz respeito a segurança, demanda um tempo maior do que o foi instituído inicialmente.

Há desconforto em seguir com o encerramento do GTT apenas por consenso, uma vez que não foram apresentadas evidências técnicas de rebaixamento de segurança. Entendemos como uma perda de oportunidade, considerando que a prorrogação traria insumos às propostas e um resultado conclusivo. Diante do impasse entre continuar os estudos ou encerrar por ausência de materialidade, colocou-se essa questão em votação pelo encerramento dos trabalhos do GTT e a **Brasscom** votou a favor pela continuidade dos estudos.

A estrutura atual é robusta, mas este resultado do GTT vai na contramão da inovação e evolução do certificado digital.

A recomendação da **Brasscom** é novas diligências com fito de viabilizar implementações voltadas à dispensa da obrigatoriedade de manutenção de salas cofre com tecnologias sem comprometer os requisitos de segurança.

Pauta 03: Aprovar os Relatórios de Auditoria da AC Raiz (2021)

DO VOTO

Pela aprovação, sem ressalvas.

A pauta tem como objetivo, aprovar o Relatórios de Conformidade e os Relatórios de Asseguração do ambiente operacional da Autoridade Certificadora Raiz (AC Raiz), bem como seu prestador de serviço de suporte, elaborados pela empresa de auditoria independente Ernst & Young Auditores Independentes S/S, referente ao período auditado de 09 de setembro de 2020 a 08 de setembro de 2021.

Pauta 04. Gerenciamento de PUK Mediante Validação Presencial.

DO VOTO

Pela aprovação, com comentários.

O DOC-ICP-05, prevê que é obrigação do titular do certificado garantir a proteção e sigilo das senhas (PIN e PUK) dos dispositivos criptográficos. O fato é que, parte dos titulares bloqueiam ou descuidam as senhas cadastradas no momento da validação do certificado digital, inviabilizando a utilização e condicionando a uma nova emissão.

Brasscom - Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais
Rua: Gomes de Carvalho, nº 1629 – Vila Olímpia – SP – CEP: 04547-006 -Caixa Postal: 112147
SHN, Qd. 1, Bl. A, Edifício Le Quartier, Sala 1514 Brasília/DF

Brasscom

A pauta propõe mudanças no DOC-ICP-05, possibilitando o gerenciamento da PUK por entidade confiável (AC ou AR) sem comprometimento da proteção da chave privada do titular. A senha PUK, tem como função desbloquear ou possibilitar a troca do código PIN, somente de forma indireta, ou seja, só possibilita acesso à chave privada de um certificado quando a mídia criptográfica da referida chave estiver ao alcance do gerenciador do PUK e com autorização do usuário.

Desta forma, a **Brasscom** é favorável à pauta, considerando melhorar experiência do usuário.

Considerações Finais

Agradecemos a disponibilidade de toda a equipe do ITI, que nos atendeu prontamente para tirar dúvidas em relação as respectivas pautas.

Sendo o que nos cumpria manifestar, permanecemos à disposição para continuar contribuindo em prol da construção de um **Brasil Digital, Conectado e Inovador.**

Respeitosamente,

Sergio Paulo Gallindo
Presidente Executivo

Brasscom - Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais
Rua: Gomes de Carvalho, nº 1629 – Vila Olímpia – SP – CEP: 04547-006 -Caixa Postal: 112147
SHN, Qd. 1, BL A, Edifício Le Quartier, Sala 1514 Brasília/DF

CONSIDERAÇÕES SOBRE SALAS-COFRE

O Grupo de Trabalho Técnico, denominado GTT Sala-cofre, foi instituído e destinado à elaboração de estudos e de propostas voltadas à dispensa da obrigatoriedade de manutenção de salas-cofre para guarda de Módulo de Segurança Criptográfica – MSC (*Hardware Security Module – HSM*). Foi instituído pela Resolução do Comitê Gestor da ICP-Brasil n° 198, de 16 de novembro de 2021, publicado no Diário Oficial da União em 19 de novembro de 2021.

Posto não haver consenso dentre os membros do GTT, acerca da dispensa da exigência de sala-cofre, a AARB, apresenta abaixo suas considerações formais e solicita que seja apensada junto ao processo e ao relatório final do referido GTT.

Originalmente, a ideia do emprego de salas-cofre na ICP-BRASIL está ligada à oferta de alta disponibilidade para o ambiente e dispositivos de Tecnologia da Informação - TI, em especial para *os HSMs.* Historicamente, as salas-cofre foram adotadas como requisito regulatório na ICP-BRASIL, a exemplo de ICPs de outros países que no passado empregaram tais dispositivos, uma vez que mitigavam os seguintes riscos relacionados com:

- efeito Van Eck, ou seja, mitigando espionagem (*phreaking*) a partir da radiação eletromagnética de monitores, especialmente aqueles providos com *Cathode Ray Tube – CRT*, localizados no interior de *data-centers*;
- incêndios, em especial suportando temperaturas até 1.090° C por até 60 minutos e protegendo contra gases ácidos;
- água, suportando colunas de até 40 cm por até 72 horas, bem como umidade relativa de até 85% por até 30 minutos;
- explosões, ocasionadas, por exemplo, por detonação de até 200 kg de TNT, em um raio de 40 metros;
- desabamentos, suportando a queda e o impacto de uma carga de até 200 kg de uma altura de 1,5 metros.

Ocorre que os ambientes da ICP-BRASIL, a exemplo de outras ICPs:

- empregam *HSMs,* nas operações do ciclo de vida dos certificados, notadamente emissão e revogação, conforme dita o item 3 do DOC-ICP01.01. Note que os *HSMs* não possuem monitores, uma vez que são *appliances*, eliminado o risco do efeito Van Eck;
- são contingenciados, conforme ditam os itens 13.2.1 do DOC-ICP-02 e 5.1.8 do DOC-ICP-05, mitigando os demais riscos acima listados.

Adicionalmente, vale ressaltar que sala-cofre não é item de segurança obrigatório nos padrões abaixo listados e é raramente empregado em outras ICPs:

- *WEBTRUST for Certification Authorities*;

- *Request For Comments - RFC 3647 (Nov/2003) - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Frameworke* (vide item 4.5.1.).

E no curso dos trabalhos do GTT Sala-Cofre, tomamos conhecimento que:

- por meio de uma nota e também apresentação do Sr. Roberto Gallo ao GTT, *"historicamente a ICP-Brasil vem relaxando requisitos dos HSMs... no início das operações, os controles de salas-cofre deviam ser combinados com HSMs com Nível de Segurança Física 2... (mais ou menos equivalente a nível 4 do FIPS 140-2) para a AC-Raiz e NSF1 (mais ou menos equivalente a algo entre nível 2 ou 3 FIPS). Acontece, no entanto que há uma diferença substancial entre as proteções físicas de HSMs nos níveis 2, 3 e 4 FIPS. Em tese, nível 4 FIPS pode operar em ambientes com substancial risco físico já que os HSMs possuem proteções anti-tamper ativas e avançadas. Ocorre, no entanto, que o MCT7 no NSF1 as contramedidas físicas são aquém do FIPS 140-2 nível 3. Ou seja, a homologação dos HSMs ICP-Brasil no NSF1 não exige contramedidas suficientes para mitigar riscos gerados por atacantes com acesso físico aos equipamentos"*. E risco de cópia/roubo de chave-privada, em especial da AC, é um risco é independente do emprego de salas-cofre ou não, especialmente quando o *HSM* não é *anti-tamper*;

- apesar das notórias diferenças de operações, tanto o BACEN, como a B3, não utiliza salas-cofre em suas operações de missão-crítica de TI. Os *data-centers* destas instituições são, como na ICP-BRASIL, contingenciados e possuem diversos controles de segurança-física (p. ex. Prevenção e Combate de Incêndios);

- um estudo do Gartner Group (vide https://www.gartner.com/document/3994667?ref=solrSearch&refval=316681589, apresentado pelo líder dos serviços de Cyber Security da PricewaterhouseCoopers – PwC, Sr. Edgar D´Andrea, apontou que *"as atuais arquiteturas de segurança física estarão obsoletas até 2025, devido ao ambiente de amaças em rápida evolução, obsolescência tecnológica e inércia organizacional"*;

- outras operações de ICPs possuem inclusive *HSMs* em nuvem, não acondicionados em salas-cofre em *data-centers* como AWS, Azure e similares.

Assim, a AARB compreende que as salas-cofre da ICP-BRASIL, podem, sem prejuízo da segurança física, serem substituídas por gaiolas (*cages*) em conjunto com o uso de *rack* cofre para os *HSMs* e FIPS 140-2 nível 3 ou superior, mantendo e, inclusive incrementando, demais controles de segurança física, garantindo, no mínimo, os seguintes benefícios:

- Reduzir custos fixos e operacionais;

- Possibilitar ingresso de novos PSSs e PSCs na ICP-BRASIL.

Por fim, a AARB entende a importância estudar a possibilidade de compartilhamento de do ambiente físico principal e de contingência (i.e. *data-centers*), com ou sem a manutenção do requerimento das salas-cofre, por Prestadores de Serviço de Suporte - PSS distintos. Neste sentido, a AARB é favorável a constituição de um GTT específico para analisar este tema.

◊◊◊ FIM DO DOCUMENTO ◊◊◊