EY
Building a better working world

Relatório de asseguração razoável dos auditores independentes

Aos Srs. Administradores,
Autoridade Certificadora Raiz
Brasília - DF

Fomos contratados para realizar um serviço de asseguração razoável sobre a conformidade operacional dos controles internos estabelecidos pela administração da Autoridade Certificadora Raiz para atendimento aos itens citados no Anexo III do documento "Relatório de asseguração razoável dos auditores independentes para auditoria de conformidade operacional de Autoridade Certificadora Raiz, primeira autoridade da cadeia de certificação da ICP-Brasil", extraídos da Declaração de Práticas de Certificação e da Política de Segurança da AC Raiz, no período compreendido entre 09 de setembro de 2015 a 08 de setembro de 2016.

Responsabilidade da administração da entidade

A Administração da Autoridade Certificadora Raiz é responsável pela manutenção dos controles internos que propiciem uma adequada segurança do ambiente de operação das atividades da AC Raiz e a qualidade dos seus respectivos procedimentos operacionais, incluindo medidas para situações de ruptura, contingência ou emergência do ambiente de certificação digital.

Responsabilidade dos auditores independentes

Nossa responsabilidade é de expressar a conclusão sobre a conformidade dos controles internos relativos à segurança do ambiente de certificação digital e à qualidade dos seus respectivos procedimentos operacionais, incluindo medidas para situações de ruptura, contingência ou emergência do ambiente de certificação digital, com base no trabalho de asseguração razoável conduzido de acordo com o Comunicado Técnico CTO 01/12, aprovado pelo Conselho Federal de Contabilidade e elaborado tomando por base a NBC TO 3000 – Trabalho de Asseguração Diferente de Auditoria e Revisão, emitida pelo Conselho Federal de Contabilidade (CFC), que é equivalente à norma internacional ISAE 3000, emitida pela Federação Internacional de Contadores, aplicáveis às informações não históricas. Essas normas requerem o cumprimento de exigências éticas, incluindo requisitos de independência e que o trabalho seja executado com o objetivo de obter segurança razoável de que as informações quantitativas e qualitativas dos controles internos relativos à segurança do ambiente de tecnologia da informação e à qualidade dos procedimentos operacionais, incluindo medidas para situações de ruptura, contingência ou emergência do ambiente de certificação digital tomadas em conjunto, estão livres de distorções relevantes.

Building a better working world

O serviço de asseguração razoável envolve a execução de procedimentos para obter evidências adequadas e suficientes de que os controles internos mencionados anteriormente estão aderentes aos requisitos citados no Anexo III do documento "Relatório de asseguração razoável dos auditores independentes para auditoria de conformidade operacional de Autoridade Certificadora Raiz, primeira autoridade da cadeia de certificação da ICP-Brasil", extraídos da Declaração de Práticas de Certificação e da Política de Segurança da AC Raiz. Os procedimentos selecionados dependem do julgamento do auditor independente, incluindo a avaliação dos riscos dos controles internos descritos anteriormente de não atenderem significativamente os requisitos citados no Anexo III do documento "Relatório de asseguração razoável dos auditores independentes para auditoria de conformidade operacional de Autoridade Certificadora Raiz, primeira autoridade da cadeia de certificação da ICP-Brasil", extraídos da Declaração de Práticas de Certificação e da Política de Segurança da AC Raiz. Nesse sentido, os procedimentos selecionados compreenderam:

(a) O planejamento dos trabalhos, considerando a relevância, o volume de informações quantitativas e qualitativas dos controles internos relativos à segurança do ambiente de certificação digital e à qualidade dos seus respectivos procedimentos operacionais, incluindo medidas para situações de ruptura, contingência ou emergência do ambiente de certificação digital da AC Raiz;

(b) O entendimento da estrutura organizacional envolvida, bem como os processos referentes à segurança do ambiente de operação e à qualidade dos seus respectivos procedimentos operacionais, conforme detalhado no corpo do relatório; e

(c) A aplicação de procedimentos de auditoria para a avaliação do desenho e operação dos controles internos relativos à segurança do ambiente de operação e à qualidade dos seus respectivos procedimentos operacionais, incluindo ações a serem tomadas em caso de eventualidade requeridas pelos normativos citados.

Acreditamos que as evidências obtidas são suficientes e adequadas para constituir a base para a nossa conclusão.

Conclusão

A emissão do parecer para as auditorias de conformidade operacional de entidades integrantes da ICP-BRASIL, obedece aos conceitos estabelecidos no documento ADE-ICP-08-F v.1.0 CRITÉRIOS PARA A EMISSÃO DE PARECER DE AUDITORIA. Desta forma, o parecer segue a tabela abaixo:

Conceito	Parecer	Situação
1	Adequado	Ausência de não conformidades.
2	Aceitável	Média da avaliação dos riscos considerada baixa.
3	Deficiente	Média da avaliação dos riscos considerada mediana.
4	Inadequado	Média da avaliação dos riscos considerada alta.
5	Inaceitável	Média da avaliação dos riscos considerada crítica.

Em vista da metodologia de análise de riscos utilizada pela EY, obtivemos o seguinte parecer com relação aos controles internos relativos à segurança do ambiente de operação e à qualidade dos seus respectivos procedimentos operacionais, incluindo ações a serem tomadas em caso de eventualidade requeridas pelos normativos supracitados em operação no período entre 09 de setembro de 2015 e 08 de setembro de 2016:

Conceito	Parecer	Situação
2	Aceitável	Média da avaliação dos riscos considerada baixa.

O parecer aceitável é decorrente da identificação de 5 (cinco) não conformidades com base nos requisitos abaixo:

Política de Segurança - Requisito 7.3.5.1 (DOC-ICP-02.7.3.5.1)

Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.

Política de Segurança - Requisito 7.3.8.1 (DOC-ICP-02.7.3.8.1)

Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos.

Política de Segurança - Requisito 7.3.5.2 (DOC-ICP-02.7.3.5.2)

Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.

Política de Segurança - Requisito 7.3.7 (DOC-ICP-02.7.3.7)

Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço esta PS e as normas e procedimentos relativos ao trato de

Building a better working world

informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.

Política de Segurança - Requisito 7.3.8.4 (DOC-ICP-02.7.3.8.4)

As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

Opinião com ressalva

Em nossa opinião, com base nos procedimentos descritos na seção "Responsabilidade dos auditores independentes", a Autoridade Certificadora Raiz (AC Raiz) atendeu aos critérios citados no Anexo III do documento "Relatório de asseguração razoável dos auditores independentes para auditoria de conformidade operacional de Autoridade Certificadora Raiz, primeira autoridade da cadeia de certificação da ICP-Brasil", extraídos da Declaração de Práticas de Certificação (DOC-ICP-01) e da Política de Segurança (DOC-ICP-02) da AC Raiz no período compreendido entre 09 de Setembro de 2015 a 08 de Setembro de 2016, exceto para o descrito nos requisitos 7.3.5.1, 7.3.5.2, 7.3.7, 7.3.8.1 e 7.3.8.4 da Política de Segurança da AC Raiz, uma vez que identificamos em seu sítio de contingência 2 (dois) profissionais com avaliações de desempenho realizadas de forma não tempestiva e também não foi possível constatar a realização do treinamento em Políticas de Segurança para 1 (um) profissional selecionado para análise.

Restrições de uso e distribuição

Este relatório, de acordo com o propósito descrito no primeiro parágrafo, destina-se ao uso da Autoridade Certificadora Raiz e do Instituto Nacional de Tecnologia da Informação - ITI. Permitimos a divulgação pela da Autoridade Certificadora Raiz e do Instituto Nacional de Tecnologia da Informação - ITI para terceiros, a seu critério e somente na íntegra, desde que tenham entendimento suficiente para considerá-lo sem assumir e sem aceitar qualquer responsabilidade perante esses terceiros.

Rio de Janeiro 14, dezembro de 2016.

ERNST & YOUNG
Auditores Independentes S.S.
CRC-2SP015199/O-6

Francesco Bottino

Francesco Bottino
Sócio