Auditorias de Conformidade ICP Brasil e Webtrust - Autoridades Certificadoras

CERTFORUM 2023

Palestrantes: Fabricio Stallone e Felipe Berge

EY
Building a better working world

The better the question. The better the answer.
The better the world works.

Sumário

1 Introdução

2 Auditorias ICP Brasil

3 Auditorias Webtrust

4 Exemplo de Abordagem

Introdução

- **Auditorias ICP-Brasil**

a. As auditorias no âmbito ICP-Brasil têm como base a avaliação da conformidade dos Prestadores de Serviço de Certificação à luz dos critérios definidos pelo Instituto de Tecnologia da Informação (ITI) por meio de Adendos e Documentos Principais disponíveis em seu sítio eletrônico;
b. Conforme previsto em DOC-ICP-08 do Instituto Nacional de Tecnologia da Informação (ITI), as auditorias podem ser classificadas em:

✓ **Pré-operacionais** – realizadas previamente ao início das atividades do Prestador de Serviço de Certificação;
✓ **Operacionais** - realizadas a partir do primeiro ano civil seguinte à data da publicação no DOU do credenciamento do PSCert.

- **Auditorias Webtrust**

a. O programa Webtrust para Autoridades Certificadoras foi desenvolvido com o intuito de fornecer maior confiança dos consumidores na Internet como um veículo para a condução do comércio eletrônico e para aumentar a confiança dos consumidores na aplicação da tecnologia PKI.
b. O Programa atualmente é gerido pela CPA Canada, entidade igualmente responsável pela emissão dos selos de Webtrust (Webtrust for CA, Code Signing, SSL Baseline, SSL EV) após conclusão de análise e aprovação de relatório não qualificado emitido por empresa de auditoria independente com base nos guias práticos disponibilizados pela CPA Canada em seu sítio eletrônico.

Certification Authorities WebTrust | Certification Authorities WebTrust BR - SSL | Certification Authorities WebTrust Extended Validation | ICP Brasil

Auditorias ICP-Brasil

Exemplos de Processos de Autoridade Certificadora Definidos em Mapa de Processos ADE-ICP-08.E v4.3

Manter Credenciamento de AC

- Manter Requisitos de Manutenção de Credenciamento;
- Manter Condições Fisco-Tributárias e Econômico-Financeiras;
- Manter Contrato de Seguro;
- Manter Histórico de Agentes de Registro;
- Manter e Cumprir Política de Segurança;
- Comunicar Mudanças Operacionais e Violação de Normas;
- Regularizar Não Conformidades Identificadas;

Credenciar e Manter Entidades Operacionalmente Vinculadas

- Auditar Entidades Operacionalmente Vinculadas;
- Observar Procedimentos de Credenciamento e Extinção De Entidades Operacionalmente Vinculadas;
- Manter Credenciamento de Entidades Operacionalmente Vinculadas

Fases do Ciclo de Vida de Certificados Digitais

- Registrar Solicitação (Ex Emissão e Revogação de Certificados)
- Tratar Validação (Ex. Identificação e Cadastramento de Indivíduos)
- Processar Solicitação de Certificado (Ex. Envio de Solicitação à AC via VPN ou SSL, Timeout de Sessão de Aplicativo)
- Emitir Certificados (Ex. Padrão de Certificado, Algoritmo Criptográfico, Módulo Criptográfico)
- Emitir LCR (Ex. Frequência, Modelo)
- Tratar Revogação (Ex. Prazo, Condições para Revogação)
- Gerenciar IDN (Ex. Geração, Armazenamento e Monitoramento)

Manter Publicação

- Manter DPC, PC e PS (Ex. Alterações, Requisitos e Estrutura)
- Manter Repositório (Ex. Disponibilidade);
- Manter Publicação de LCR (Ex. Frequência de Publicação da LCR)

Auditorias ICP-Brasil

Exemplos de Processos de Autoridade Certificadora Definidos em Mapa de Processos ADE-ICP-08.E v4.3

Manter Sítio de Contingência

- Manter Integridade dos Dados (Ex. Transporte de Chaves, Recursos de VPN para troca de Informações);
- Ativar Sítio de Contingência (Ex. Testes Periódicos; Prazo p/ Ativação);
- Ativar Retorno ao Sítio Principal (Ex. Testes Periódicos);
- Manter Infraestrutura e Segurança Lógica (Ex. Espelhamento entre Ambiente Principal e de Contingência);

Manter Segurança da Informação

- Manter Inventário de Ativos;
- Manter Análise de Risco e Plano De Continuidade Do Negócio – PCN. (Ex. Incidentes e Revisão de PCN);
- Manter Documentos Armazenados e Classificados (Ex. Classificação de Informações);

Manter Sistemas Aplicativos

- Manter Sistemas de Informação (Ex. Documentação de Sistemas, Cópia de Segurança e Avaliação Periódica de Vulnerabilidades);
- Manter Sistema de AC (Ex. Parâmetros de Segurança, Controle de Acesso);
- Manter Base de Dados (Ex. Backup de Dados; Tráfego de Dados Seguro)

Manter Segurança Lógica e Rede

- Manter Sistemas Básicos (Ex. Homologação de Equipamentos, Testes em Ambiente de Homologação)
- Manter Equipamentos Protegidos de Ameaças; (Ex. IDS, Firewall e Antivírus)
- Manter Logs e Trilhas de Auditoria (Ex. Iniciação/Desligamento de Sistema de Certificação)

Auditorias ICP-Brasil

Exemplos de Processos de Autoridade Certificadora Definidos em Mapa de Processos ADE-ICP-08.E v4.3

Manter Segurança Lógica e Rede (Cont.)

- Manter Cópias de Segurança e Restauração; (Ex. Backup e Restore)
- Manter Controles de Acesso a Rede; (Ex. Firewall; IDS; Avaliação de Eventos de Segurança)
- Manter Controle de Acesso Lógico (Ex. Parâmetros de Senha; Concessão de Acesso)

Manter Infraestrutura

- Manter Equipamentos de Computação (Ex. Certificação Módulo Criptográfico)
- Manter Controle de Acesso Físico (Ex. Regras de Concessão, Revogação e Monitoramento de Acesso à Infraestrutura)
- Manter Ar Condicionado
- Manter Energia Elétrica (Ex. Características de Instalação)
- Manter Sistema de Combate a Incêndio (Ex. Detecção e Extinção)

Manter Recursos Humanos

- Admitir Pessoas (Ex. Due Diligence)
- Manter Capacitação de Pessoas; (Ex Treinamentos de PS, Sistemas, Segurança da Informação)
- Avaliar Desempenho;
- Suspender, Movimentar e Desligar Pessoas (Ex. Desligamento)

Avaliação de Entidades Operacionalmente Vinculadas

- Verificar em Mapa de Processos os Que São Cabíveis a Cada Natureza de Entidade (Ex. ACT, PSBIO, PSC)

Auditorias Webtrust

Princípios Definidos nos Guidelines do Webtrust (Ex. CA, CS, SSL e SSL EV)

Webtrust for CA

- Princípio 01: Divulgação das Práticas de AC (Ex. Divulgação de PC e DPC Conforme Requisitos De RFC Vigentes e Aplicáveis)
- Princípio 02: Gerenciamento de Práticas de Negócio da AC (Ex. Gerenciamento de PC; (Ex. Gerenciamento de PC e DPC Conforme Requisitos De RFC Vigentes e Aplicáveis)
- Princípio 03: Controles de Ambiente de Negócio da AC (Ex. Classificação e Gerenciamento de Ativos, Segurança de Pessoal, Segurança Física de Ambientes, Gestão de Mudanças, Gestão de Operações (Backup, PCN)
- Princípio 04: Gerenciamento do Ciclo de Vida das Chaves de AC (Ex. Geração e Utilização de Chaves)
- Princípio 05: Gerenciamento do Ciclo de Vida das Chaves de Usuários Finais (Ex. Gerenciamento de ICC (Ex. Transporte e Personalização))
- Princípio 06 – Gerenciamento de Ciclo de Vida de Certificado (Ex. Registro de Usuário (Ex. Verificação de Identidade), Emissão de Certificado (Ex. Layout de Certificado))

Webtrust for CA (Cont.)

- Princípio 07: Gerenciamento de ACs Subordinadas e Certificados Cruzados. (Ex. Gerenciamento dos Certificados das ACs Subordinadas)

Webtrust SSL

- Princípio 01: Divulgação e Gerenciamento das Práticas de AC (Ex. Divulgação e Gerenciamento de PC e DPC - Conforme Requisitos De RFC Vigentes e Aplicáveis)
- Princípio 02: Integridade de Serviço SSL (Ex. Geração de Chaves, Perfil de Certificado, Requisição, Emissão e Revogação de Certificado)
- Princípio 03 : Segurança de Ambiente da AC (Ex. Controles de Acessos Físico e Lógico, Gestão de Mudanças e Gestão de Operações)
- Princípio 04: Requisitos de Segurança de Rede e de Sistema de Emissão de Certificados.

Auditorias Webtrust

Princípios Definidos nos Guidelines do Webtrust (Ex. CA, CS, SSL e SSL EV)

Webtrust SSL EV

- Princípio 01: Divulgação e Gerenciamento das Práticas de AC (Ex. Divulgação e Gerenciamento de PC e DPC - Conforme Requisitos De RFC Vigentes e Aplicáveis)
- Princípio 02: Integridade de Serviço SSL EV (Ex. Geração de Chaves, Perfil de Certificado, Requisição, Emissão e Revogação de Certificado)

Webtrust CS

- Princípio 01: Divulgação e Gerenciamento das Práticas de AC (Ex. Divulgação e Gerenciamento de PC e DPC - Conforme Requisitos De RFC Vigentes e Aplicáveis)
- Princípio 02: Integridade de Serviço CS (Ex. Geração de Chaves, Perfil de Certificado, Requisição, Emissão e Revogação de Certificado)
- Princípio 03: Integridade de Serviço CS EV (Ex. Geração de Chaves, Perfil de Certificado, Requisição, Emissão e Revogação de Certificado)

Webtrust CS (Cont.)

- Princípio 04: Requisitos de Segurança de Rede e de Sistema de Emissão de Certificados.

Exemplos de Auditoria Webtrust

- Point in Time: Avaliação de Adequabilidade de DPC, PC, PS, Normativos Internos e Desenho dos Controles Implementados pela AC em Atendimento aos Requisitos Definidos no Programa Webtrust.
- Period of Time: Avaliação de Adequabilidade de DPC, PC, PS, Normativos Internos, bem como Desenho e Operação dos Controles Implementados pela AC em Atendimento aos Requisitos Definidos no Programa Webtrust durante um período de tempo específico. (Mínimo de 2 Meses e Máximo de 12 Meses)

Exemplo de Abordagem

Modelo de Abordagem Técnica em Trabalhos de Asseguração.

Agradecimento e Informações de Contato

Agradecemos a todos pela atenção e encarecidamente ao Instituto de Tecnologia da Informação (ITI) pelo convite. Em tempo, disponibilizamos abaixo algumas informações de contato caso queiram encaminhar dúvidas ou comentários acerca da presente Palestra.

Informações de Contato:

- ✓ Telefone: **+55 11 2573 3000**
- ✓ Website: https://www.ey.com/pt_br

Fabricio Stallone

EY Partner – Technology Risk
fabricio.stallone@br.ey.com

Felipe Berge

EY Manager – Technology Risk
felipe.berge@br.ey.com