Serasa information:

1. Sub-CA Company Name
   Serasa S.A.

2. Sub-CA Corporate URL
   http://www.serasa.com.br/us/index.htm (english version)

3. Sub-CA cert download URL
   http://publicacao.certificadodigital.com.br/suporte/serasacdv1.cer

4. General CA hierarchy under the sub-CA.
   Already provided by ITI.

5. Sub-CA CP/CPS Links
   http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a1.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a2.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a3.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-a4.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s1.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s2.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s3.pdf
   http://publicacao.certificadodigital.com.br/repositorio/pc/politica-s4.pdf

6. The section numbers and text (in English) in the CP/CPS that demonstrate that reasonable measures are taken to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of our Mozilla CA certificate policy.
   - domain ownership/control

3.1.11.2. Procedures for identification of equipment or application
3.1.11.2.1. For licenses to use equipment or application URL in the Common Name field must be verified if the applicant holds the certificate of registration of the domain name from the competent body, or has permission of the holder of the domain to use that name. In this case must be presented related documentation (term of authorization for use of domain or similar) duly signed by the holder of the domain. (extract from http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf)

   - email address ownership/control

There is no reference in CP/CPS

- digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate

There is no reference in CP/CPS

7. Identify if the SSL certificates chaining up to the sub-CA are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates.
   - DV: Organization attribute is not verified. Only the Domain Name referenced in the certificate is verified to be owned/controlled by the subscriber.
   - OV: Both the Organization and the ownership/control of the Domain Name are verified.

There is no DV or OV certificates in this chain.

8. Review the CP/CPS for Potentially Problematic Practices. Provide further info when a potentially problematic practice is found.

We detected that only “Delegation of Domain / Email validation to third parties” is a potentially problematic practice. InBrazil, Registration Authorities (RA) perform such functions.

Acording to ICP-Brasil regulation, RA contract and conduct their own audit process, but the audit reports are presented to the related CA.

Audit process is regulated by ICP-Brasil as below:

a) audit companies request a registration to operate in ICP-Brasil infra-structure
b) RA and CA contract the audit company and presents to ITI the audit schedule
c) ITI approves the audit schedule
d) RA or CA send the audit report to ITI
e) ITI analizes the audit report

9. If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of our Mozilla CA certificate policy.

Serasa contract and conduct their own audit process .

Audit process is regulated by ICP-Brasil as below:

f) audit companies request a registration to operate in ICP-Brasil infra-structure
g) RA and CA contract the audit company and presents to ITI the audit schedule
h) ITI approves the audit schedule
i) RA or CA send the audit report to ITI
j) ITI analizes the audit report

10. Provide information about the CRL update frequency for end-entity certificates. There should be a statement in the CP/CPS that the sub-CA must follow to the effect that the

CRL for end-entity certs is updated whenever a cert is revoked, and at least every 24 or 36 hours.

4.4.9.2. The maximum frequency allowed for the issuance of CRL for the certificates of end users is 6 hours.

(extract from http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf)