Plano de Continuidade de Negócios de Autoridades de Registro e Instalações Técnicas

[JUNHO/2019]

- Índice –

1. Introdução

Este Plano de Continuidade de Negócios (PCN) contém as **políticas seguidas pelas Autoridades de Registro e Instalações Técnicas** na eventualidade de uma interrupção nas suas operações de Negócios e que, como consequência, seja necessária a declaração e operação em contingência - *situação excepcional decorrente de um desastre (Fonte: Site ITI – Glossário).*

O objetivo principal deste PCN é apresentar diretrizes para que o responsável da Autoridade de Registro e/ou Instalação Técnica saiba como atuar em situações de emergência.

Os cenários previstos para a utilização deste PCN são:

- Fraude ou Erro no Processo de Validação e Emissão de Certificados;
- Impossibilidade de Revogação de Certificados pela AR/IT.

IMPORTANTE: É obrigatório que exista uma cópia impressa deste documento, armazenada em local seguro fora da AR/IT, em poder do respectivo responsável.

2. Estrutura do PCN

O Plano de Continuidade de Negócios está organizado em estrutura hierárquica contendo duas fases:

- **Fase Resposta:** iniciada imediatamente após a ocorrência de um dos cenários descritos na Seção 4 "Procedimentos – Fase Resposta" adiante. Somente a ocorrência destes eventos não caracteriza uma situação de contingência.

  Nesta fase, as seguintes ações podem ser tomadas:
  - Avaliação dos danos;
  - Estimativa do prazo de retorno;
  - Notificação do problema à área de **Gestão Operacional da AC**;
  - Tomada de decisão, declaração ou não da contingência.

  Uma vez declarada a contingência é iniciada a fase seguinte, sendo acionado então o plano correspondente.

- **Fase Contingência:** iniciada imediatamente após declarar a contingência. O responsável deve seguir as instruções descritas na Seção 5 "Procedimentos – Fase Contingência".

3. Áreas Envolvidas e Responsabilidades

As áreas envolvidas na contingência de uma AR/IT são:

- A própria AR/IT (por meio do seu Responsável Operacional);
- Gestão Operacional da AC;
- Suporte Corporativo AC (realizado pelo Prestador de Serviços de Suporte - PSS);
- Departamento de Segurança do PSS.

Ao Responsável Operacional da AR/IT caberá:

a) Prestar atendimento aos clientes que se encontrem afetados pela contingência;
b) Atuar como ponto inicial de informações;
c) Reportar-se à área de Gestão Operacional da AC, conforme previsto neste PCN;
d) Acionar o Suporte Corporativo AC, quando previsto neste PCN;
e) Realizar os procedimentos necessários à apuração dos fatos e à realização das operações visando à recuperação das atividades, conforme orientações da Gestão Operacional da AC e do Suporte Corporativo AC;
f) Elaborar relatórios e encaminhá-los à área de Gestão Operacional da AC.

À Gestão Operacional da AC caberá:

a) Atuar como ponto focal, recebendo as informações sobre o ocorrido, extensão dos danos e prazo estimado de retorno;
b) Declarada a contingência, coordenar todas as atividades dos times operando em contingência;
c) Interagir com o Suporte Corporativo AC, se necessário;
d) Acionar o Departamento de Segurança do PSS, quando necessário;
e) Encerrar todas as atividades da contingência;
f) Avaliar toda a execução da contingência;
g) Propor alterações nas estratégias de recuperação;
h) Solicitar aos responsáveis pelo desenvolvimento e manutenção as correções/alterações nos planos, em prazos aceitáveis;
i) Certificar-se de que os responsáveis pelo desenvolvimento e manutenção efetuaram as correções/alterações nos planos, nos prazos solicitados.

Ao Suporte Corporativo AC caberá:

a) Prestar atendimento às solicitações da área de Gestão Operacional da AC.

Ao Departamento de Segurança do PSS caberá:

a) Atuar como segunda instância na solução de problemas, quando acionado pela Gestão Operacional da AC ou pelo Suporte

Corporativo AC.

4. Procedimentos – Fase Resposta

4.1 Fraude ou Erro no Processo de Validação e Emissão de Certificados

Time: Resposta à emergência
Responsável: Autoridade de Registro/Instalação Técnica (Responsável Operacional)

- Em caso de Suspeita de fraude ou erro no processo de validação:
    - Identificar fonte da suspeita – Auditoria Interna ou Fonte Externa;
    - Realizar processo de identificação da "Não Conformidade" do certificado sob suspeita de fraude;
- Se não houver nenhuma evidência de fraude ou erro no certificado, encerrar a investigação mediante registro e envio do **Anexo B – Formulário - Fraude ou Erro na geração de certificados** à área de Gestão Operacional da AC;
- Se confirmada a ocorrência de fraude ou erro, notificar, via e-mail, a área de Gestão Operacional da AC e acionar a Fase indicada na Seção 5.1 adiante;
- No caso de Instalação Técnica, notificar também o responsável da Autoridade de Registro à qual está subordinada.

4.2 Impossibilidade de Revogação de Certificados pela AR/IT

Time: Resposta à emergência
Responsável: Autoridade de Registro/Instalação Técnica (Responsável Operacional)

- Identificar a real necessidade de revogação do certificado;
- Se não for confirmada a necessidade de revogação, registrar e enviar essa ocorrência no **Anexo D – Formulário – Impossibilidade de Revogação de certificados pela AR/IT** à área de Gestão Operacional da AC;
- Se confirmada a necessidade de revogação emergencial do certificado, acionar a Fase de Contingência deste plano

"Impossibilidade de Revogação de Certificados pela AR/IT" (Seção 5.2);

- No caso de Instalação Técnica, notificar também o responsável da Autoridade de Registro à qual está subordinada.

5. Procedimentos – Fase Contingência

5.1 Fraude ou erro no Processo de Validação e Emissão de Certificados

Time: Resposta à emergência
Responsável: Área de Gestão Operacional da AC e Autoridade de Registro/Instalação Técnica (Responsável Operacional)

- O Responsável Operacional da AR/IT deve documentar todos os passos (bem como os horários das ocorrências) dessa fase, incluindo as justificativas para revogação do certificado no **Anexo B - Formulário – Fraude ou Erro na geração de certificados** adiante;

- O Responsável da área de Gestão Operacional da AC deve autorizar a revogação e orientar o Responsável Operacional da AR/IT quanto ao procedimento para revogar o certificado do cliente;

- A AR/IT mantém contato com o cliente afetado e comunica a revogação do certificado (e-mail, telefone, fax) o mais rápido possível;

- Após a revogação, o Responsável Operacional da AR/IT consulta a "Lista de Certificados Revogados"(LCR) para confirmar a publicação do certificado revogado;

- Caso o certificado tenha sido revogado indevidamente, o Responsável Operacional da AR/IT deve entrar em contato com o cliente afetado (e-mail, fax, telefone) para comunicar a necessidade de emissão de novo certificado, sem ônus para o mesmo. Deve ser concedida prioridade para a emissão desse certificado.

- A AR/IT deve armazenar uma cópia do Anexo B e enviar uma outra cópia para a Gestão Operacional da AC; esse documento servirá como evidência de execução do PCN em futuras auditorias que a AR/IT possa sofrer.

5.2 Impossibilidade de Revogação de Certificados pela AR/IT

Time: Resposta à emergência
Responsável: Área de Gestão Operacional da AC e Autoridade de Registro/Instalação Técnica (Responsável Operacional)

- O Responsável Operacional da AR/IT deve documentar todos os passos (bem como os horários das ocorrências) dessa fase, incluindo as justificativas para revogação do certificado no **Anexo D - Formulário – Impossibilidade de Revogação de certificado pela AR/IT** adiante, colhendo as respectivas assinaturas;

- Depois da identificação do titular do certificado, a AR/IT deve solicitar que o mesmo assine manualmente, de forma semelhante ao documento de identificação apresentado, duas vias do **Anexo C - Solicitação de Revogação de Certificado Digital** adiante (uma via para o cliente e uma via para ser arquivada na AR/IT);

- O Responsável Operacional da AR/IT deve notificar, via e-mail, a área de Gestão Operacional da AC sobre a ocorrência, anexando os formulários mencionados acima;

- O Responsável da área de Gestão Operacional da AC deve solicitar ao Suporte Corporativo AC que realize a revogação do certificado no sistema, encaminhando a notificação da AR/IT, com a sua autorização para este procedimento. Caso o Suporte Corporativo AC esteja impossibilitado de efetuar a revogação por qualquer motivo, a área de Gestão Operacional da AC deve acionar de imediato a Gerência de Segurança do PSS.

- Após a revogação, o Responsável da área de Gestão Operacional da AC deve consultar a LCR para confirmar a revogação do certificado;

- O Responsável da área de Gestão Operacional da AC deve comunicar à AR/IT, via e-mail, que a revogação foi executada com sucesso;

- Caso não receba confirmação em até 48 horas, a AR/IT deve solicitar da Autoridade Certificadora a confirmação que o certificado revogado foi publicado na LCR;

- A AR/IT deve registrar e armazenar de maneira correta os documentos manipulados durante esse procedimento, que servirão como evidência de execução do PCN em futuras auditorias que a AR/IT possa sofrer.

- A AR/IT deve armazenar a via física do **Anexo C - Solicitação de Revogação de Certificado Digital** assinada pelo titular do certificado no respectivo dossiê, juntamente com cópia do **Anexo D - Formulário – Impossibilidade de Revogação de certificado pela AR/IT**

Anexo A – Estrutura dos Times

Resposta a emergências

Responsável Operacional da AR

Agente de Registro designado como responsável operacional da AR/IT ou seu substituto.

Gestão Operacional da AC:

E-mail: auditoria@redeicpbrasil.com.br

Suporte Corporativo AC

E-mail: suporte.ac@certisign.com.br

Departamento de Segurança do PSS:

E-mail: seguranca@certisign.com.br

Anexo B – Formulário - Fraude ou Erro na geração de certificados

Responsável da AR/IT:		
Data da Ocorrência:	**Hora Início:**	**Hora Final:**
Autoridade de Registro/Instalação Técnica:		
Nome do Cliente:		
Tipo de Certificado:	**CPF / CNPJ:**	
Registros / Justificativas que evidenciam a fraude / erro		
Assinatura do Responsável da AR/IT		

NOTA: É importante ressaltar nas Justificativas para a revogação do Certificado quais foram as ações tomadas levando em consideração os horários em que essas ocorreram.

As Justificativas que evidenciam a fraude / erro na geração de certificados devem ser listadas, lembrando que todas as evidências devem ser armazenadas.

Anexo C - Solicitação de Revogação de Certificado Digital

SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DIGITAL

Nome: _____

RG nº _____ CPF nº _____

Tipo de Certificado: _____

O subscritor acima qualificado, doravante denominado TITULAR, declara, para todos os fins legais, ter solicitado à AUTORIDADE CERTIFICADORA – **[NOME DA AC emissora do certificado]** – a revogação do certificado identificado acima.

NOME DO TITULAR DO CERTIFICADO

Dados do Funcionário da Autoridade de Registro/Instalação Técnica:

Nome: _____

RG nº _____ CPF nº _____

Cargo ou Nº funcional:_____

NOTA: Esta Solicitação de Revogação de Certificado Digital faz parte do Plano de Continuidade de Negócios da AR/IT e deve ser utilizada somente nos casos previstos no item 5.2 deste documento.

Anexo D – Formulário - Impossibilidade de Revogação de Certificados pela AR/IT

Responsável da AR/IT:		
Data da Ocorrência:	**Hora Início:**	**Hora Final:**
Autoridade de Registro/Instalação Técnica:		
Nome do Cliente:		
Tipo de Certificado:	**CPF / CNPJ:**	
Registros / Justificativas que evidenciam a impossibilidade de revogação pela AR/IT e procedimentos adotados para contorná-la		
Assinatura do Responsável da AR/IT		

NOTA: É importante ressaltar nas Justificativas para a revogação do Certificado quais foram as ações tomadas levando em consideração os horários em que essas ocorreram.

DECLARAÇÃO

Declaro estar ciente de todo o conteúdo do Plano de Continuidade de Negócios (PCN).

Declaro, ainda, que a guarda e utilização do referido documento será feita de acordo com as instruções contidas na Legislação ICP-Brasil (DOC-ICP-03.01 - Características Mínimas de Segurança para as ARs da ICP-Brasil), estando ciente de que o PCN deverá ser impresso em duas vias, devendo a primeira cópia ser armazenada em local de fácil acesso aos Agentes de Registro dentro do ambiente da AR/IT, e a segunda armazenada, em local seguro fora do ambiente da AR/IT.

CLAUDIO ROTAVA:38683326934

Assinado de forma digital por CLAUDIO ROTAVA:38683326934
Dados: 2019.06.14 11:15:44 -03'00'

Assinatura do responsável legal da AR/IT