GESTÃO CENTRALIZADA DO SISTEMA EPROTOCOLO

COMUNICADO 03/2026

Atualização Obrigatória da Cadeia Certificadora da Central de Segurança – Integrações eProtocolo

Para: Gestores de TI, Administradores de Sistemas e Equipes Técnicas responsáveis por aplicações integradas ao eProtocolo

Assunto: Atualização obrigatória de certificado digital e cadeia de certificação

Prazo limite para aplicação: 03/11/2026 (impreterivelmente)

Informamos a necessidade mandatória de atualização do certificado digital e de sua respectiva cadeia certificadora da **Central de Segurança**, serviço essencial para a comunicação e autenticação de sistemas integrados ao **eProtocolo**.

O novo certificado digital, acompanhado da cadeia completa de certificação concatenada, encontra-se disponível no arquivo anexo a este comunicado.

1. Escopo e Responsabilidade de Atualização

A falta de atualização impedirá o estabelecimento de conexões seguras (TLS/SSL), resultando na indisponibilidade imediata das integrações com o eProtocolo:

- **Sistemas hospedados no Datacenter da Celepar:** a intervenção técnica será realizada diretamente pela equipe da Gerência de Tecnologia da Informação (GTI);
- **Sistemas externos (fora do Datacenter da Celepar):** a atualização técnica nos servidores de aplicação e *truststores* deve ser realizada **obrigatoriamente pelas equipes técnicas responsáveis por cada sistema** até o prazo limite de **03/11/2026**.

2. Impactos e Erros Decorrentes da Não Atualização

Caso a cadeia de certificação não seja instalada até a data informada, a comunicação entre os sistemas será interrompida, gerando falhas operacionais e mensagens de erro como:

- Falhas em chamadas de API/Web Services: `SSLHandshakeException`, `SSL certificate problem`, `HTTP 500 (Internal Server Error)` ou `HTTP 502 (Bad Gateway)`;
- Falhas em interfaces web/navegadores: "Certificado não confiável", "Sua conexão não é privada" (Google Chrome / Microsoft Edge) ou "Alerta: Risco de segurança à frente" (Mozilla Firefox).

3. Validade e Cronograma de Segurança

- **Validade do certificado atual:** 6 meses a partir da emissão;
- **Redução progressiva de ciclos:** em conformidade com as diretrizes globais de segurança da informação e padrões de mercado, o tempo de validade dos certificados será encurtado gradualmente (estimativa de redução para aproximadamente 100 dias no próximo ano e cerca de 45 dias até o final de 2027);
- **Automação:** a Celepar já avalia a implementação de mecanismos de renovação automatizada para simplificar manutenções futuras.

4. Ações Necessárias

1. Baixar o arquivo anexo contendo o certificado e as cadeias intermediária e raiz concatenadas;
2. Importar os certificados na base de certificados confiáveis (*truststore*/repositório do servidor) do ambiente de integração;
3. Realizar testes de comunicação com o eProtocolo em ambiente controlado e garantir a publicação em produção antes de **03/11/2026**.

Dúvidas e suporte técnico para validação das cadeias devem ser encaminhados aos canais habituais de atendimento da Celepar.