

**RESULTADO DA POC/DILIGÊNCIA DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO - PE 26/2024 -
EMPRESA BENNER**

DATA: 20/12/2024

Horário: 09:00 às 14:40

LOCAL: ESCOLA JUDICIAL DO TRT3 - SALA 01.

**RESULTADO APURADO -
REQUISITOS DE SEGURANÇA DA
INFORMAÇÃO**

Dos requisitos de segurança, diligenciados durante a prova de conceito/POC do sistema ofertado pela empresa Benner, ocorrida no dia 20/12/2024 nas instalações da Escola Judicial do TRT3, das 09:00 às 14:40, verificou-se que dos dezenove requisitos de segurança da informação auditados, três deles não foram atendidos, conforme destacado abaixo:

- **Requisito:** Publicar url do Prometheus Exporter para ser incluída no monitoramento do TRT3. No caso de aplicações Java, existe o JMX Exporter.

Justificativa do não atendimento: A empresa Benner não apresentou uma URL no formato prometheus.

- **Requisito:** Assegurar que todos os recursos e informações de logs sejam protegidos contra alterações ilegítimas e acessos não autorizados.

Justificativa do não atendimento: A habilitação de logs é realizada por tabela de forma lógica, o que, em análise inicial, permitiria um invasor desativar o log, executar procedimentos indevidos e reativar o log. Em primeira análise, uma solução para resolver esse achado seria garantir que alterações na própria habilitação de logs sejam logadas.

- **Requisito:** Todos os sistemas e seus componentes da CONTRATADA devem:

"Manter registros em sistema que permitam auditar as ações executadas através de logs dos seguintes eventos:

"Tentativas de acesso ao sistema, aceitas e bloqueadas, identificando minimamente: usuário, hora e data do login e logout e IP da requisição.

Ações realizadas no sistema, identificando minimamente: usuário executor, data e hora, ação realizada, dono do dado (quando fizer sentido), IP da requisição a partir da qual a ação foi realizada.

As operações que realizam modificações no banco de dados, registrando minimamente: usuário, data e hora da operação, tabela alterada, operação realizada (inclusão, exclusão, alteração), dados alterados (antigo e novo), IP da requisição a partir da qual a ação foi realizada.

Justificativa do não atendimento: O fornecedor apresentou que não é registrado o IP da requisição, mas sim o IP interno de componentes da aplicação.

CONCLUSÃO:

Os requisitos atendidos representam **84,21% (oitenta e quatro por cento e vinte e um décimos)** do total de requisitos de segurança, o que enseja a **classificação** da empresa para a próxima fase da POC, que avaliará o atendimento dos requisitos funcionais e técnicos ainda não avaliados.

Belo Horizonte, 20 de dezembro de 2024

Luiz Felipe Campos Fernandes

Raphael Eustaquio Alves Vilela