1

ATA DE REUNIÃO	
POC/DILIGÊNCIA DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO - PE 26/2024 - EMPRESA REZEK	
DATA: 05/12/2024	**Horário**: 09:30 às 18:25
LOCAL: ESCOLA JUDICIAL DO TRT3 - SALA 01.	

PARTICIPANTES E ASSINATURA

TRT3 -

LUIZ FELIPE CAMPOS FERNANDES

ROBSON Gomes Ferreira

MÁRCIA CAROLINA MARRA DE OLIVEIRA

RAPHAEL EUSTAQUIO ALVES VILELA

ISABEL GOMES BARBOSA

RODNER RODRIGUES MADUREIRA DE ALMEIDA

GRAZIELLA MELGAÇO PIRES FURTADO DE MENDONÇA

GRUPO FÁCIL

BRUNO SANTOS DA MOTTA PRADO

ALEX GONÇALVES SOARES

ROBERTO GUILHERME SPELLER

PEDRO ARAÚJO MEDEIROS

SYDLE

THAMYRES FERNANDA SIQUEIRA

PAUTA

1) Diligência/POC dos itens de segurança dos requisitos técnicos do edital PE 26/2024, itens 18 a 45.Há itens que conforme planilha, não foram objetos de diligência.

Itens avaliados

Manter e aplicar uma "Política de segurança da informação, privacidade e proteção de dados pessoais"; que esteja em conformidade com as normas ISO 27001/27002 e 27701.

Plano de auditoria: para o item manter : Deve ser apresentada política de segurança da informação conjuntamente com a política de privacidade e de dados pessoais (em um mesmo documento ou apartado). Para o item aplicar, deverá ser comprovada a aplicação dos controles contidos nas políticas.

O grupo Fácil, por meio da apresentação do Sr. Bruno Prado, exibiu a política de segurança da informação.Observamos prontamente que a política de segurança da informação é datada de 23/06/2023 com revisão anual, contudo, a norma deveria ter sido revisada em 2024 após um ano de sua publicação.A política registra que há auditorias, mas, não foi apresentada nenhuma evidência nesses sentido, sendo inclusive, confirmado pelo sr. Bruno que não havia tais documentos.

Observou-se que não consta na política controle de acesso lógico e físico (para seus centro de processamento de dados internos), ou política de senhas, itens constantes nas melhores práticas preconizadas pela ISO27001:2022

O grupo Fácil irá nos enviar até às 23:59 do dia 05/12/2024, as políticas apresentadas neste tópico e aquelas complementares, como por exemplo, mas não se limitando: gestão de riscos,incidentes,desenvolvimento seguro de software, entre outras que façam parte do seu sistema de gestão de segurança da informação e proteção de dados pessoais.

Não existe uma política para gestão de senhas, não tem uma politica de gestão de acesso

Após diversos questionamentos sobre a política, o senhor Bruno registra que não possui certificação ISO.

Os presentes fizeram pausa para café às 10:51 e retornaram às 11:15.

Manter e testar anualmente o "Plano de Recuperação de Desastres".

Plano de auditoria : Deve ser apresentado o plano documental e o teste evidenciado com seu resultado, de pelo menos do ano de 2023 e 2024. Tudo devidamente documentado.
A empresa informou na planilha : Como o ambiente é NUVEM, diariamente recriamos as diversas estruturas que compõem a arquitetura."

Foi apresentado pelo sr. Bruno o plano de recuperação de desastre na AWS (sem data e sem aprovação formal interna).Bruno explica que data center principal é em North Virginia na AWS.Os backups dizem ser replicados em regiões geográficas distintas e são armazenados por 5 anos. São feitos backup lógicos

Itens avaliados
diariamente. Bruno explica que não tem evidências dos teste do plano de contingência pois na sua arquitetura não comporta promover o banco de dados de standby em produção.
Publicar, manter e garantir a execução de uma "Política de Senhas Segura". O senhor Bruno explica que não dispõe de documento de política de senhas seguras publicada, internamente, o controle é realizado pelo serviço de diretórios e na AWS pelo IAM. Já no sistema FACPLAN será demonstrado após o almoço.Sr.Bruno solicita enviar o print da configuração do Serviço de Diretório de até o final do dia (23:59).
Estabelecer plano e processo de reação a incidentes de segurança da informação e de proteção de dados pessoais. Foi apresentado o documento norma de gestão de Incidentes emitido em 14/11/2023, código NOR.GSI.002. Sr. Bruno informa que não há na norma de gestão de incidentes para o tema específico de proteção de dados pessoais, mas que no procedimento operacional há a previsão.Os incidentes são registrados no CRM.Há procedimento de gestão de vulnerabilidade que considera crítico o não tratamento de vulnerabilidades no SLA previsto. A norma está assinada. Foi apresentado o procedimento operacional padrão de gestão de incidentes. Luiz Felipe do TRT3 solicita o relatório de um incidente, preferencialmente de dados pessoais, podendo ser anonimizado.Caso não haja evidência que o sistema está apto a receber incidentes de dados pessoais, deverá ser demonstrado como o cliente faz o registro no CRM externamente. Pausa para almoço às 13:30 com retorno às 14:30.
Apenas realizar e aceitar requisições com criptografia de tráfego SSL/TLS em versão 1.2 ou superior, com certificado válido. Retorno do almoço às 14:35. Validado via tenable que a URL do sistema disponibilizada para teste (novowebplanpocfacplan.facilinformatica.com.br) está em conformidade com o requisito e que há certificado ativo: Output Copy Protocol Supported --- SSL 2.0 No SSL 3.0 No TLS 1.0 No TLS 1.1 No TLS 1.2 Yes TLS 1.3 Yes

Itens avaliados
A Contratada deve possuir um processo de gerenciamento de riscos e de vulnerabilidades de segurança da informação, visando a atualização constante dos componentes da solução. **A Contratada deve aplicar regularmente os patches de segurança das tecnologias adotadas na disponibilização da solução.** Sr. Bruno apresenta a norma de gestão de vulnerabilidade - NOR-GSI.001 de 22/06/2023 versão 1.0. O documento estabelece que deve haver uma estratégia de remediação baseada em risco documentada em um processo de remediação, com revisões mensais ou mais frequentes.Os patches devem ser aplicados de maneira automatizada a cada mês. Luiz do TRT3 solicita que seja demonstrada a varredura e aplicação de patches nos componentes no mês 08/2024 e 09/2024 para fins de apresentação de evidência.Solicita que sejam fornecidas evidência de identificação e tratamento de vulnerabilidade na aplicação, podendo ser um pentest. Foi apresentada uma política de análise de riscos que não está implantada, está em implantação, motivo pelo o qual o item não está em conformidade. Foi verificado via tenable que há uma versão de IIs crítica como componente da solução : IIS7.5 que deixou de ter suporte em Jan 2020, isso demonstra que o windows que hospeda a solução está desatualizado há muito tempo, demonstrando que o processo de aplicação de patches contido na política não é seguido.
Efetuar backup automático diário da base de dados em local seguro. **Ser protegidos por firewall.** **Ser protegidos por WAF (Web Application Firewall).** Sr. Bruno apresentou os backups diários tanto em dump no s3 quanto no RDS. No item firewall apresentou os security groups na AWS com filtros ativos,não possuindo o serviço de firewall da AWS em si. Em relação ao WAF existe uma regra chamada Regra-top-10-OWASP que está aplicada no albfacil loadbalancer.Tal regra está no modo count não tomando nenhuma ação. Segundo o sr. Bruno as ações são tomadas com base no monitoramento, mas em diligência observamos que tratam-se de milhões de requisições. Luiz Felipe do TRT3 solicitou comprovação de bloqueio do WAF para demonstrar que este está bloqueando acessos como um WAF deve comportar-se.
Publicar url do Prometheus Exporter para ser incluída no monitoramento do TRT3. No caso de aplicações Java, existe o JMX Exporter. Raphael solicitou ao Sr. Bruno que nos demonstre o endpoint de monitoramento.Raphael destaca que não foi apresentada a URL solicitada no requisito,contudo, existe um monitoramento em grafana e que

Itens avaliados
também poderia ser utilizado um component em ASP.NET para exportação dos dados em formato Prometheus.
As APIs disponibilizadas e utilizadas pela CONTRATADA devem estar restritas a acessos autenticados e autorizados. Raphael solicitou ao Sr. Bruno que nos demonstrasse como é implementado o controle.Bruno explicou que são realizados controles de acesso por usuário e seus respectivos papeis.Demonstrou a documentação de uma API da hi plataform (chatbot),contudo, Raphael solicitou que fosse demonstrada uma API do core da aplicação, sendo validado o requisito corretamente.
Por padrão, o usuário não deve possuir nenhum Perfil vinculado a ele. Em diligência no sistema, apurou-se que todo usuário tem um perfil vinculado, contudo,Raphael ponderou que pode ser aplicado um perfil sem autorização, aceitando o requisito. **Por padrão, o acesso às funcionalidades que não sejam públicas deve ser restrito.** Em diligência no sistema, apurou-se que o colaborador sem permissão não consegue acessar nenhuma funcionalidade não pública nos exemplos diligenciados, aceitando o requisito.
Disponibilizar os registros de log através de relatórios para usuários autorizados. Em diligência no sistema, apurou-se que há serviço de relatório disponibilizado via delphi. **Assegurar que todos os recursos e informações de logs sejam protegidos contra alterações ilegítimas e acessos não autorizados.** Sr. Bruno informou que os logs podem ser apagados via usuários do banco de dados. **Assegurar que quaisquer falhas no sistema não comprometam os registros de logs.** Em diligência no sistema verificou-se que o comprometimento do banco de dados inviabiliza o controle de logs e que usuários de banco de dados conseguem alterar os logs.De forma geral não foram identificados controles que garantam a integridade dos registros de logs. **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.** Em diligência no sistema, apurou-se que o ip apresentado no log é do guacamole que roda o Delphi, não demonstrado o IP de acesso da máquina do usuário do sistema.No relatório de tentativas de acesso não foi identificado o 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.**

Itens avaliados
Em diligência no sistema, apurou-se que o ip apresentado no log é do guacamole que roda o Delphi, não demonstrado o IP de acesso da máquina do usuário do sistema.Apenas dados configurados como dados pessoais geram registro de visualização no log. **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.** Em diligência no sistema, apurou-se que o ip apresentado no log é do guacamole que roda o Delphi, não demonstrado o IP do usuário.
Mascarar senhas e outros campos de entrada sensíveis na tela; Em diligências no sistema, apurou-se que campos sensíveis, como por exemplo senha, são mascarados. **O sistema deve impedir o acesso indevido a informações por usuários sem perfil de acesso necessário a determinadas classes de informação.** Em diligências no sistema, apurou-se que dados configurados como dados pessoais possuem autorização de acesso e registro de log que permite auditoria. O Sr. Bruno apresentou que os acessos de dados não classificados como pessoais são programáticos.
Contratação da solução na modalidade Software as a Service – modalidade de Software como Serviço, com infraestrutura operacional em nuvem e operações/funcionalidades para todos os usuários 100% (cem por cento) WEB. Tal item não é objeto de validação de segurança, contudo, apurou-se em diligência que a aplicação não é 100% web para todos os usuários, visto que as funcionalidades de de backoffice rodam em Delphi sobre um sistema de Acesso remoto RDP baseado no produto de software livre Guacamole.

Presentes conferiram e assinaram a ata. Ao final da reunião não houve nenhum apontamento dos presentes.

Rophael Vilela