TRIBUNAL DE CONTAS DO DISTRITO FEDERAL

CARGO 3: AUDITOR DE CONTROLE EXTERNO – ÁREA ESPECIALIZADA
ESPECIALIDADE TECNOLOGIA DA INFORMAÇÃO
ORIENTAÇÃO SISTEMAS DE TI

Prova Discursiva P_4 – Questão 1

Aplicação: 17/12/2023

PADRÃO DE RESPOSTA DEFINITIVO

2.1 COBIT 2019 – DSS05 – Serviços de Segurança Gerenciados

Descrição: processo do Domínio Entregar, Servir e Suportar (DSS) que visa proteger as informações da empresa para manter o nível de risco de segurança da informação aceitável para a empresa de acordo com a política de segurança. Estabelecer e manter funções de segurança da informação e privilégios de acesso. Realizar monitoramento de segurança.

Objetivo: minimizar o impacto comercial de vulnerabilidades e incidentes operacionais de segurança da informação.

Obs.: não deve haver decréscimo de nota caso o candidato não insira em sua resposta o domínio do processo.

2.2 ITIL 4 – Prática de gerenciamento de incidentes

Objetivo da prática: o objetivo da prática de gerenciamento de incidentes é minimizar o impacto negativo dos incidentes, restaurando a operação normal do serviço o mais rápido possível.

Definição de incidente: uma interrupção não planejada de um serviço ou redução na qualidade de um serviço.

2.3 OWASP – IDOR e *eavesdropping*

Referência insegura a objetos (insecure direct object references — IDOR). Os *bugs* do tipo IDOR permitem que invasores manipulem aplicativos através de uma referência insegura a objetos, como uma entrada a banco de dados, uma busca, etc. IDOR inseguras ocorrem quando um aplicativo fornece acesso direto a objetos com base na entrada fornecida pelo usuário. Como resultado dessa vulnerabilidade, os invasores podem ignorar a autorização e acessar recursos diretamente no sistema, como registros ou arquivos de banco de dados. Referências diretas inseguras a objetos permitem que invasores ignorem a autorização e acessem recursos diretamente, modificando o valor de um parâmetro usado para apontar diretamente para um objeto.

*Eavesdroppin*g: um ataque de espionagem ocorre quando um *hacke*r intercepta, exclui ou modifica dados transmitidos entre dois dispositivos. A espionagem, também conhecida como *sniffin*g ou *snooping*, depende de comunicações de rede inseguras para acessar dados em trânsito entre dispositivos.

Os riscos habituais da comunicação insegura estão relacionados com a integridade dos dados, a confidencialidade dos dados e a integridade da origem. A possibilidade de os dados serem alterados durante o trânsito, sem que a alteração seja detectável (por exemplo, através de um ataque *man-in-the-middle*) é um exemplo desse risco. A possibilidade de dados confidenciais serem expostos, aprendidos ou derivados pela observação das comunicações conforme elas acontecem (ou seja, espionagem) ou pela gravação da conversa conforme ela acontece e atacando-a mais tarde (ataque *offlin*e) também é um problema de comunicação insegura.

QUESITOS AVALIADOS

QUESITO 2.1

Conceito 0 – Não descreveu o processo nem o seu objetivo ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu, de maneira precária, apenas o processo OU apenas o objetivo.
Conceito 2 – Descreveu, de maneira precária, tanto o processo quanto o seu objetivo.
Conceito 3 – Descreveu de maneira satisfatória apenas o processo OU apenas o objetivo.
Conceito 4 – Descreveu de maneira satisfatória tanto o processo quanto o seu objetivo.

QUESITO 2.2

Conceito 0 – Não descreveu o objetivo da prática de gerenciamento de incidentes nem definiu incidentes ou o fez de forma totalmente equivocada.

Conceito 1 – Apenas descreveu, de maneira precária, o objetivo da prática de gerenciamento de incidentes OU apenas definiu incidentes de maneira precária.
Conceito 2 – Descreveu, de maneira precária, o objetivo da prática de gerenciamento de incidentes e definiu incidentes de maneira precária.
Conceito 3 – Apenas descreveu, de maneira satisfatória, o objetivo da prática de gerenciamento de incidentes OU apenas definiu incidentes corretamente.
Conceito 4 – Descreveu, de maneira satisfatória, o objetivo da prática de gerenciamento de incidentes E definiu incidentes corretamente.

QUESITO 2.3
Conceito 0 – Não discorreu sobre IDOR nem sobre *eavesdropping* ou o fez de forma totalmente equivocada.
Conceito 1 – Discorreu de maneira precária apenas sobre IDOR OU apenas sobre *eavesdroppin*g.
Conceito 2 – Discorreu de maneira precária sobre IDOR E sobre *eavesdropping*.
Conceito 3 – Discorreu de maneira satisfatória apenas sobre IDOR OU apenas sobre *eavesdropping*.
Conceito 4 – Discorreu de maneira satisfatória sobre IDOR E sobre *eavesdropping*.

TRIBUNAL DE CONTAS DO DISTRITO FEDERAL

CARGO 3: AUDITOR DE CONTROLE EXTERNO – ÁREA ESPECIALIZADA
ESPECIALIDADE TECNOLOGIA DA INFORMAÇÃO
ORIENTAÇÃO SISTEMAS DE TI

Prova Discursiva P_4 – Questão 2

Aplicação: 17/12/2023

PADRÃO DE RESPOSTA DEFINITIVO

2.1 Algumas das principais práticas do XP são:

- padrão de desenvolvimento: definição de um padrão de código (*design pattern*) para facilitar a compreensão do trabalho realizado por diferentes integrantes da equipe;
- *design* simples: o foco do desenvolvimento são as funcionalidades da solução, para evitar retrabalho nos *designs*, caso surjam alterações nos requisitos; após validação das funcionalidades implementadas e estabilização da solução desenvolvida, o *design* da solução pode ser melhorado; essa prática também requer que o código seja o mais simples possível, evitando complexidade desnecessária;
- planejamento/jogo de planejamento: os requisitos da solução são divididos em partes (histórias do usuário), o que permite ao cliente priorizar o desenvolvimento de cada uma; o desenvolvimento observa a ordem de prioridades definidas pelo cliente e o planejamento considera a quantidade de histórias que serão desenvolvidas em cada interação ou *release*;
- desenvolvimento de cliente/cliente disponível: envolvimento ativo do cliente no processo de desenvolvimento, incluindo-se revisões e testes do *softwar*e; o cliente participa na definição das histórias, dos documentos e da descrição das funcionalidades e, na medida em que o *software* está sendo desenvolvido, ele tem uma visão de como ficará e poderá solicitar mudanças pontuais;
- programação em pares: dois desenvolvedores trabalham juntos em um computador para revisar e escrever código, e a dupla de desenvolvedores pode ser constantemente substituída, promovendo-se um rodízio, de modo a se garantir a uniformidade do código e possibilitar que todos os membros da equipe tenham conhecimento de todas as funcionalidades implementadas;
- refatoração: prática de revisar e refinar continuamente o código para melhorar sua qualidade e legibilidade;
- desenvolvimento orientado a testes: o desenvolvimento das funcionalidades deve ser acompanhado de testes unitários, para validar se a implementação atente aos requisitos do cliente;
- testes de aceitação: criar testes de aceitação que definem critérios claros para a aceitação das funcionalidades;
- código coletivo: não existe divisão de responsabilidade por determinadas funcionalidades, partes do código ou módulos da solução; todos os desenvolvedores da equipe devem ter acesso a todas as partes do código, com liberdade de alterar e melhorar, sendo uma responsabilidade coletiva;
- metáfora: facilita a comunicação entre a equipe e os clientes, pois evita o uso de termos técnicos durante as reuniões ou interações com clientes, adotando metáforas para que eles possam compreender melhor o que está sendo realizado pela equipe de desenvolvimento;
- ritmo sustentável: manter um ritmo de trabalho sustentável, com carga horária de 40 horas semanais, evitando-se horas extras, sobrecarga e esgotamento da equipe;
- integração contínua: integrar as alterações de código ao repositório principal várias vezes ao dia, com execução de testes automatizados para garantir que a integração não quebre a funcionalidade existente;
- pequenas liberações/*releases* curtos: objetiva a entrega de pequenas partes do *software* com frequência e em curto espaço de tempo; o *software* será desenvolvido de forma incremental, em que cada *release* libera novas funcionalidades;
- *feedback* contínuo: buscar *feedback* constante dos clientes e da equipe para identificar melhorias e ajustes necessários.

2.2 O Kanban propicia a visualização do trabalho, por meio de um quadro físico ou virtual composto por colunas que representam as etapas ou a fase do processo. Os cartões, que representam as atividades, são posicionados em cada uma das colunas, o que permite identificar a fase, ou etapa, em que se encontra cada uma das atividades planejadas. A limitação do trabalho em progresso é definida por um número inserido em cada coluna do quadro do Kanban, que representa as etapas ou fases do processo, e representa a quantidade máxima de tarefas ou atividades que podem ser executadas simultaneamente naquela fase/etapa. O objetivo de limitar o trabalho em progresso é evitar a sobrecarga da equipe, o que pode resultar em atrasos ou problemas de qualidade.

2.3 O SCRUM prevê as seguintes reuniões, também conhecidas como eventos:

- reunião de planejamento de *sprint*: reunião realizada entre a equipe de desenvolvimento, o Scrum Master e o Product Owner; essa reunião visa definir os itens do *product backlog* a serem implementados e entregues ao final da próxima *sprint*;
- reunião diária: tem por objetivo alinhar a equipe de desenvolvimento sobre o progresso da Sprint bem como identificar e discutir os obstáculos encontrados; esse tipo de reunião deve ser rápido e a participação do Product Owner é opcional;
- reunião de revisão de *sprint*: reunião realizada entre a equipe de desenvolvimento, o Scrum Master e o Product Owner, com o objetivo de apresentar para o Product Owner as funcionalidades desenvolvidas durante a *sprin*t. Nesta reunião o Product Owner verifica se os critérios de aceitação foram atendidos e fornece *feedback* para equipe de desenvolvimento;
- reunião de retrospectiva de *sprin*t: reunião realizada entre a equipe de desenvolvimento e o Scrum Master, com o objetivo de discutir as lições aprendidas na *sprint* passada e identificar oportunidades de melhorias para as próximas *sprints*;
- reunião de refinamento do *product backlog*: reunião realizada entre a equipe de desenvolvimento, o Product Owner e com participação facultativa do Scrum Master, com o objetivo de discutir e refinar os itens de *backlog* que serão priorizados em *sprints* futuras.

QUESITOS AVALIADOS

Quesito 2.1
Conceito 0 – Não citou nenhuma prática do XP ou citou práticas que não são do XP.
Conceito 1 – Citou apenas uma prática do XP, sem explicá-la.
Conceito 2 – Citou apenas uma prática do XP, explicando-a, ou citou as duas práticas do XP, sem explicá-las.
Conceito 3 – Citou e explicou duas práticas do XP.

Quesito 2.2
Conceito 0 – Não explicou como o Kanban propicia a visualização do trabalho nem a limitação do trabalho em progresso.
Conceito 1 – Explicou apenas como o Kanban propicia a visualização do trabalho, ou apenas a limitação do trabalho em progresso, abordando pelo menos uma de suas características corretamente.
Conceito 2 – Explicou adequadamente como o Kanban propicia a visualização do trabalho e a limitação do trabalho em progresso, abordando corretamente pelo menos uma de suas características.

Quesito 2.3
Conceito 0 – Não citou nenhuma reunião prevista no SCRUM.
Conceito 1 – Citou apenas uma reunião prevista no SCRUM sem explicar seu objetivo.
Conceito 2 – Citou e explicou o objetivo de apenas uma reunião prevista no SCRUM ou citou duas reuniões previstas no SCRUM, sem explicar o objetivo de nenhuma delas.
Conceito 3 – Citou e explicou o objetivo de duas reuniões previstas no SCRUM.

TRIBUNAL DE CONTAS DO DISTRITO FEDERAL

CARGO 3: AUDITOR DE CONTROLE EXTERNO – ÁREA ESPECIALIZADA
ESPECIALIDADE TECNOLOGIA DA INFORMAÇÃO
ORIENTAÇÃO SISTEMAS DE TI

Prova Discursiva P_4 – Peça de Natureza Técnica

Aplicação: 17/12/2023

PADRÃO DE RESPOSTA DEFINITIVO

PARECER N.º 9.876/202X

Processo n.º: 1.234/202X
Assunto: Análise a respeito da Lei n.º 13.709/2018 (Lei de Proteção de Dados Pessoais)
Ementa: xxxxxxxxxxxx

A LGPD, instruída pela Lei n.º 13.709/2018, dispõe sobre o tratamento de dados pessoais no Brasil, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. O principal objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural no Brasil. A LGPD não se aplica a tratamento de dados realizado para fins exclusivamente jornalísticos e artísticos; o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular; também pode ser realizado para a proteção da vida ou da incolumidade física do titular ou de terceiro.

Segundo a LGPD, o controlador de dados é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Entre suas responsabilidades constam a criação de relatório de impacto à proteção de dados pessoais, cumprir obrigação legal ou regulatória voltada ao tratamento de dados pessoais e obter consentimento específico do titular de dados para compartilhar dados pessoais com outros controladores. Outras responsabilidades podem ser descritas conforme a LGPD.

Segundo a LGPD, o operador de dados é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Entre suas responsabilidades estão a de manter registro das operações de tratamento de dados pessoais que realizar; de realizar o tratamento segundo as instruções fornecidas pelo controlador e se ficar caracterizado dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Segundo a LGPD, o encarregado de dados é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O encarregado de dados tem como possíveis responsabilidades a de fornecer seus dados para o controlador de dados para identificação pública; a de aceitar reclamações e comunicações dos titulares de dados; e a de receber comunicações da autoridade nacional e adotar providências. Outras responsabilidades podem ser consideradas.

Segundo o que preconiza a LGPD, o TCDF deve considerar: 1) a criação de papéis e responsabilidades para o controlador de dados e os processos correspondentes para o tratamento de dados pessoais e dados pessoais sensíveis; 2) a criação de papéis e responsabilidades para o operador de dados e os processos correspondentes; 3) alterar atos normativos internos que lidam com informações pessoais, observando o que determina a LGPD; 4) estabelecer ponto de contato com a ANPD para sanar dúvidas e entendimentos específicos no caso do TCDF. Outras recomendações podem ser consideradas.

QUESITOS AVALIADOS

QUESITO 2.1 – Introdução sobre a LGPD e citação de três características importantes da lei
Conceito 0 – Não apresentou uma introdução sobre LGPD nem citou nenhuma característica da LGPD ou o fez de forma totalmente equivocada.
Conceito 1 – Apresentou introdução coerente sobre a LGPD, mas não citou nenhuma característica da LGPD.
Conceito 2 – Apresentou introdução coerente sobre a LGPD e citou uma característica da LGPD.
Conceito 3 – Apresentou introdução coerente sobre a LGPD e citou duas características da LGPD.
Conceito 4 – Apresentou uma introdução coerente sobre a LGPD e citou três características da LGPD.

QUESITO 2.2 – Definição de controlador de dados e descrição de três de suas possíveis responsabilidades

Conceito 0 – Não definiu controlador de dados e não descreveu nenhuma de suas possíveis responsabilidades ou o fez de forma totalmente equivocada.
Conceito 1 – Definiu corretamente controlador de dados, mas não descreveu nenhuma de suas possíveis responsabilidades.
Conceito 2 – Definiu corretamente controlador de dados e descreveu apenas uma de suas possíveis responsabilidades.
Conceito 3 – Definiu corretamente controlador de dados e descreveu duas de suas possíveis responsabilidades.
Conceito 4 – Definiu corretamente controlador de dados e descreveu três de possíveis responsabilidades.

QUESITO 2.3 – Definição de operador de dados e descrição de três de suas possíveis responsabilidades
Conceito 0 – Não definiu operador de dados nem descreveu nenhuma de suas possíveis responsabilidades ou o fez de forma totalmente equivocada.
Conceito 1 – Definiu corretamente operador de dados, mas não descreveu nenhuma de suas possíveis responsabilidades.
Conceito 2 – Definiu corretamente operador de dados e descreveu apenas uma de suas possíveis responsabilidades.
Conceito 3 – Definiu corretamente operador de dados e descreveu duas de suas possíveis responsabilidades.
Conceito 4 – Definiu corretamente operador de dados e descreveu três de suas possíveis responsabilidades.

QUESITO 2.4 – Definição de encarregado de dados e descrição de três de suas possíveis responsabilidades
Conceito 0 – Não definiu encarregado de dados nem descreveu nenhuma de suas possíveis responsabilidades ou o fez de forma totalmente equivocada.
Conceito 1 – Definiu corretamente encarregado de dados, mas não descreveu nenhuma possível responsabilidade.
Conceito 2 – Definiu corretamente encarregado de dados e descreveu apenas uma de suas possíveis responsabilidades.
Conceito 3 – Definiu corretamente encarregado de dados e descreveu duas de suas possíveis responsabilidades.
Conceito 4 – Definiu corretamente encarregado de dados e descreveu três de suas possíveis responsabilidades.

QUESITO 2.5 – Apresentação de quatro recomendações que o TCDF deve adotar segundo o que preconiza a LGPD
Conceito 0 – Não apresentou nenhuma recomendação que o TCDF deve adotar segundo a LGPD.
Conceito 1 – Apresentou apenas uma recomendação que o TCDF deve adotar segundo a LGPD.
Conceito 2 – Apresentou duas recomendações que o TCDF deve adotar segundo a LGPD.
Conceito 3 – Apresentou três recomendações que o TCDF deve adotar segundo a LGPD.
Conceito 4 – Apresentou quatro recomendações que o TCDF deve adotar segundo a LGPD.