Aula 03 - Prof. Fernando Pedrosa

TJ-SP (Analista de Sistemas Judiciário)
Passo Estratégico de Legislação - 2025
(Pós-Edital)

Autor:
Telma Vieira, Fernando Pedrosa Lopes

10 de Fevereiro de 2025

Normativos da Plataforma Digital do Poder Judiciário

Sumário

Conteúdo

Resolução CNJ nº 335/2020. Resolução CNJ nº 396/2021. Portaria CNJ nº 252/2020. Portaria CNJ nº 253/2020. Portaria CNJ nº 131/2021. Portaria CNJ nº 162/2021.

Análise Estatística

Inicialmente, convém destacar o percentual de incidência do assunto, dentro da disciplina Legislação dos TRFs, STJ, STF e CNJ em concursos/cargos similares. Quanto maior o percentual de cobrança de um dado assunto, maior sua importância.

Obs.: um mesmo assunto pode ser classificado em mais de um tópico devido à multidisciplinaridade de conteúdo.

Assunto	Relevância na disciplina em concursos similares
Conselho Nacional de Justiça (CNJ)	**49.0 %**
1. Resoluções do CNJ	**45.1 %**
Lei Complementar 35 de 1979 - Lei Orgânica da Magistratura	**3.9 %**
Lei nº 11.416-2006 - Carreiras dos Servidores do Poder Judiciário da União	**1.0 %**
Código de Ética da Magistratura Nacional	**1.0 %**

Glossário de termos

Faremos uma lista de termos que são relevantes ao entendimento do assunto desta aula. Caso tenha alguma dúvida durante a leitura, esta seção pode lhe ajudar a esclarecer.

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

Agente responsável pela ETIR: servidor público do Poder Judiciário incumbido de chefiar e gerenciar a ETIR.

Alta administração: unidades organizacionais com poderes deliberativos ou normativos no âmbito da organização.

Ameaças: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização.

Apetite a risco: nível de risco que a organização está disposta a aceitar para atingir os objetivos identificados no contexto analisado.

Aquisição de evidência: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais.

Ativo: qualquer coisa que represente valor para uma instituição, tal como a informação.

Ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

Autenticação: processo de identificação das partes envolvidas em um processo.

Autenticidade: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Autorização: processo que visa a garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.

Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, ao documento, ao material, à área ou à instalação.

Coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.

Competência: habilidade para aplicar conhecimentos e habilidades para atingir resultados pretendidos.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

Conformidade: preenchimento de um requisito.

Continuidade de serviços: capacidade estratégica e tática do órgão de se planejar e de responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em nível aceitável, previamente definido.

Crise: um evento ou série de eventos danosos que apresenta propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram; e que apresenta implicações que afetam proporção considerável da organização e de seus constituintes.

Crise cibernética: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores. É decorrente de incidentes que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização.

Controle: providência que modifica o risco, incluindo qualquer processo, política, dispositivo, prática ou ação.

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

Escopo de auditoria: extensão e fronteiras de uma auditoria.

Endereço IP (Internet Protocol): refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.

ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança de Cibernética. Denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia.

Estratégia de continuidade de serviços: abordagem do órgão que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou com outro incidente maior.

Evento: qualquer ocorrência observável em um sistema ou rede de uma organização.

Evidência digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento.

Evidência de auditoria: registros, declarações de fato ou outras informações verificáveis e relevantes para os critérios de auditoria.

Gerenciamento de crise: decisões e atividades coordenadas que ocorrem em uma organização durante uma crise corporativa, incluindo crises cibernéticas.

Gestão de continuidade de serviços: processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, concretizando-se, poderiam causar, fornecendo e mantendo nível aceitável de serviço diante de rupturas e desafios à operação normal do dia a dia.

Gestão de Riscos de Segurança da Informação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos.

Gestão de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

Gestor da informação: pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades.

Gestor de Segurança da Informação e das Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da administração pública federal (APF).

Impacto do risco: efeito resultante da ocorrência do risco.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado e aquela abrangida pelas demais hipóteses legais de sigilo.

Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Incidente grave: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação.

Incidente de Segurança da Informação: evento que viola ou representa ameaça iminente de violação de política de segurança, de política de uso aceitável ou de prática de segurança padrão.

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional.

Metadados: conjunto de dados estruturados que descrevem informação primária.

Nível de risco: magnitude do risco, expressa pelo produto das variáveis impacto e probabilidade.

Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado para ser usado quando ocorrer incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

Política de Segurança da Informação e das Comunicações (POSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

Preservação de evidência de incidentes em redes computacionais: processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.

Probabilidade do risco: possibilidade de ocorrência do risco.

Procedimento: conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim.

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

Requisito: necessidade ou expectativa declarada, geralmente implícita ou obrigatória.

Resiliência: poder de recuperação ou capacidade de determinada organização resistir aos efeitos de um incidente.

Recursos computacionais: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, computadores, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura.

Resumo criptográfico: é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho desta, gera resultado único e de tamanho fixo, também chamado de hash.

Risco de Tecnologia da Informação e Comunicação (TIC): evento capaz de afetar positiva ou negativamente os objetivos da organização nos níveis estratégico, tático e operacional.

Segurança cibernética: é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares. A Segurança Cibernética se aplica a uma parte da segurança da informação com foco na proteção digital, cuidando das ameaças as informações transportadas por meios cibernéticos. Já a Segurança da informação tem um foco mais amplo, cuidando da redução de riscos no transporte de dados por qualquer meio, seja digital ou não.

Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Sistema de gestão de segurança da informação (SGSI): políticas, procedimentos, manuais e recursos associados e atividades coletivamente gerenciadas por uma organização na busca de proteger seus ativos de informação.

Tolerância a risco: margem que a administração permite aos gestores de suportar o impacto de determinado risco em troca de benefícios específicos, ainda que esse seja superior ao "apetite ao risco" determinado pela organização.

Roteiro de revisão

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

Resolução CNJ nº 335/2020

Escopo:

Institui política pública para a governança e a gestão de processo judicial eletrônico. Integra os tribunais do país com a criação da Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br. Mantém o sistema PJe como sistema de Processo Eletrônico prioritário do Conselho Nacional de Justiça.

CAPÍTULO I

DA PLATAFORMA DIGITAL DO JUDICIÁRIO BRASILEIRO

O Capítulo I institui uma política pública para a governança e gestão de processo judicial eletrônico no Brasil, estabelecendo a criação da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br). Esta plataforma tem como objetivos integrar e consolidar todos os sistemas eletrônicos do Judiciário em um ambiente unificado, implantar o desenvolvimento comunitário com contribuições tecnológicas comuns, estabelecer padrões de desenvolvimento e arquitetura, e instituir uma plataforma única para publicação e disponibilização de aplicações, incluindo inteligência artificial (IA), por meio de computação em nuvem.

A PDPJ-Br funcionará como um modelo de convergência, provida por um repositório de soluções, e adotará obrigatoriamente conceitos como processo eletrônico em plataforma pública, desenvolvimento comunitário, modularização, microsserviços,

computação em nuvem, autenticação uniformizada, segurança da informação, otimização de fluxos de trabalho, automação, foco na redução da taxa de congestionamento dos processos, adequação à Lei no 13.709/2018 (LGPD), e preferência por tecnologias de código aberto.

O documento ainda proíbe a contratação de novos sistemas, módulos ou funcionalidades privados que causem dependência tecnológica e que não permitam o compartilhamento não oneroso da solução na PDPJ-Br. É estipulado um prazo para adequação para os tribunais que possuem contratos nas condições previstas, e o descumprimento da regra pode levar à responsabilização por improbidade administrativa e possível responsabilidade disciplinar dos gestores envolvidos.

CAPÍTULO II

DA POLÍTICA DE GOVERNANÇA E GESTÃO DA PDPJ-Br

O Capítulo II institui a política de governança e gestão para implantação e sustentação da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br). A política será coordenada pelo CNJ, com a participação de representantes do Poder Judiciário e do Sistema de Justiça, regulamentada por ato da Presidência do CNJ. Qualquer solução pública existente que atenda aos requisitos estabelecidos poderá ser aceita na PDPJ-Br, após aprovação da equipe técnica do CNJ, e o descumprimento dessa regra pode acarretar consequências legais.

O Ato da Presidência que disciplinar a política de governança e gestão da PDPJ-Br deverá estabelecer requisitos para os sistemas, incluindo padrões de desenvolvimento, documentação, operação de software, comunicação, interoperabilidade, arquitetura, autenticação, desenvolvimento compartilhado, interface, usabilidade, acessibilidade, experiência do usuário, inteligência artificial (IA), computação em nuvem e desenvolvimento modularizado. A política também poderá adotar outros requisitos devido à evolução tecnológica da plataforma.

A política deverá estabelecer ainda requisitos para os dados e documentos, como padrões das tabelas unificadas, bases centralizadas ou descentralizadas, padrões de dados e documentos digitais e padrões de assinaturas digitais. O CNJ também ficará responsável por definir e coordenar uma força-tarefa para o desenvolvimento de um portal com interface nacional única para os usuários externos, e todos os sistemas judiciais atuais deverão aderir à solução, integrando-a como um microsserviço.

CAPÍTULO III

DA POLÍTICA DE GOVERNANÇA E GESTÃO DA PDPJ-Br

O Capítulo III delineia as responsabilidades do CNJ na gestão da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br). Primeiramente, o CNJ deverá coordenar e promover ações para avaliar o estágio atual de desenvolvimento dos sistemas judiciais eletrônicos. Isso inclui a elaboração de um censo para identificar os sistemas utilizados em todos os tribunais, o grau de adesão ao PJe, as tecnologias empregadas e a identificação de sistemas onerosos, além de fixar diretrizes para alinhamento da governança com todos os tribunais.

Em segundo lugar, o CNJ deverá garantir a eficiência operacional da PDPJ-Br por meio de monitoramento, indicadores e metas. Essas metas incluem agilidade na tramitação dos processos, razoável duração do processo, excelência na gestão de custos, economicidade dos recursos, responsabilidade ambiental, melhor alocação de recursos humanos na área de tecnologia da informação e comunicações (TIC), e promoção e facilitação do acesso à Justiça para democratizar a relação do cidadão com os órgãos judiciais.

Por fim, a PDPJ-Br será hospedada em nuvem, podendo utilizar serviços de computação em nuvem providos por entidades privadas, inclusive na modalidade de integrador de nuvem (broker). Essa hospedagem deverá observar critérios como armazenamento dos dados em território nacional, cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), atendimento a requisitos de disponibilidade, escalabilidade, redundância, criptografia, capacidade de mensuração individualizada do uso dos recursos da nuvem, e conformidade com normas técnicas estabelecidas pelo CNJ.

CAPÍTULO IV

DOS SISTEMAS ATUAIS

O Capítulo IV aborda a gestão dos sistemas atuais no contexto da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br). O projeto PJe, já em estágio avançado de desenvolvimento e coordenado pelo CNJ, será mantido e aprimorado como parte central da nova Plataforma. A PDPJ-Br proverá aplicações, módulos e microsserviços por meio do conceito de "nuvem nacional", centralizando todas as bases de dados e aplicações. Os custos de processamento e armazenamento na nuvem nacional serão rateados proporcionalmente, e as regras para adoção e implantação da nuvem nacional serão regulamentadas pelo CNJ.

Os demais projetos de sistema processual público coordenados por outros tribunais poderão ser mantidos e aprimorados para se adequar à PDPJ-Br, desde que estejam em conformidade com a plataforma de interoperabilidade, permitam coexistência mediante desenvolvimento colaborativo e disponibilizem novos módulos e evoluções na Plataforma Nacional. Tribunais sem projetos de sistema processual público também poderão aderir à PDPJ-Br, colaborando no desenvolvimento de microsserviços e compartilhando melhorias e evoluções com todos os tribunais.

O CNJ coordenará a definição de critérios para a evolução dos sistemas, considerando o desenvolvimento comunitário, e monitorará os sistemas legados, sem interferir no desenvolvimento de soluções tecnológicas pelos tribunais, desde que justificadas pelas peculiaridades regionais ou metodologia de trabalho. Os tribunais deverão promover ações para facilitar a troca de informações com os demais sistemas e reduzir os custos de tecnologia da informação e comunicações (TIC) com ações isoladas.

Resumo

Capítulo I: Da Plataforma Digital do Judiciário Brasileiro

- Instituição da política pública para governança e gestão de processo judicial eletrônico.
- Criação da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) para integrar e consolidar sistemas eletrônicos.
- Estabelecimento de padrões de desenvolvimento, arquitetura e operação de software.
- Proibição de contratação de sistemas que causem dependência tecnológica.

Capítulo II: Da Política de Governança e Gestão da PDPJ-Br

- Instituição da política de governança e gestão da PDPJ-Br, coordenada pelo CNJ.
- Aceitação de soluções públicas que atendam aos requisitos estabelecidos.
- Estabelecimento de requisitos para sistemas, dados e documentos.
- Desenvolvimento de um portal com interface nacional única.

Capítulo III: Da Gestão da PDPJ-Br

- Coordenação pelo CNJ de ações para avaliar o estágio atual dos sistemas judiciais eletrônicos.
- Garantia de eficiência operacional da PDPJ-Br através de monitoramento, indicadores e metas.

- Hospedagem da PDPJ-Br em nuvem, observando critérios como armazenamento em território nacional e cumprimento da Lei Geral de Proteção de Dados Pessoais.

Capítulo IV: Dos Sistemas Atuais

- Manutenção e aprimoramento do projeto PJe como parte central da PDPJ-Br.
- Provisão de aplicações, módulos e microsserviços através da "nuvem nacional".
- Possibilidade de manutenção e adequação de outros projetos de sistema processual público.
- Adesão e colaboração de tribunais sem projetos de sistema processual público.
- Coordenação pelo CNJ da definição de critérios para evolução de sistemas e monitoramento dos sistemas legados.
- Promoção de ações pelos tribunais para facilitar a troca de informações e reduzir custos de TIC.

Resolução CNJ nº 396/2021

Escopo:

Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

CAPÍTULO I

DISPOSIÇÕES GERAIS

O Capítulo I da Resolução CNJ nº 396/2021 institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) para todos os órgãos do Poder Judiciário, exceto o Supremo Tribunal Federal (STF).

A ENSEC-PJ contempla temas essenciais para a segurança cibernética, incluindo segurança da informação, proteção de dados pessoais e institucionais, segurança física e proteção de ativos de tecnologia da informação.

Além disso, abrange ações destinadas a garantir a disponibilidade, integridade, confidencialidade e autenticidade de dados e informações, assegurando o funcionamento dos processos de trabalho, a continuidade operacional e das atividades fim e administrativas, com foco em planejamento, comunicação, conscientização,

direcionamento institucional e formação técnica e acadêmica na área de segurança cibernética.

CAPÍTULO II

OBJETIVOS DA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ENSEC-PJ)

Art. 2º A ENSEC-PJ tem o objetivo de aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito.

Art. 3º Para a concretização dos objetivos da segurança cibernética instituídos na Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), estrutura-se a presente Estratégia Nacional de Segurança Cibernética com visão, objetivos e ações capazes de conduzir os órgãos do Poder Judiciário a um ambiente desenvolvido, resistente e seguro.

CAPÍTULO III

DA VISÃO, DOS OBJETIVOS E DAS AÇÕES

O Capítulo III delineia a visão, objetivos e ações da Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ). A visão é alcançar a excelência em segurança cibernética, com objetivos que incluem tornar o Judiciário mais seguro e inclusivo no ambiente digital, aumentar a resiliência às ameaças cibernéticas, estabelecer governança integrada e permitir a continuidade dos serviços. Estes objetivos são a base para tornar o espaço cibernético mais confiável, resistente, inclusivo e seguro, direcionando as ações dos órgãos do Poder Judiciário, exceto o STF.

As ações da ENSEC-PJ foram estabelecidas para possibilitar o alcance dos objetivos e baseiam-se no estágio de maturidade geral dos órgãos do Judiciário. Essas ações incluem o fortalecimento das ações de governança cibernética, elevação do nível de segurança das infraestruturas críticas, estabelecimento de rede de cooperação e modelo centralizado de governança cibernética nacional. A alta administração de cada tribunal é considerada essencial para a consecução dessas finalidades, especialmente

quando necessária a rápida suspensão do acesso ao público para evitar ataques cibernéticos.

Os detalhes para fortalecer a governança cibernética e elevar a segurança das infraestruturas críticas são delineados em diversos pontos. Isso inclui estabelecer um Sistema de Gestão em Segurança da Informação baseado em riscos, criar e manter uma Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), utilizar tecnologia para análise consolidada de registros de auditorias, providenciar cópias de segurança atualizadas, elaborar requisitos específicos de segurança cibernética e realizar avaliações e testes semestrais de conformidade, entre outros.

CAPÍTULO IV

DO MODELO CENTRALIZADO DE GOVERNANÇA NACIONAL NA SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO

Art. 12. O modelo centralizado de governança nacional na segurança cibernética do Poder Judiciário tem os seguintes objetivos:

I – promover a coordenação dos diversos entes relacionados com a segurança cibernética;

II – possibilitar a análise conjunta do nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário;

III – estabelecer e desenvolver padrão de maturidade unificado de segurança cibernética, de forma que seja possível avaliar o nível de maturidade de cada órgão do Judiciário, por meio de indicadores estabelecidos;

IV – estabelecer rotinas de verificações de conformidade em segurança cibernética; e

V – possibilitar a convergência de esforços e iniciativas na apuração de incidentes e na promoção de ações de capacitação e educação em segurança cibernética.

Art. 13. O CNJ coordenará as ações para viabilizar a governança nacional em segurança cibernética do Poder Judiciário.

CAPÍTULO V

DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DO PODER

JUDICIÁRIO

O Capítulo V institui o Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ). Este comitê tem a atribuição de assessorar o CNJ nas atividades relacionadas à segurança da informação e é composto por especialistas representantes de várias entidades judiciais, incluindo o Conselho Nacional de Justiça, o Supremo Tribunal Federal, o Superior Tribunal de Justiça, entre outros. O CGSI-PJ será coordenado por um representante do CNJ designado pela Presidência, e seus integrantes devem possuir conhecimento técnico na área de segurança da informação.

A composição do CGSI-PJ permite a inclusão de dois especialistas de cada um dos Conselhos Nacional de Justiça e Tribunais de Justiça Estaduais, e um especialista dos outros órgãos judiciais mencionados. O CGSI-PJ também pode convidar representantes de órgãos de segurança pública, do Ministério Público, das Forças Armadas e especialistas técnicos de outros órgãos públicos ou privados. Reuniões ordinárias serão realizadas semestralmente, e reuniões extraordinárias podem ser convocadas pelo coordenador.

A competência do CGSI-PJ inclui estabelecer normas e critérios metodológicos para a gestão de risco dos ativos da informação, aprovar políticas e diretrizes, elaborar e implementar programas de conscientização e capacitação, monitorar e avaliar a execução da estratégia de segurança, criar e gerir o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CPTRIC-PJ) e promover a troca de informações e experiências com outros comitês gestores e a sociedade.

CAPÍTULO VI

DA REDE NACIONAL DE COOPERAÇÃO DO PODER JUDICIÁRIO NA ÁREA DE SEGURANÇA CIBERNÉTICA

O Capítulo VI estabelece a Rede de Cooperação do Judiciário na área de segurança cibernética, com o objetivo de promover um ambiente colaborativo e seguro entre os órgãos do Poder Judiciário. Essa rede visa acompanhar ameaças e ataques cibernéticos, compartilhar informações sobre incidentes, realizar exercícios cibernéticos, fortalecer o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CPTRIC-PJ), aprimorar a estrutura judiciária para investigações de crimes cibernéticos, incentivar a criação de equipes de resposta a incidentes, emitir alertas e

recomendações e ampliar parcerias com outros órgãos. Todos os órgãos do Judiciário que detectarem incidentes de segurança cibernética devem reportá-los ao CPTRIC-PJ.

Além disso, a alta administração dos órgãos do Poder Judiciário (exceto o STF) é responsável pela governança da segurança da informação. Isso inclui a implementação da Política de Segurança Cibernética, elaboração de normas internas, destinação de recursos orçamentários, promoção de capacitação, instituição e implementação de equipes de tratamento e resposta a incidentes, coordenação e execução de ações de segurança da informação e aplicação de ações corretivas e disciplinares em casos de violação.

Cada órgão do Poder Judiciário, com exceção do STF, deve constituir um Comitê de Governança de Segurança da Informação (CGSI) e uma estrutura de segurança da informação. O CGSI será responsável por assessorar, propor alterações, constituir grupos de trabalho, consolidar e analisar resultados de auditoria sobre a gestão da segurança da informação. A estrutura de segurança será subordinada diretamente à alta administração e terá um gestor responsável por instituir e gerir o Sistema de Gestão de Segurança da Informação, implementar controles internos, planejar a execução de programas e projetos, implantar procedimentos de tratamento e resposta a incidentes e observar as normas e procedimentos específicos aplicáveis.

CAPÍTULO VII

DA POLÍTICA DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO

O Capítulo VII estabelece a Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), com a finalidade de prover princípios, objetivos e instrumentos para assegurar a Segurança Cibernética no Poder Judiciário. Os princípios da PSEC-PJ incluem segurança jurídica, respeito aos direitos humanos, visão sistêmica da segurança cibernética, integração e cooperação, educação e inovação, orientação à gestão de riscos, prevenção e resposta a incidentes cibernéticos, articulação entre segurança cibernética e proteção de dados, e garantia ao sigilo e inviolabilidade da vida privada.

Os objetivos da PSEC-PJ envolvem contribuir para a segurança do indivíduo, sociedade e Estado; fomentar atividades de pesquisa e desenvolvimento tecnológico; aprimorar o arcabouço normativo; fortalecer a cultura de segurança cibernética; aprimorar o nível de maturidade em segurança cibernética; e orientar ações relacionadas à gestão em segurança da informação, infraestruturas críticas, proteção de dados pessoais, prevenção e resposta a incidentes, entre outros. Os instrumentos

da PSEC-PJ incluem a Estratégia Nacional de Segurança Cibernética, Protocolos de Prevenção, Gerenciamento de Crises e Investigação para Ilícitos Cibernéticos, e Manuais de Referência, que devem ser revisados e aprovados pelo Presidente do CNJ.

Além disso, todos os órgãos do Poder Judiciário, exceto o STF, deverão adotar e seguir os protocolos e manuais mencionados, contemplando diretrizes para prevenção, resposta e gestão de incidentes cibernéticos. Cada tribunal deve estabelecer em sua Política de Segurança da Informação ações para gestão dos ativos de informação, controles para tratamento de informações restritas, treinamento contínuo, requisitos de segurança nas contratações, uso de criptografia e comunicação com a alta administração do órgão. Em caso de crise cibernética, o Comitê de Crise deverá ser acionado conforme o Protocolo de Gerenciamento de Incidentes e de Crises Cibernéticas.

CAPÍTULO VIII

DA GESTÃO DE USUÁRIOS

Art. 29. Cada órgão do Poder Judiciário, com exceção do STF, deverá implementar a gestão de usuários de sistemas informatizados composta de:

I – gerenciamento de identidades;

II – gerenciamento de acessos; e

III – gerenciamento de privilégios.

Parágrafo único. A gestão de usuários será disciplinada por ato do Presidente do CNJ, que definirá o padrão a ser adotado para utilização de credenciais de login único e interface de interação dos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas judiciais.

CAPÍTULOS IX E X

DA POLÍTICA DE CULTURA E EDUCAÇÃO EM SEGURANÇACIBERNÉTICA E DO ORÇAMENTO

Art. 30. Fica instituída, no âmbito dos órgãos do Poder Judiciário, à exceção do STF, a Política de Cultura e Educação em Segurança Cibernética no âmbito do Poder Judiciário (PCESC-PJ).

Parágrafo único. A PCESC-PJ será disciplinada por ato do Presidente do CNJ.

Art. 31. Para execução das ações estratégicas, os órgãos do Poder Judiciário, objeto desta norma, deverão destinar os recursos orçamentários necessários.

Parágrafo único. Os recursos orçamentários deverão ser discriminados em rubrica específica para possibilitar que a Governança Nacional em Segurança Cibernética possa avaliar, de forma clara, os investimentos no setor.

Resumo

CAPÍTULO I: DISPOSIÇÕES GERAIS

- Instituição da Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ).
- Contempla temas como segurança da informação, segurança física, proteção de dados, disponibilidade, integridade, continuidade operacional, planejamento, normatização, comunicação, conscientização e formação técnica em segurança cibernética.

CAPÍTULO III: DA VISÃO, DOS OBJETIVOS E DAS AÇÕES

- Visão de excelência em segurança cibernética no Poder Judiciário.
- Objetivos de tornar o espaço cibernético mais confiável, resistente, inclusivo e seguro.
- Ações estabelecidas para possibilitar o alcance dos objetivos, baseadas no estágio de maturidade dos órgãos.
- Engajamento da alta administração essencial para a consecução das finalidades.
- Definição de ações para fortalecimento da governança, elevação da segurança, estabelecimento de rede de cooperação e modelo centralizado de governança cibernética.

CAPÍTULO V: DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DO PODER JUDICIÁRIO

- Instituição do Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ) para assessorar o CNJ.
- Composição do CGSI-PJ inclui representantes de diversos órgãos judiciários.
- O comitê se reunirá semestralmente ou em caráter extraordinário.

- Compete ao CGSI-PJ estabelecer normas, aprovar políticas, elaborar programas, estabelecer critérios de monitoramento, criar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos e promover a troca de informações.

CAPÍTULO VI: DA REDE NACIONAL DE COOPERAÇÃO DO PODER JUDICIÁRIO NA ÁREA DE SEGURANÇA CIBERNÉTICA

- Estabelece a Rede de Cooperação do Judiciário na área de segurança cibernética.
- Objetivos incluem promoção de ambiente colaborativo e seguro, compartilhamento de informações, realização de exercícios cibernéticos, fortalecimento do CPTRIC-PJ, aprimoramento de investigações de crimes cibernéticos e incentivo à criação de ETIR.
- Responsabilidades da alta administração dos órgãos judiciários na governança da segurança da informação.
- Cada órgão deve constituir um Comitê de Governança de Segurança da Informação (CGSI) e uma estrutura de segurança da informação.

CAPÍTULO VII: DA POLÍTICA DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO

- Estabelecimento da Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ) para assegurar a Segurança Cibernética.
- Princípios da PSEC-PJ incluem segurança jurídica, respeito aos direitos humanos, visão sistêmica, integração e cooperação, educação e inovação, orientação à gestão de riscos, prevenção e resposta a incidentes.
- Objetivos para contribuir para a segurança do indivíduo, sociedade e Estado; fomentar pesquisa e desenvolvimento; aprimorar normativas; fortalecer a cultura de segurança; orientar ações relacionadas à segurança da informação.
- Instrumentos incluem Estratégia Nacional de Segurança Cibernética, Protocolos de Prevenção, Gerenciamento de Crises e Investigação para Ilícitos Cibernéticos, e Manuais de Referência.
- Todos os órgãos do Poder Judiciário, exceto o STF, deverão adotar os protocolos e manuais, e cada tribunal deve estabelecer em sua Política de Segurança da Informação ações específicas.

Portaria CNJ nº 252/2020

Escopo:

Dispõe sobre o Modelo de Governança e Gestão da Plataforma Digital do Poder Judiciário – PDPJ-Br.

Resumo

A Portaria nº 252, de 18 de novembro de 2020, estabelece a governança e gestão da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) e pode ser resumida nos seguintes parágrafos:

1. Modelo de Governança e Condições para Integração: A portaria dispõe sobre o Modelo de Governança da PDPJ-Br e estabelece condições para integração à plataforma, incluindo a conformidade com padrões e normas, não sobreposição de soluções, não dependência de componentes licenciados, e conformidade com a Lei Geral de Proteção de Dados (LGPD).
2. Obrigações dos Órgãos e Instituições Aderentes: Os órgãos ou instituições que desejam integrar-se à PDPJ-Br devem possuir propriedade intelectual das aplicações, seguir as normas do Programa Nacional de Gestão Documental, possuir planos de suporte, e colaborar com o CNJ na gestão de soluções.
3. Segurança e Proteção de Dados: A portaria enfatiza a necessidade de proteger dados e informações contra ameaças, garantindo integridade, confidencialidade, disponibilidade e autenticidade. Os usuários são responsáveis pela guarda e sigilo de suas senhas e dispositivos móveis.
4. Estrutura de Governança: A Rede de Governança da PDPJ-Br é estabelecida, incluindo uma Comissão Permanente de Tecnologia da Informação, Comitê Gestor Nacional, Comitês Gestores dos Tribunais, Gerência Executiva e Grupos de Trabalho. O Comitê Gestor Nacional é responsável pela supervisão geral da Plataforma, e os Comitês Gestores dos tribunais têm atribuições específicas para a implementação e avaliação da PDPJ-Br em seus respectivos tribunais.
5. Gerência Executiva e Grupos Nacionais: A Gerência Executiva é responsável por orquestrar as atividades colaborativas e definir responsabilidades no desenvolvimento da Plataforma. São criados Grupos Nacionais para gerenciamento, desenvolvimento e sustentação, bem como para avaliar requisitos de negócios. A portaria também estabelece mecanismos para resolução de casos omissos.

Portaria CNJ nº 253/2020

Escopo:

Institui os critérios e diretrizes técnicas para o processo de desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br.

Resumo

A Portaria nº 253, de 18 de novembro de 2020, critérios e diretrizes técnicas para o processo de desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br e pode ser resumida nos seguintes parágrafos:

1. Criação da Plataforma e Diretrizes Gerais: A Portaria institui os critérios e diretrizes técnicas para o desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br). A PDPJ-Br fornecerá padrões de API, modelos de dados, eventos e mensagens para permitir que desenvolvedores criem e mantenham aplicações. O processo de disponibilização de soluções será comunitário e descentralizado, envolvendo tribunais, órgãos públicos externos e particulares.
2. Comunidade e Acompanhamento de Projetos: O CNJ disponibilizará a lista de projetos em andamento, concluídos e pendentes, e acompanhará a execução dos projetos por meio de líderes técnicos e do Escritório de Projetos do Departamento de Tecnologia da Informação e Comunicação. Profissionais envolvidos serão identificados por órgão e área de atuação, e mecanismos de reputação serão adotados.
3. Classificação dos Serviços e Arquitetura da Plataforma: Os serviços e aplicações da PDPJ-Br serão classificados em categorias como serviços estruturantes, negociais, de integração e soluções da comunidade externa. A PDPJ-Br seguirá o modelo arquitetural de microsserviços, utilizando a metodologia Domain Driven Design (DDD) e um modelo de coreografia com alto nível de desacoplamento.

   Serviços Estruturantes: Implementam as funcionalidades essenciais básicas para um sistema de processo judicial de tramitação eletrônica, bem como àqueles serviços necessários à integração, à coreografia e à interoperabilidade entre os serviços e soluções que compõe a PDPJ-Br (Plataforma Digital do Poder Judiciário).

   Serviços negociais: Serviços que implementam necessidade de negócio relevante para a tramitação de processo judicial eletrônico e sistemas judiciais, tais como distribuição de processos, controle de custas, comunicação de atos, controle de agendamento de audiências, central de mandados, dentre outros;

   Serviços de Integração com Sistemas Externos: Serviços que fazem interface com sistemas, serviços e/ou aplicações externas ao Poder Judiciário, como o sistema de penhora on-line fornecido em parceira com o Banco Central (Sisbajud), o sistema de

envio eletrônico de correspondências pela Empresa Brasileira de Correios e Telégrafos (eCARTA), dentre outros de especial interesse à prestação do serviço jurisdicional.

Soluções e aplicações da comunidade externa ao judiciário: Serviços desenvolvidos por entes externos ao judiciário voltados a atender às suas necessidades, adotando padrões de API que se integrem à PDPJ-Br mediante chancela do Poder Judiciário.

4. Tecnologia, Segurança e Práticas de Desenvolvimento: A Portaria estabelece que a linguagem de programação Java, com o framework Spring, será preferencialmente adotada. Os microsserviços devem ser versionados com Git, protegidos com OAuth2 e desenvolvidos com práticas como Continuous Integration (CI), Continuous Delivery (CD) e Test Driven Development (TDD), no qual é obrigatória a produção de relatório de cobertura de testes automatizados, o qual deverá ser atualizado a cada execução do pipeline de integração contínua. Além disso, são estabelecidas diretrizes para a interface gráfica, documentação técnica, e o uso de nuvem computacional e Inteligência Artificial.
5. Cooperação e Vigência: Tribunais ou entes participantes devem assinar um Termo de Cooperação Técnica, e o Departamento de Tecnologia da Informação e Comunicação do CNJ será responsável por prover manutenção e detalhamento dessas diretrizes.

Portaria CNJ nº 131/2021

Escopo:

Institui o Grupo Revisor de Código-Fonte das soluções da Plataforma Digital do Poder Judiciário (PDPJ-Br) e do Processo Judicial Eletrônico (PJe).

Resumo

A Portaria CNJ nº 131/2021 pode ser resumida nos seguintes parágrafos:

1. Instituição e Objetivo: A Portaria institui o Grupo de Trabalho de revisão de código-fonte das soluções da Plataforma Digital do Poder Judiciário (PDPJ) e do sistema Processo Judicial Eletrônico (PJe). O objetivo do grupo é garantir a qualidade das implementações feitas pelo Conselho Nacional de Justiça (CNJ) e pela comunidade de desenvolvedores, analisando mudanças no código-fonte.

2. **Composição e Qualificação**: O Grupo Revisor será composto por membros indicados pelo Departamento de Tecnologia da Informação e Comunicação (DTI) do CNJ, por representantes dos tribunais e por servidores lotados na Divisão do Processo Judicial Eletrônico (DPJe). Os membros devem ter experiência ou formação em desenvolvimento de sistemas, e a composição pode ser revista a qualquer tempo.
3. **Funções e Responsabilidades**: Os objetivos do Grupo incluem promover a análise de mudanças de código-fonte, executar testes de qualidade, e definir critérios para orientar a evolução de projetos. O código-fonte deve ser submetido à análise sintática automatizada, e os que não atingirem os critérios mínimos serão rejeitados. Servidores da DPJe coordenarão as atividades, convocando reuniões e definindo metas.
4. **Processo de Revisão**: Os encontros ocorrerão principalmente virtualmente, com sprints quinzenais para análise de "merge requests." A aprovação deve ser acompanhada de comprovação de testes, e as análises pendentes terão prioridade na próxima sprint. O CNJ proverá um ambiente de testes padronizado, e as atividades serão documentadas em um repositório centralizado.
5. **Disposições Finais**: O Grupo Revisor de Código-Fonte será permanente, iniciando suas atividades a partir da publicação da Portaria, e incluirá servidores indicados por diversos órgãos judiciais.

Portaria CNJ nº 162/2021

Escopo:

Aprova Protocolos e Manuais criados pela Resolução CNJ no 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

Anexo I - Protocolo – Prevenção de Incidentes Cibernéticos do Poder Judiciário

1. Escopo

O Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) estabelece um conjunto de diretrizes adaptáveis para prevenir incidentes cibernéticos. O escopo é definido em termos de gestão de risco organizacional, permitindo decisões eficazes para enfrentar ameaças e melhorar as práticas existentes, com possibilidade de ajustes de acordo com a realidade de cada órgão do Poder Judiciário.

2. Funções Básicas

As funções básicas do PPINC-PJ são explicitadas em cinco categorias: identificar, proteger, detectar, responder e recuperar. Essas funções abordam aspectos como o entendimento e gerenciamento de riscos, implementação de salvaguardas para proteção de dados, monitoramento contínuo para detecção de incidentes e planos de resiliência e restauração para recuperação após incidentes.

3. Princípios críticos

O protocolo também apresenta princípios críticos adaptáveis que asseguram a construção de um sistema de segurança cibernética eficaz. Estes incluem o uso de informações de ataques reais, priorização na formação e revisão de controles, definição de métricas comuns, diagnóstico contínuo, formação e conscientização, automação, e a capacidade de resiliência. Esses princípios visam fornecer uma estrutura flexível e robusta, contribuindo para uma cultura de segurança cibernética organizacional.

4. Gestão de Incidentes de Segurança Cibernética

O Protocolo Gestão de Incidentes de Segurança Cibernética enfatiza um processo formal que inclui detecção, triagem, análise e resposta aos incidentes. Esse processo é essencial para a identificação e o tratamento eficaz dos incidentes de segurança cibernética.

5. Competência de atuação

Na Seção 5, o protocolo detalha a Competência de Atuação, estabelecendo a necessidade de uma Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) em todos os órgãos do Poder Judiciário, exceto o STF. A ETIR tem autonomia compartilhada para recomendar procedimentos e debater ações, podendo solicitar apoio multidisciplinar em áreas como tecnologia da informação, segurança da informação, jurídica, entre outras.

6. Funcionamento da ETIR

O Funcionamento da ETIR deve ser regulado por um documento formal. Esse documento deve incluir definições da missão, público-alvo, modelo de implementação, nível de autonomia, designação de integrantes, canal de comunicação de incidentes e serviços prestados, fornecendo uma estrutura clara e transparente para a equipe.

7. Boas Práticas de Segurança Cibernéticas

Finalmente, a última seção aborda as Boas Práticas de Segurança Cibernética, ressaltando que a segurança cibernética é um esforço coletivo. Essa seção define as dimensões e práticas, incluindo preparação, identificação, contenção, erradicação, recuperação e lições aprendidas. Ela destaca a necessidade de adaptar e ajustar essas práticas de acordo com a realidade de cada órgão, promovendo uma abordagem metódica e colaborativa para prevenir e responder a ataques cibernéticos.

Anexo II - Protocolo – Gerenciamento de Crises Cibernéticas do Poder Judiciário

Fases do Gerenciamento de Crises:

O Gerenciamento de Crises pode ser dividido em 3 (três) fases:

a) planejamento (pré-crise);

b) execução (durante a crise); e

c) melhoria Contínua (pós-crise).

1. Planejamento da Crise (pré-crise): Esta fase envolve a preparação prévia e adequada para lidar com crises cibernéticas. Os órgãos do Poder Judiciário devem estabelecer um Programa de Gestão da Continuidade de Serviços, que inclui observar o Protocolo de Prevenção a Incidentes Cibernéticos, definir atividades críticas, identificar ativos de informação críticos, avaliar riscos, categorizar incidentes, priorizar monitoramento e tratamento de riscos, e realizar simulações e testes. Também deve ser definida uma sala de situação e criado um Comitê de Crises Cibernéticas, composto por representantes de várias áreas, e o Plano de Gestão de Incidentes Cibernéticos deve ser estabelecido.

2. Execução (durante a crise): Nesta fase, a comunicação entre as áreas envolvidas é vital para reagir a uma crise cibernética. Quando a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) identifica uma crise, o Comitê de Crise deve se reunir imediatamente. Os planos de contingência devem ser efetivados, e a sala de situação deve ser equipada com meios necessários para gerenciar a crise. A eficácia do trabalho depende de uma série de ações, como entender o incidente, levantar informações, avaliar a necessidade de suspender serviços, centralizar a

comunicação, definir estratégias, solicitar colaboração de especialistas, avaliar recursos, e elaborar um plano de retorno à normalidade.

3. Melhoria Contínua (lições aprendidas no pós-crise): Após o retorno à normalidade, é necessário realizar uma análise criteriosa das ações tomadas durante a crise, identificando o que foi bem-sucedido e o que foi inadequado. A avaliação deve incluir a análise da causa-raiz do incidente, a linha do tempo das ações, o impacto nos dados, mecanismos de detecção e proteção, coordenação da crise, tomada de decisão, e estratégias de recuperação. As lições aprendidas devem ser usadas para revisar os procedimentos de resposta e melhorar o processo de preparação para futuras crises cibernéticas. Um Relatório de Comunicação de Incidente de Segurança Cibernética deve ser elaborado, detalhando a crise e o plano de ação para evitar incidentes similares no futuro.

Anexo III - Protocolo – Investigação para Ilícitos Cibernéticos do Poder Judiciário

1. Objetivo e Requisitos para Adequação dos Ativos de Tecnologia da Informação: O Protocolo de Investigação para Ilícitos Cibernéticos (PIILC-PJ) tem como objetivo estabelecer procedimentos para coleta e preservação de evidências em incidentes cibernéticos, bem como para comunicação ao Ministério Público e à polícia. Os ativos de tecnologia da informação devem ser sincronizados com a Hora Legal Brasileira e configurados para registrar eventos relevantes de Segurança da Informação e Comunicações (SIC), incluindo autenticação, acesso a recursos e dados, e alterações nos registros de auditoria. Os registros devem ser armazenados por no mínimo 6 meses e, se possível, armazenados também remotamente.

2. Procedimento para Coleta e Preservação das Evidências: A ETIR, sob supervisão, deve coletar e preservar mídias de armazenamento, dados voláteis, e registros de eventos. Em caso de inviabilidade de preservação das mídias, a ETIR deve coletar cópias dos arquivos afetados. A integridade das evidências deve ser preservada e o material coletado deve ser lacrado e custodiado. Todos os procedimentos devem ser documentados e o material ficará à disposição da autoridade competente.

3. Comunicação do Incidente de Segurança: Ao tomar conhecimento de um Incidente de Segurança Cibernética penalmente relevante, o responsável pelo órgão afetado

deve comunicá-lo imediatamente ao órgão de polícia e ao Ministério Público. Se o incidente for considerado Crise Cibernética, o Comitê de Crise deve ser acionado. Após a coleta e preservação das evidências, o responsável pela ETIR deve elaborar um Relatório de Comunicação de Incidente de Segurança Cibernética, detalhando os eventos verificados.

4. Detalhes do Relatório e Encaminhamento: O Relatório de Comunicação deve conter informações como nome do responsável, descrição do incidente, atividades de tratamento e resposta, resumo criptográfico dos arquivos coletados, e justificativa sobre inviabilidade de preservação das mídias, entre outros. O relatório deve ser acondicionado em envelope lacrado, protocolado, e encaminhado à autoridade responsável, que, por sua vez, o encaminhará formalmente ao Ministério Público e ao órgão de polícia judiciária, juntamente com todo o material, para fins de instrução da notícia crime.

Anexo IV - Manual de Referência – Proteção de Infraestruturas Críticas de TIC

1. Campo de Aplicação: O Manual é obrigatório no âmbito do Poder Judiciário, exceto no Supremo Tribunal Federal. Todos os órgãos do Judiciário com infraestrutura tecnológica devem seguir as orientações e implementar os controles mínimos recomendados neste documento.

2. Finalidade e Escopo: O Manual estabelece diretrizes para a implementação dos controles de segurança cibernética para proteger as infraestruturas de TIC. Aplica-se a todos os membros do órgão, incluindo magistrados, servidores, colaboradores, fornecedores, prestadores de serviços e estagiários. As orientações são a base mínima para a proteção e não limitam a adoção de outros controles, processos e frameworks.

3. Princípios: Os princípios que devem orientar este documento incluem Eficiência (busca pelo melhor resultado), Ética (seguição de valores morais), Impessoalidade (servir a todos), Legalidade (atuar dentro das leis), Moralidade (preservação dos princípios éticos), e Publicidade (transparência do Poder Público).

4. Controles Mínimos Recomendados: O Judiciário apresenta diversidade em suas características, mas este Manual baseia-se em controles mínimos considerados pertinentes. Os controles foram selecionados do framework CIS Controls versão 7.1, que estima prevenir 85% dos principais ataques. A aplicabilidade é categorizada por grupos, dependendo do porte e recursos da organização. A busca pela adequação deve ser contínua, com avaliações periódicas, para permitir a melhoria constante da segurança digital.

Anexo V - Manual de referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

Requisitos de Resiliência Cibernética

Com base nas metas, objetivos, princípios e framework, estabelecem-se requisitos para um ambiente de segurança cibernética resiliente. São definidas normas e processos para criar um ambiente robusto e seguro, capaz de enfrentar e superar ameaças cibernéticas.

Da Identificação

Na organização, espera-se que haja inventário e configuração de todos os itens de TIC, uma base centralizada de processos, gerenciamento de risco cibernético, exposição ao risco, mapeamento de comunicações e fluxos de dados, políticas de segurança cibernética, identificação de vulnerabilidades, e compartilhamento de informações sobre ameaças.

Da Proteção

A proteção envolve o gerenciamento de identidades e credenciais, autenticação de usuários e dispositivos, verificação de identidades, gerenciamento de acesso, proteção de rede através de firewalls e outros mecanismos, controle de acesso remoto, integridade da rede, conscientização e treinamento em segurança cibernética, gerenciamento de mudanças, verificação de integridade, melhoria contínua de proteção, e registro de manutenção e reparo.

Da Detecção

Para a detecção, são implementados mecanismos de alta disponibilidade e balanceamento de carga, estabelecidas linhas de base de operações de rede, análise de eventos detectados, coleta e correlação de dados, regras para geração de incidentes, monitoramento específico de segurança, detecção de códigos maliciosos, monitoramento de pessoal e conexões, comunicação de eventos detectados, e melhoria contínua dos processos de detecção.

Da Resposta

A resposta inclui um plano a ser executado durante e após um incidente, investigação de notificações de detecção de ameaças, classificação de incidentes, contenção e mitigação de incidentes, investigação forense, processos para receber, analisar e responder às vulnerabilidades, e atualização constante das estratégias de resposta.

Da Recuperação

A fase de recuperação envolve um plano a ser executado durante ou após um incidente de segurança cibernética, gerenciamento de comunicação com o público, plano de recuperação de reputação após incidentes, e constante teste e atualização do plano de recuperação. A recuperação busca restaurar a operação normal da organização após um incidente, aprendendo com a experiência e fortalecendo as defesas contra futuros incidentes.

Anexo VI - Manual de Referência – Gestão de Identidade e de Controle de Acessos

1. Diretrizes Gerais: Os órgãos do Poder Judiciário devem gerenciar a identidade e o controle de acesso de seus usuários. Isso inclui a definição de padrão de identidade, consideração de privilégios mínimos, utilização de login único, adoção de controle baseado em funções, verificações de identidade, registro de auditoria, requisitos de senha, autenticação múltipla e outros aspectos de segurança cibernética.

2. Tipos de Contas: Há diferentes tipos de contas, como contas de usuário (associadas a uma pessoa específica), contas compartilhadas (suporte a vários usuários), contas de serviço (autenticação entre sistemas), contas privilegiadas (com privilégios adicionais), e Serviços de Diretório Corporativos (centralizadas). Contas compartilhadas não são recomendadas, enquanto contas privilegiadas e de serviço devem ser monitoradas e usadas com cautela.

3. Autenticação: A autenticação confirma a identidade e autoriza o acesso ao recurso solicitado. Pode ser dividida em três tipos: algo que você sabe (senha), algo que você tem (token), e algo que você é (biometria). A autenticação multifator combina mais de um tipo, fornecendo maior garantia da identidade. Em alguns casos, a autenticação pode ser dispensada, como em informações públicas.

4. Autorização: Autorizações são permissões para usar um recurso, determinadas após a autenticação. Isso envolve princípios como o menor privilégio, separação de funções e custodiantes de dados. É incentivado o desenvolvimento de procedimentos para atender aos requisitos de autorização, como a remoção de autorizações e contas em momentos adequados.

5. Responsabilidades dos Usuários: Cada pessoa com credencial de acesso é responsável por selecionar senhas fortes, mantê-las seguras, e relatar qualquer uso não autorizado. Isso inclui a criação de senhas seguras, não compartilhamento de senhas, não reutilização de senhas em contas pessoais, alteração imediata de senhas se comprometidas, uso adequado dos privilégios, e logoff ou bloqueio de tela quando o dispositivo estiver sem supervisão.

Anexo VII - Manual de Referência – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário

1. Introdução: A política aqui estabelecida define ações permanentes para segurança cibernética no Poder Judiciário. Ela enfatiza a importância da formação de cultura e educação em segurança cibernética, atualização tecnológica e colaboração com instituições de ensino e pesquisa. A diversidade de cursos e programas de treinamento disponíveis no mercado contemporâneo deve guiar as ações do Judiciário.

2. Disposições Gerais: A Política de Educação e Cultura em Segurança Cibernética (PECSC-PJ) visa desenvolver a cultura e as habilidades em segurança cibernética, conscientização, e fomentar pesquisas e inovações. Os objetivos incluem aprimorar a

segurança cibernética, inserir o tema como estratégico, promover o conhecimento, e assegurar que os usuários compreendam suas responsabilidades. A abrangência cobre diversos aspectos de segurança, incluindo proteção de dados, continuidade operacional, e formação de profissionais.

3. Programa de Capacitação em Segurança Cibernética (PCASC-PJ): Os órgãos do Poder Judiciário devem desenvolver ações de capacitação e conscientização, incluindo programas de formação, reciclagem, pesquisa, cooperação, cursos em diversas modalidades e níveis, e temas como governança, tratamento de incidentes, forense computacional, segurança em desenvolvimento de software, entre outros. As ações devem ser adaptadas ao formato mais efetivo, seja presencial, online, ou híbrido.

4. Competências para Implementação das Ações: A responsabilidade pela implementação está dividida entre as Escolas de Formação (para a concretização da PECSC-PJ), Área de Gestão de Pessoas (para viabilizar inscrição, participação e pagamento), e Área de Comunicação Social e Institucional (para programas de divulgação e conscientização). Essas competências incluem o estabelecimento de parcerias, adoção de procedimentos, e inclusão de programas de divulgação.

5. Resultados Previstos: Os programas devem levar a uma qualificação em segurança cibernética dos profissionais de Tecnologia da Informação e Comunicação (TIC) e de Segurança da Informação (SI) e a uma educação básica em segurança cibernética para todos os usuários internos. Os órgãos do Poder Judiciário devem apresentar relatórios ao CNJ anualmente, comprovando a efetividade das ações e o desempenho dos usuários e profissionais treinados.

APOSTA ESTRATÉGICA

A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em

provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais[1].

O Grupo Revisor de Código-Fonte, instituído pela Portaria CNJ nº 131/2021, desempenha um papel fundamental na manutenção e aprimoramento da infraestrutura tecnológica do Poder Judiciário. Este grupo é encarregado de garantir que as implementações de software feitas tanto pelo Conselho Nacional de Justiça quanto pela comunidade de desenvolvedores atendam a padrões rigorosos de qualidade. Através de uma análise detalhada e revisão sistemática, o grupo foca em identificar e corrigir possíveis falhas ou vulnerabilidades no código-fonte, o que é crucial para a segurança e eficiência dos sistemas judiciários.

A relevância deste grupo se torna ainda mais evidente quando consideramos sua relação com a Plataforma Digital do Poder Judiciário (PDPJ) e com o sistema Processo Judicial Eletrônico (PJe). Ambas as plataformas são essenciais para a digitalização e otimização dos processos judiciais, facilitando o acesso e a gestão dos casos pelos cidadãos e profissionais do direito. Ao revisar e aperfeiçoar o código-fonte dessas soluções, o Grupo Revisor de Código-Fonte contribui diretamente para a estabilidade, segurança e funcionalidade desses sistemas, assegurando que eles operem de maneira eficaz e alinhada com as necessidades do sistema judicial.

Questões Estratégicas

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.

1. (FGV - 2022 - TRT - 16ª REGIÃO (MA) - Técnico Judiciário - Tecnologia da Informação) De acordo com a política pública para a governança e a gestão de processo judicial eletrônico (Resolução CNJ nº 335/2020), a Plataforma Digital do Poder Judiciário Brasileiro hospedada em nuvem pode se valer de serviço de computação em nuvem provido por pessoa jurídica de direito privado, desde que

[1] Vale deixar claro que nem sempre será possível realizar uma aposta estratégica para um determinado assunto, considerando que às vezes não é viável identificar os pontos mais prováveis de serem cobrados a partir de critérios objetivos ou minimamente razoáveis.

A) seja possível mensurar o uso dos recursos da nuvem de forma agregada por unidade federativa.

B) opere em conformidade com as normas técnica estabelecidas pela PCI DSS.

C) os recursos computacionais utilizados sejam imunes a interrupções que possam ameaçar a operação da plataforma.

D) o armazenamento dos dados seja em datacenter abrigado em território nacional.

E) as operações na nuvem sobre dados pessoais coletados sem consentimento do titular fiquem arquivadas por 24 meses.

Comentários:

Por fim, a PDPJ-Br será hospedada em nuvem, podendo utilizar serviços de computação em nuvem providos por entidades privadas, inclusive na modalidade de integrador de nuvem (broker). Essa hospedagem deverá observar critérios como armazenamento dos dados em território nacional, cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), atendimento a requisitos de disponibilidade, escalabilidade, redundância, criptografia, capacidade de mensuração individualizada do uso dos recursos da nuvem, e conformidade com normas técnicas estabelecidas pelo CNJ.

Gabarito: D

2. (FCC - 2023 - TRT - 18ª Região (GO) - Técnico Judiciário - Tecnologia da Informação) De acordo com a Resolução CNJ nº 335/2020, a Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) tem como objetivos:

I. Integrar e consolidar todos os sistemas eletrônicos do Judiciário brasileiro em um ambiente unificado.

II. Implantar o conceito de desenvolvimento centralizado, no qual todos os tribunais recebem as melhores soluções tecnológicas definidas pelo Comitê Gestor do PDPJ-Br para aproveitamento de todos.

III. Estabelecer padrões de desenvolvimento, arquitetura, experiência do usuário (User Experience – UX) e operação de software, obedecendo às melhores práticas de mercado e disciplinado pelo Comitê Gestor do PDPJ-Br.

IV. Instituir plataforma única para publicação e disponibilização de aplicações, microsserviços e modelos de inteligência artificial (I.A.) por meio de computação em nuvem.

Está correto o que se afirma em

A) I, II, III e IV.

B) I e III, apenas.

C) I e IV, apenas.

D) II e IV, apenas.

E) II e III, apenas.

Comentários:

II e III estão errados:

II - O CNJ coordenará a definição de critérios para a evolução dos sistemas, considerando o desenvolvimento comunitário, e monitorará os sistemas legados, sem interferir no desenvolvimento de soluções tecnológicas pelos tribunais, desde que justificadas pelas peculiaridades regionais ou metodologia de trabalho

III - O Ato da Presidência que disciplinar a política de governança e gestão da PDPJ-Br deverá estabelecer requisitos para os sistemas

Gabarito: C

3. (FGV - 2023 - TJ-RN - Analista Judiciário - Tecnologia de Informação – Análise de Suporte) O Tribunal de Justiça do Rio Grande do Norte, por meio do Departamento de Tecnologia, está implementando a Plataforma Digital do Poder Judiciário (PDPJ-Br) para auxiliar o trabalho de seus servidores públicos. Essa Plataforma tem como objetivo integrar e consolidar todos os sistemas eletrônicos do Judiciário brasileiro em um ambiente unificado. O Departamento de Tecnologia recebeu uma cópia da Resolução CNJ nº 335/2020, que institui essa política pública de Governança e Gestão de processos judiciais eletrônicos. Dentre as opções abaixo, o Departamento de Tecnologia deverá implementar:

A) uma solução pública existente que atenda a todos os requisitos estabelecidos na política de governança e gestão, a qual poderá ser aceita no CNJ, após aprovação da equipe técnica do PDPJ-Br;

B) o módulo anteriormente utilizado que pertencia à empresa externa e que não disponibilizava o acesso ao código fonte, documentação e quaisquer outros artefatos que venham a ser utilizados na tarefa;

C) uma força-tarefa para definir e coordenar o desenvolvimento do portal com interface nacional única para os usuários externos;

D) um censo para identificar os sistemas processuais empregados em tribunais próximos, com identificação das tecnologias empregadas, práticas de desenvolvimento utilizadas, atividade no repositório etc.;

E) a política de governança e gestão da PDPJ-Br, a qual poderá adotar um padrão de autenticação, dentre outros requisitos, face à evolução tecnológica da plataforma, nos termos disciplinados por ato da Presidência do CNJ.

Comentários:

A letra E está correta porque é possível adotar novos padrões frente às atualizações tecnológicas:

Artigo 9, Parágrafo único: A política de governança e gestão da PDPJ-Br poderá adotar outros requisitos face a evolução tecnológica da plataforma, nos termos disciplinados por ato da Presidência do CNJ.

Gabarito: E

4. (FGV - 2022 - TJ-DFT - Analista Judiciário - Suporte em Tecnologia da Informação0) A Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) foi instituída com o objetivo de incrementar a segurança cibernética nos órgãos do Poder Judiciário, abrangendo aspectos essenciais da segurança da informação e definindo objetivos para fortalecer o espaço cibernético do Poder Judiciário, assim como divulgar ações para os órgãos em seu âmbito de atuação. Um dos objetivos da ENSEC-PJ, instituída pela Resolução

CNJ nº 396/2021, é:

A) estabelecer modelo centralizado de governança cibernética nacional;

B) permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível;

C) fortalecer as ações de governança cibernética;

D) realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo;

E) estabelecer rede de cooperação do Judiciário para a segurança cibernética.

Comentários:

Resolução CNJ nº 396/2021

Art. 6º São objetivos da ENSEC-PJ:

I – tornar o Judiciário mais seguro e inclusivo no ambiente digital;

II – aumentar a resiliência às ameaças cibernéticas;

III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e

IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

Gabarito: B

5. (FGV - 2022 - TRT - 13ª Região (PB) - Analista Judiciário - Tecnologia da Informação) A Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) tem sua regulamentação instituída pela Resolução CNJ nº 396/2021 e pela Portaria CNJ nº 162/2021. Quanto às definições de eventos Cibernéticos do Poder Judiciário, assinale V para a afirmativa verdadeira e F para a falsa.

I. Na Prevenção de Incidentes Cibernéticos do Poder Judiciário são princípios críticos que asseguram a construção de sistema de segurança cibernética eficaz: base de conhecimento de

vírus, diagnóstico contínuo e automação.

II. Na Investigação para Ilícitos Cibernéticos do Poder Judiciário o protocolo tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao

Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

III. Considerando a Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, na etapa de recuperação espera-se que a organização conte com plano que preveja ações a serem executadas durante ou após um incidente e que incorpore as lições aprendidas, bem como que exista gerenciamento de comunicação com o público e um plano de recuperação de reputação após incidentes.

As afirmativas são, respectivamente,

A) F, V e V.

B) F, F e V.

C) V, F e F.

D) V, V e F.

E) V, F e V.

Comentários:

Base de Conhecimento de vírus não é um dos princípios críticos, por isso a Letra A é falsa. Veja:

O protocolo também apresenta princípios críticos adaptáveis que asseguram a construção de um sistema de segurança cibernética eficaz. Estes incluem o uso de informações de ataques reais, priorização na formação e revisão de controles, definição de métricas comuns, diagnóstico contínuo, formação e conscientização, automação, e a capacidade de resiliência.

Gabarito: A

6. (FGV - 2022 - TJ-TO - Técnico Judiciário - Informática) De acordo com o Art. 12 da Portaria CNJ nº 252/2020, que dispõe sobre o Modelo de Governança e Gestão da PDPJ-Br (Plataforma Digital do Poder Judiciário), a responsabilidade por corrigir erros e falhas e assegurar a qualidade dos artefatos depositados, bem como zelar pela estrutura e padrões de arquitetura

estabelecidos, é do(a):

A) Grupo Revisor de Código-Fonte;

B) Comitê Gestor Nacional da PDPJ;

C) Grupo Nacional de Requisitos de Negócio;

D) Grupo Nacional de Gerenciamento, Desenvolvimento e

Sustentação;

E) Comissão Permanente de Tecnologia da Informação e Infraestrutura.

Comentários:

A Gerência Executiva é responsável por orquestrar as atividades colaborativas e definir responsabilidades no desenvolvimento da Plataforma. São criados Grupos Nacionais para gerenciamento, desenvolvimento e sustentação, bem como para avaliar requisitos de negócios. A portaria também estabelece mecanismos para resolução de casos omissos.

Gabarito: D

7. (FGV - 2022 - TJ-TO - Técnico Judiciário - Informática) De acordo com o Art. 5º da Portaria CNJ nº 253/2020, os serviços que implementam as funcionalidades essenciais básicas para um sistema de processo judicial de tramitação eletrônica, bem como aqueles serviços necessários à integração, à coreografia e à interoperabilidade entre os serviços e soluções que compõem a

   PDPJ-Br (Plataforma Digital do Poder Judiciário) são os serviços:

   A) negociais;

   B) estruturantes;

   C) de integração com sistemas externos;

   D) de aplicações da comunidade externa ao Judiciário;

   E) de nuvem computacional.

   Comentários:

   Serviços Estruturantes: Implementam as funcionalidades essenciais básicas para um sistema de processo judicial de tramitação eletrônica, bem como àqueles serviços necessários à integração, à coreografia e à interoperabilidade entre os serviços e soluções que compõe a PDPJ-Br (Plataforma Digital do Poder Judiciário).

   Gabarito: B

8. (FGV - 2022 - TRT - 16ª REGIÃO (MA) - Analista Judiciário - Tecnologia da Informação) De acordo com os critérios e diretrizes técnicas para o processo de desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro, portaria CNJ nº 253/2020, é correto afirmar que

A) é obrigatória a produção de relatório de cobertura de testes automatizados.

B) os microsserviços precisam ser coesos e manter a característica statefull para permitir maior escalabilidade.

C) deve ser adotada, preferencialmente, a linguagem de programação Python para implementar microsserviços.

D) aplicações monolíticas existentes devem manter suas funcionalidades na íntegra, sem decomposição funcional.

E) as interfaces de programação de aplicações (APIs) devem ser providas por meio de tecnologia SOAP.

Comentários:

Os microsserviços devem ser versionados com Git, protegidos com OAuth2 e desenvolvidos com práticas como Continuous Integration (CI), Continuous Delivery (CD) e Test Driven Development (TDD), no qual é obrigatória a produção de relatório de cobertura de testes automatizados, o qual deverá ser atualizado a cada execução do pipeline de integração contínua.

Gabarito: A

9. (FGV - 2022 - TRT - 16ª REGIÃO (MA) - Técnico Judiciário - Tecnologia da Informação) De acordo com os critérios e diretrizes técnicas para o processo de desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro, portaria CNJ nº 253/2020, o acesso a microsserviços deve ser protegido com mecanismos de autenticação e autorização baseado em

A) LDAP.

B) Kerberos.

C) OAuth2.

D) SAML.

E) RADIUS.

Comentários:

Os microsserviços devem ser versionados com Git, protegidos com OAuth2 e desenvolvidos com práticas como Continuous Integration (CI), Continuous Delivery (CD) e Test Driven Development (TDD), no qual é obrigatória a produção de relatório de cobertura de testes automatizados, o qual deverá ser atualizado a cada execução do pipeline de integração contínua.

Gabarito: C

10. (FCC - 2022 - TRT - 23ª REGIÃO (MT) - Analista Judiciário - Área Apoio - Tecnologia da Informação) O artigo 6º da Portaria CNJ nº 131/2021 diz que os encontros do Grupo Revisor de Código-Fonte ocorrerão, prioritariamente, por meio virtual. Nos parágrafos do referido artigo, afirma-se que:

A) As sprints do Grupo Revisor possuirão periodicidade quinzenal e abarcarão todas as requisições de aceite de código (merge requests) pendentes de análise.

B) O merge request será aceito se pelo menos dois tribunais, distintos daquele que desenvolveu a funcionalidade ou solução, o aprovarem.

C) O merge request que não for expressamente aceito ou rejeitado pela gerência de TI será descartado sem a necessidade de aval do Grupo Revisor.

D) Caso o Grupo Revisor não consiga analisar todas as merge requests que compõem a sprint mensal, as que ficarem pendentes ficarão por último na próxima sprint.

E) Caberá ao Departamento de Tecnologia da Informação e Comunicação do CNJ priorizar, se for necessário, os merge requests da próxima sprint, conforme critérios de relevância nacional.

Comentários:

Os encontros ocorrerão principalmente virtualmente, com sprints quinzenais para análise de "merge requests."

Gabarito: A

11. (CESPE / CEBRASPE - 2022 - TRT - 8ª Região (PA e AP) - Técnico Judiciário - Tecnologia da Informação) Segundo a Portaria CNJ n.º 131/2021, o Grupo Revisor de Código-Fonte é responsável pela análise das mudanças no código-fonte que forem sugeridas pela comunidade de desenvolvimento nas soluções disponibilizadas na PDPJ-Br e também no sistema PJe, e seus membros desempenharão as atividades em caráter honorífico. Com relação à composição desse grupo revisor, assinale a opção correta.

A) As atividades desempenhadas pelos membros do grupo possuem caráter sigiloso, logo, não é permitida a participação de colaboradores eventuais nos projetos e reuniões.

B) O grupo será composto por membros indicados pelo Departamento de Tecnologia da Informação e Comunicação do CNJ e por representantes indicados pelos tribunais.

C) Os membros do grupo devem ser servidores efetivos e devem também possuir experiência ou formação na área de desenvolvimento de sistemas.

D) A composição do Grupo Revisor de Código-Fonte somente poderá ser revista a cada dois anos.

E) Os servidores lotados nos tribunais de Justiça estaduais e com mais de 10 anos de experiência na área de TI são considerados membros natos do Grupo Revisor de Código-Fonte.

Comentários:

O Grupo Revisor será composto por membros indicados pelo Departamento de Tecnologia da Informação e Comunicação (DTI) do CNJ, por representantes dos tribunais e por servidores lotados na Divisão do Processo Judicial Eletrônico (DPJe).

Gabarito: B

12. (FGV - 2022 - TJ-DFT - Analista Judiciário - Segurança da Informação) O Comitê de Segurança Cibernética do Poder Judiciário instituiu o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) com diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível. O PPINC-PJ baseia-se em um conjunto de boas práticas de segurança cibernéticas para melhor detectar, conter e eliminar ataques cibernéticos, minimizando eventuais impactos na operação das atividades dos órgãos. De acordo com o Anexo I, da Portaria CNJ nº 162/2021, o princípio crítico da PPINC-PJ que tem foco na formação, na revisão de controles/acessos, nos processos e na disseminação da cultura de segurança cibernética é:

A) priorização;

B) diagnóstico contínuo;

C) formação, capacitação e conscientização;

D) automação;

E) resiliência.

Comentários:

O protocolo também apresenta princípios críticos adaptáveis que asseguram a construção de um sistema de segurança cibernética eficaz. Estes incluem o uso de informações de ataques reais, priorização na formação e revisão de controles, definição de métricas comuns, diagnóstico contínuo, formação e conscientização, automação, e a capacidade de resiliência. Esses princípios visam fornecer uma estrutura flexível e robusta, contribuindo para uma cultura de segurança cibernética organizacional.

Gabarito: A

13. (CESPE / CEBRASPE - 2022 - TRT - 8ª Região (PA e AP) - Analista Judiciário - Tecnologia da Informação) De acordo com o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), instituído pela Portaria CNJ n.º 162/2021, o protocolo de prevenção a incidentes cibernéticos criado no âmbito de cada tribunal contemplará um conjunto de princípios críticos que assegurem a construção de sistema de segurança cibernética eficaz. Considerando as informações apresentadas, assinale a opção que contém o princípio que representa o poder de recuperação ou a capacidade de uma organização resistir aos efeitos de um incidente bem como impedir a reincidência secundária do incidente identificado.

A) base de conhecimento de defesa

B) priorização

C) diagnóstico contínuo

D) resiliência

E) automação

Comentários:

O protocolo também apresenta princípios críticos adaptáveis que asseguram a construção de um sistema de segurança cibernética eficaz. Estes incluem o uso de informações de ataques reais, priorização na formação e revisão de controles, definição de métricas comuns, diagnóstico contínuo, formação e conscientização, automação, e a capacidade de resiliência.

Gabarito: D

QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma auto explicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível!

Vamos ao nosso questionário:

Perguntas

1. Quais são os principais componentes necessários para estabelecer um ambiente de segurança cibernética resiliente na organização?
2. Como a organização deve gerenciar identidades e credenciais para proteção cibernética?
3. Quais são as expectativas em relação ao gerenciamento de acessos remotos e tecnologia de implementações de rede privada na organização?
4. Como a organização deve lidar com a integridade da rede para garantir a segurança cibernética?
5. Quais são os métodos recomendados para detecção de ameaças cibernéticas?
6. Como a organização deve responder a um incidente de segurança cibernética?
7. Qual é o papel da alta administração na proteção e resposta a incidentes de segurança cibernética?
8. Quais são as medidas recomendadas para a recuperação após um incidente de segurança cibernética?
9. Como a organização deve gerenciar e proteger as mídias removíveis dentro do contexto de segurança cibernética?
10. Por que é importante a implementação de um processo de melhoria contínua das soluções de proteção e detecção em segurança cibernética?
11. Qual é o objetivo principal do Grupo Revisor de Código-Fonte instituído pela Portaria CNJ nº 131/2021, e como ele se relaciona com a Plataforma Digital do Poder Judiciário (PDPJ) e o sistema Processo Judicial Eletrônico (PJe)?
12. Quais são as qualificações necessárias para os membros do Grupo Revisor de Código-Fonte, e como a composição do grupo pode ser alterada?
13. Quais são as responsabilidades dos servidores lotados na Divisão do Processo Judicial Eletrônico (DPJe) no contexto do Grupo Revisor de Código-Fonte?
14. Como o Grupo Revisor de Código-Fonte conduzirá o processo de revisão, e quais são os critérios para aceitação ou rejeição dos códigos-fonte?
15. Quem são os possíveis integrantes do Grupo Revisor de Código-Fonte, além dos servidores da Divisão do Processo Judicial Eletrônico, e como os encontros do grupo serão realizados?
16. Quais são os principais objetivos e características da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) conforme a Portaria CNJ nº 253/2020?
17. Como a Portaria CNJ nº 253/2020 define a participação da comunidade e o acompanhamento dos projetos na PDPJ-Br?
18. Quais são as práticas e tecnologias específicas recomendadas pela Portaria CNJ nº 253/2020 para o desenvolvimento na PDPJ-Br?
19. Como a Portaria CNJ nº 253/2020 aborda a questão da segurança e uso de tecnologias emergentes como Inteligência Artificial e computação em nuvem?

20. Qual é o processo para tribunais ou entes participarem do desenvolvimento na PDPJ-Br, e qual departamento do CNJ é responsável pela manutenção das diretrizes técnicas?
21. Qual é o propósito da Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), e quais são alguns dos temas contemplados por ela no Capítulo I da resolução CNJ nº 396/2021?
22. Quais são as responsabilidades do Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ) conforme o Capítulo V da resolução CNJ nº 396/2021?
23. Quais são os objetivos da Rede de Cooperação do Judiciário na área de segurança cibernética, conforme o Capítulo VI da resolução CNJ nº 396/2021?
24. Quais são os princípios, objetivos e instrumentos da Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ) conforme o Capítulo VII da resolução CNJ nº 396/2021?
25. Quais são as obrigações dos órgãos do Poder Judiciário, exceto o STF, no contexto da segurança cibernética conforme os Capítulos VI e VII da resolução CNJ nº 396/2021?
26. Quais são os principais objetivos e componentes da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) conforme definido no Capítulo I da Resolução No 335?
27. Como o Capítulo II da Resolução No 335 define a política de governança e gestão da PDPJ-Br, e quais requisitos devem ser estabelecidos para os sistemas e dados?
28. Quais são as responsabilidades do CNJ na gestão da PDPJ-Br, conforme delineado no Capítulo III da Resolução No 335?
29. Como o Capítulo IV da Resolução No 335 aborda a gestão dos sistemas atuais e a integração com a PDPJ-Br?
30. Quais são as principais medidas para garantir a eficiência operacional da PDPJ-Br e como a resolução aborda a hospedagem da plataforma em nuvem?

Perguntas e Respostas

1. Quais são os principais componentes necessários para estabelecer um ambiente de segurança cibernética resiliente na organização?
   Resposta: Os principais componentes incluem a identificação de itens críticos e de múltiplo uso, a centralização de processos, o gerenciamento e precificação de risco cibernético, o mapeamento de comunicações e fluxos de dados, a definição de políticas de segurança cibernética, e a identificação e documentação de vulnerabilidades.

2. Como a organização deve gerenciar identidades e credenciais para proteção cibernética?
   Resposta: As identidades e credenciais devem ser emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos. A autenticação deve ser feita de acordo com o risco da transação, preferencialmente usando múltiplos fatores de autenticação.
3. Quais são as expectativas em relação ao gerenciamento de acessos remotos e tecnologia de implementações de rede privada na organização?
   Resposta: É esperado que existam gerenciamento de acessos remotos e tecnologia de implementações de rede privada, utilizando, se possível, certificados pessoais e por dispositivos, para garantia de controle legítimo.
4. Como a organização deve lidar com a integridade da rede para garantir a segurança cibernética?
   Resposta: A integridade da rede deve ser protegida através da segmentação e segregação de ambientes, estabelecendo barreiras de contenção de danos e garantindo recursos para serviços prioritários.
5. Quais são os métodos recomendados para detecção de ameaças cibernéticas?
   Resposta: Os métodos recomendados incluem a implementação de mecanismos como alta disponibilidade e balanceamento de carga, estabelecimento de linhas de base de operações de rede, análise de eventos detectados, uso de sistemas como EDR e UEBA, e realização de escaneamentos de vulnerabilidades frequentes.
6. Como a organização deve responder a um incidente de segurança cibernética?
   Resposta: A organização deve executar um plano de resposta durante e após o incidente, investigar as notificações, classificar, conter e mitigar os incidentes, realizar investigação forense, e incorporar as lições aprendidas para atualizar constantemente as estratégias de resposta.
7. Qual é o papel da alta administração na proteção e resposta a incidentes de segurança cibernética?
   Resposta: A alta administração deve estar envolvida em programas de conscientização e treinamento, conhecer os procedimentos a serem adotados em cenários de crise cibernética, e ser envolvida na comunicação de incidentes quando houver comprometimento de imagem.
8. Quais são as medidas recomendadas para a recuperação após um incidente de segurança cibernética?
   Resposta: As medidas recomendadas incluem a execução de um plano de recuperação, gerenciamento de comunicação com o público, plano de recuperação de reputação, e constante teste e atualização do plano de recuperação.
9. Como a organização deve gerenciar e proteger as mídias removíveis dentro do contexto de segurança cibernética?

Resposta: As mídias removíveis devem ser protegidas e seu uso deve ser restrito de acordo com uma política específica.

10. Por que é importante a implementação de um processo de melhoria contínua das soluções de proteção e detecção em segurança cibernética?
Resposta: A melhoria contínua é vital para adaptar-se às mudanças nas ameaças e vulnerabilidades, garantir que as soluções de proteção e detecção permaneçam eficazes e alinhadas com os objetivos e requisitos da organização, e fortalecer continuamente as defesas contra incidentes futuros.

11. Qual é o objetivo principal do Grupo Revisor de Código-Fonte instituído pela Portaria CNJ nº 131/2021, e como ele se relaciona com a Plataforma Digital do Poder Judiciário (PDPJ) e o sistema Processo Judicial Eletrônico (PJe)?
Resposta: O objetivo principal do Grupo Revisor de Código-Fonte é garantir a qualidade das implementações realizadas pelo Conselho Nacional de Justiça (CNJ) e pela comunidade de desenvolvedores, analisando e revisando as mudanças no código-fonte das soluções da PDPJ e do sistema PJe.
12. Quais são as qualificações necessárias para os membros do Grupo Revisor de Código-Fonte, e como a composição do grupo pode ser alterada?
Resposta: Os membros do Grupo Revisor devem possuir experiência ou formação na área de desenvolvimento de sistemas, sendo preferencialmente servidores efetivos. A composição do Grupo Revisor de Código-Fonte pode ser revista a qualquer tempo, a critério da Gerência Executiva da PDPJ-Br.
13. Quais são as responsabilidades dos servidores lotados na Divisão do Processo Judicial Eletrônico (DPJe) no contexto do Grupo Revisor de Código-Fonte?
Resposta: Os servidores lotados na DPJe coordenarão as atividades do Grupo Revisor de Código-Fonte, convocando e coordenando as reuniões, organizando a pauta dos trabalhos, e definindo as prioridades, as metas e os objetivos do grupo.
14. Como o Grupo Revisor de Código-Fonte conduzirá o processo de revisão, e quais são os critérios para aceitação ou rejeição dos códigos-fonte?
Resposta: O Grupo conduzirá o processo de revisão principalmente virtualmente, com sprints quinzenais para análise de "merge requests." O código-fonte deve ser submetido à análise sintática automatizada, e aqueles que não atingirem os critérios mínimos serão rejeitados. A aprovação deve vir acompanhada de comprovação da realização de testes.
15. Quem são os possíveis integrantes do Grupo Revisor de Código-Fonte, além dos servidores da Divisão do Processo Judicial Eletrônico, e como os encontros do grupo serão realizados?
Resposta: Além dos servidores da DPJe, o Grupo Revisor pode incluir cinco ou mais servidores indicados por diversos órgãos judiciais, como os Tribunais de Justiça estaduais, o Conselho da Justiça Federal, o Tribunal Superior Eleitoral e o Conselho

Superior da Justiça do Trabalho. Os encontros ocorrerão prioritariamente por meio virtual.

16. Quais são os principais objetivos e características da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) conforme a Portaria CNJ nº 253/2020?
Resposta: A PDPJ-Br tem como objetivo fornecer padrões de API, modelos de dados, eventos e mensagens para permitir que desenvolvedores criem, mantenham e evoluam aplicações. A plataforma seguirá o modelo arquitetural de microsserviços com alto nível de desacoplamento e será gerida de maneira comunitária e descentralizada, envolvendo tribunais, órgãos públicos externos e particulares.
17. Como a Portaria CNJ nº 253/2020 define a participação da comunidade e o acompanhamento dos projetos na PDPJ-Br?
Resposta: A Portaria estabelece que o processo de disponibilização de soluções será comunitário, com a participação de quaisquer tribunais brasileiros, órgãos públicos externos e particulares. Os profissionais serão identificados por órgão e área de atuação, e o CNJ acompanhará a execução dos projetos através de líderes técnicos e do Escritório de Projetos.
18. Quais são as práticas e tecnologias específicas recomendadas pela Portaria CNJ nº 253/2020 para o desenvolvimento na PDPJ-Br?
Resposta: A Portaria recomenda a utilização preferencial da linguagem de programação Java com o framework Spring e a aplicação de práticas como Continuous Integration (CI), Continuous Delivery (CD), Test Driven Development (TDD) e OAuth2 para autenticação e autorização. Também são estabelecidos padrões para documentação técnica, interface gráfica e versionamento com Git.
19. Como a Portaria CNJ nº 253/2020 aborda a questão da segurança e uso de tecnologias emergentes como Inteligência Artificial e computação em nuvem?
Resposta: A Portaria estabelece mecanismos de autenticação e autorização baseados em OAuth2 e diretrizes para tratamento da informação em ambiente de Computação em Nuvem, conforme a Portaria GSI no 9/2018. Quanto à Inteligência Artificial, as soluções devem estar de acordo com os termos da Resolução CNJ no 332/2020, que disciplina ética, transparência e governança.
20. Qual é o processo para tribunais ou entes participarem do desenvolvimento na PDPJ-Br, e qual departamento do CNJ é responsável pela manutenção das diretrizes técnicas?
Resposta: Os tribunais ou entes participantes devem assinar um Termo de Cooperação Técnica e podem formalizar interesse por e-mail. O Departamento de Tecnologia da Informação e Comunicação do CNJ é responsável por prover a manutenção e detalhamento das diretrizes técnicas da Portaria.
21. Qual é o propósito da Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), e quais são alguns dos temas contemplados por ela no Capítulo I da resolução CNJ nº 396/2021?

Resposta: O propósito da ENSEC-PJ é instituir uma estratégia para a segurança da informação e cibernética no âmbito dos órgãos do Poder Judiciário, exceto o Supremo Tribunal Federal (STF). Ela contempla temas como segurança da informação de forma ampla, segurança física, proteção de dados pessoais e institucionais, disponibilidade, integridade, confidencialidade, autenticidade, continuidade operacional, planejamento, normatização, comunicação, formação técnica e acadêmica em segurança cibernética.

22. Quais são as responsabilidades do Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ) conforme o Capítulo V da resolução CNJ nº 396/2021?
Resposta: O CGSI-PJ tem a responsabilidade de assessorar o CNJ em temas relacionados à segurança da informação. Suas competências incluem estabelecer normas para a gestão de riscos, aprovar políticas, diretrizes, estratégias e recomendações, elaborar e implementar programas de conscientização e capacitação, estabelecer critérios para monitorar e avaliar a execução da PSEC-PJ, criar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CPTRIC-PJ), e promover a troca de informações com outros comitês gestores e a sociedade.
23. Quais são os objetivos da Rede de Cooperação do Judiciário na área de segurança cibernética, conforme o Capítulo VI da resolução CNJ nº 396/2021?
Resposta: Os objetivos da Rede de Cooperação incluem promover um ambiente participativo, colaborativo e seguro; estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas; realizar exercícios cibernéticos; fortalecer o CPTRIC-PJ; aperfeiçoar a estrutura judiciária para investigações de crimes cibernéticos; incentivar a criação e atuação de ETIR; emitir alertas e recomendações de segurança cibernética; e ampliar parceria com outros órgãos do poder público, setor privado e meio acadêmico.
24. Quais são os princípios, objetivos e instrumentos da Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ) conforme o Capítulo VII da resolução CNJ nº 396/2021?
Resposta: Os princípios da PSEC-PJ incluem segurança jurídica, respeito aos direitos humanos, visão sistêmica, integração e cooperação, educação e inovação, orientação à gestão de riscos, prevenção e resposta a incidentes, entre outros. Os objetivos visam contribuir para a segurança do indivíduo, sociedade e Estado, fomentar pesquisa e desenvolvimento, aprimorar normativas e fortalecer a cultura de segurança. Os instrumentos incluem a ENSEC-PJ, Protocolos de Prevenção, Gerenciamento de Crises e Investigação para Ilícitos Cibernéticos, e Manuais de Referência.
25. Quais são as obrigações dos órgãos do Poder Judiciário, exceto o STF, no contexto da segurança cibernética conforme os Capítulos VI e VII da resolução CNJ nº 396/2021?

Resposta: Os órgãos do Poder Judiciário devem aderir à Rede de Cooperação na área de segurança cibernética, com responsabilidades na governança da segurança da informação, incluindo a implementação de políticas e normas, destinação de recursos, promoção de capacitação e coordenação de ações de segurança. Eles também devem adotar e seguir os protocolos e manuais da PSEC-PJ, incluindo diretrizes para prevenção, resposta e investigação de incidentes cibernéticos, além de estabelecer ações específicas em sua Política de Segurança da Informação.

26. Quais são os principais objetivos e componentes da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) conforme definido no Capítulo I da Resolução No 335?
Resposta: Os principais objetivos da PDPJ-Br incluem a integração e consolidação de todos os sistemas eletrônicos do Judiciário brasileiro em um ambiente unificado, a implantação do desenvolvimento comunitário, o estabelecimento de padrões de desenvolvimento e arquitetura, e a instituição de uma plataforma única para publicação e disponibilização de aplicações, microsserviços e modelos de inteligência artificial. Além disso, o capítulo proíbe a contratação de sistemas que causem dependência tecnológica.
27. Como o Capítulo II da Resolução No 335 define a política de governança e gestão da PDPJ-Br, e quais requisitos devem ser estabelecidos para os sistemas e dados?
Resposta: O Capítulo II institui a política de governança e gestão da PDPJ-Br, coordenada pelo CNJ. Os requisitos estabelecidos para os sistemas incluem padrões de desenvolvimento, comunicação, interoperabilidade, arquitetura, autenticação, usabilidade, inteligência artificial e computação em nuvem. Para os dados e documentos, são definidos padrões das tabelas unificadas, bases centralizadas ou descentralizadas, padrões de dados mínimos, documentos digitais e assinaturas digitais.
28. Quais são as responsabilidades do CNJ na gestão da PDPJ-Br, conforme delineado no Capítulo III da Resolução No 335?
Resposta: O CNJ é responsável por coordenar e promover a avaliação do estágio atual dos sistemas judiciais eletrônicos, garantir a eficiência operacional da PDPJ-Br por meio de monitoramento, indicadores e metas, e observar critérios específicos para a hospedagem da PDPJ-Br em nuvem, como armazenamento em território nacional e conformidade com a Lei Geral de Proteção de Dados Pessoais.
29. Como o Capítulo IV da Resolução No 335 aborda a gestão dos sistemas atuais e a integração com a PDPJ-Br?
Resposta: O Capítulo IV aborda a manutenção e aprimoramento do projeto PJe como parte central da PDPJ-Br, a provisão de aplicações através da "nuvem nacional", a possibilidade de manutenção de outros projetos de sistema processual público, a adesão de tribunais sem projetos, e a coordenação pelo CNJ da evolução de sistemas e monitoramento dos sistemas legados. Também enfatiza a promoção de ações pelos tribunais para facilitar a troca de informações e reduzir custos.

30. Quais são as principais medidas para garantir a eficiência operacional da PDPJ-Br e como a resolução aborda a hospedagem da plataforma em nuvem?
Resposta: As principais medidas para garantir a eficiência operacional incluem agilidade na tramitação dos processos, razoável duração do processo, excelência na gestão de custos, economicidade dos recursos, responsabilidade ambiental, melhor alocação de recursos humanos e promoção do acesso à Justiça. Quanto à hospedagem em nuvem, a PDPJ-Br será hospedada em nuvem, observando critérios como armazenamento em território nacional, cumprimento da Lei Geral de Proteção de Dados Pessoais e atendimento a requisitos de disponibilidade, escalabilidade, redundância e criptografia.

Lista de Questões Estratégicas

1. (FGV - 2022 - TRT - 16ª REGIÃO (MA) - Técnico Judiciário - Tecnologia da Informação) De acordo com a política pública para a governança e a gestão de processo judicial eletrônico (Resolução CNJ nº 335/2020), a Plataforma Digital do Poder Judiciário Brasileiro hospedada em nuvem pode se valer de serviço de computação em nuvem provido por pessoa jurídica de direito privado, desde que

A) seja possível mensurar o uso dos recursos da nuvem de forma agregada por unidade federativa.

B) opere em conformidade com as normas técnica estabelecidas pela PCI DSS.

C) os recursos computacionais utilizados sejam imunes a interrupções que possam ameaçar a operação da plataforma.

D) o armazenamento dos dados seja em datacenter abrigado em território nacional.

E) as operações na nuvem sobre dados pessoais coletados sem consentimento do titular fiquem arquivadas por 24 meses.

2. (FCC - 2023 - TRT - 18ª Região (GO) - Técnico Judiciário - Tecnologia da Informação) De acordo com a Resolução CNJ nº 335/2020, a Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) tem como objetivos:

I. Integrar e consolidar todos os sistemas eletrônicos do Judiciário brasileiro em um ambiente unificado.

II. Implantar o conceito de desenvolvimento centralizado, no qual todos os tribunais recebem as melhores soluções tecnológicas definidas pelo Comitê Gestor do PDPJ-Br para aproveitamento de todos.

III. Estabelecer padrões de desenvolvimento, arquitetura, experiência do usuário (User Experience – UX) e operação de software, obedecendo às melhores práticas de mercado e disciplinado pelo Comitê Gestor do PDPJ-Br.

IV. Instituir plataforma única para publicação e disponibilização de aplicações, microsserviços e modelos de inteligência artificial (I.A.) por meio de computação em nuvem.

Está correto o que se afirma em

A) I, II, III e IV.

B) I e III, apenas.

C) I e IV, apenas.

D) II e IV, apenas.

E) II e III, apenas.

3. (FGV - 2023 - TJ-RN - Analista Judiciário - Tecnologia de Informação – Análise de Suporte) O Tribunal de Justiça do Rio Grande do Norte, por meio do Departamento de Tecnologia, está implementando a Plataforma Digital do Poder Judiciário (PDPJ-Br) para auxiliar o trabalho de seus servidores públicos. Essa Plataforma tem como objetivo integrar e consolidar todos os sistemas eletrônicos do Judiciário brasileiro em um ambiente unificado. O Departamento de Tecnologia recebeu uma cópia da Resolução CNJ nº 335/2020, que institui essa política pública de

Governança e Gestão de processos judiciais eletrônicos. Dentre as opções abaixo, o Departamento de Tecnologia deverá implementar:

A) uma solução pública existente que atenda a todos os requisitos estabelecidos na política de governança e gestão, a qual poderá ser aceita no CNJ, após aprovação da equipe técnica do PDPJ-Br;

B) o módulo anteriormente utilizado que pertencia à empresa externa e que não disponibilizava o acesso ao código fonte, documentação e quaisquer outros artefatos que venham a ser utilizados na tarefa;

C) uma força-tarefa para definir e coordenar o desenvolvimento do portal com interface nacional única para os usuários externos;

D) um censo para identificar os sistemas processuais empregados em tribunais próximos, com identificação das tecnologias empregadas, práticas de desenvolvimento utilizadas, atividade no repositório etc.;

E) a política de governança e gestão da PDPJ-Br, a qual poderá adotar um padrão de autenticação, dentre outros requisitos, face à evolução tecnológica da plataforma, nos termos disciplinados por ato da Presidência do CNJ.

4. (FGV - 2022 - TJ-DFT - Analista Judiciário - Suporte em Tecnologia da Informação0) A Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) foi instituída com o objetivo de incrementar a segurança cibernética nos órgãos do Poder Judiciário, abrangendo aspectos essenciais da segurança da informação e definindo objetivos para fortalecer o espaço cibernético do Poder Judiciário, assim como divulgar ações para os órgãos em seu âmbito de atuação. Um dos objetivos da ENSEC-PJ, instituída pela Resolução

CNJ nº 396/2021, é:

A) estabelecer modelo centralizado de governança cibernética nacional;

B) permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível;

C) fortalecer as ações de governança cibernética;

D) realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo;

E) estabelecer rede de cooperação do Judiciário para a segurança cibernética.

5. (FGV - 2022 - TRT - 13ª Região (PB) - Analista Judiciário - Tecnologia da Informação) A Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) tem sua regulamentação instituída pela Resolução CNJ nº 396/2021 e pela Portaria CNJ nº 162/2021. Quanto às definições de eventos Cibernéticos do Poder Judiciário, assinale V para a afirmativa verdadeira e F para a falsa.

I. Na Prevenção de Incidentes Cibernéticos do Poder Judiciário são princípios críticos que asseguram a construção de sistema de segurança cibernética eficaz: base de conhecimento de

vírus, diagnóstico contínuo e automação.

II. Na Investigação para Ilícitos Cibernéticos do Poder Judiciário o protocolo tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

III. Considerando a Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, na etapa de recuperação espera-se que a organização conte com plano que preveja ações a serem executadas durante ou após um incidente e que incorpore as lições aprendidas, bem como que exista gerenciamento de comunicação com o público e um plano de recuperação de reputação após incidentes.

As afirmativas são, respectivamente,

A) F, V e V.

B) F, F e V.

C) V, F e F.

D) V, V e F.

E) V, F e V.

6. (FGV - 2022 - TJ-TO - Técnico Judiciário - Informática) De acordo com o Art. 12 da Portaria CNJ nº 252/2020, que dispõe sobre o Modelo de Governança e Gestão da PDPJ-Br (Plataforma Digital do Poder Judiciário), a responsabilidade por corrigir erros e falhas e assegurar a qualidade dos artefatos depositados, bem como zelar pela estrutura e padrões de arquitetura

   estabelecidos, é do(a):

   A) Grupo Revisor de Código-Fonte;

   B) Comitê Gestor Nacional da PDPJ;

   C) Grupo Nacional de Requisitos de Negócio;

   D) Grupo Nacional de Gerenciamento, Desenvolvimento e Sustentação;

   E) Comissão Permanente de Tecnologia da Informação e Infraestrutura.

7. (FGV - 2022 - TJ-TO - Técnico Judiciário - Informática) De acordo com o Art. 5º da Portaria CNJ nº 253/2020, os serviços que implementam as funcionalidades essenciais básicas para um sistema de processo judicial de tramitação eletrônica, bem como aqueles serviços necessários à integração, à coreografia e à interoperabilidade entre os serviços e soluções que compõem a

   PDPJ-Br (Plataforma Digital do Poder Judiciário) são os serviços:

   A) negociais;

B) estruturantes;

C) de integração com sistemas externos;

D) de aplicações da comunidade externa ao Judiciário;

E) de nuvem computacional.

8. (FGV - 2022 - TRT - 16ª REGIÃO (MA) - Analista Judiciário - Tecnologia da Informação) De acordo com os critérios e diretrizes técnicas para o processo de desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro, portaria CNJ nº 253/2020, é correto afirmar que

A) é obrigatória a produção de relatório de cobertura de testes automatizados.

B) os microsserviços precisam ser coesos e manter a característica statefull para permitir maior escalabilidade.

C) deve ser adotada, preferencialmente, a linguagem de programação Python para implementar microsserviços.

D) aplicações monolíticas existentes devem manter suas funcionalidades na íntegra, sem decomposição funcional.

E) as interfaces de programação de aplicações (APIs) devem ser providas por meio de tecnologia SOAP.

9. (FGV - 2022 - TRT - 16ª REGIÃO (MA) - Técnico Judiciário - Tecnologia da Informação) De acordo com os critérios e diretrizes técnicas para o processo de desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro, portaria CNJ nº 253/2020, o acesso a microsserviços deve ser protegido com mecanismos de autenticação e autorização baseado em

A) LDAP.

B) Kerberos.

C) OAuth2.

D) SAML.

E) RADIUS.

10. (FCC - 2022 - TRT - 23ª REGIÃO (MT) - Analista Judiciário - Área Apoio - Tecnologia da Informação) O artigo 6º da Portaria CNJ nº 131/2021 diz que os encontros do Grupo Revisor de Código-Fonte ocorrerão, prioritariamente, por meio virtual. Nos parágrafos do referido artigo, afirma-se que:

A) As sprints do Grupo Revisor possuirão periodicidade quinzenal e abarcarão todas as requisições de aceite de código (merge requests) pendentes de análise.

B) O merge request será aceito se pelo menos dois tribunais, distintos daquele que desenvolveu a funcionalidade ou solução, o aprovarem.

C) O merge request que não for expressamente aceito ou rejeitado pela gerência de TI será descartado sem a necessidade de aval do Grupo Revisor.

D) Caso o Grupo Revisor não consiga analisar todas as merge requests que compõem a sprint mensal, as que ficarem pendentes ficarão por último na próxima sprint.

E) Caberá ao Departamento de Tecnologia da Informação e Comunicação do CNJ priorizar, se for necessário, os merge requests da próxima sprint, conforme critérios de relevância nacional.

11. (CESPE / CEBRASPE - 2022 - TRT - 8ª Região (PA e AP) - Técnico Judiciário - Tecnologia da Informação) Segundo a Portaria CNJ n.º 131/2021, o Grupo Revisor de Código-Fonte é responsável pela análise das mudanças no código-fonte que forem sugeridas pela comunidade de desenvolvimento nas soluções disponibilizadas na PDPJ-Br e também no sistema PJe, e seus membros desempenharão as atividades em caráter honorífico. Com relação à composição desse grupo revisor, assinale a opção correta.

A) As atividades desempenhadas pelos membros do grupo possuem caráter sigiloso, logo, não é permitida a participação de colaboradores eventuais nos projetos e reuniões.

B) O grupo será composto por membros indicados pelo Departamento de Tecnologia da Informação e Comunicação do CNJ e por representantes indicados pelos tribunais.

C) Os membros do grupo devem ser servidores efetivos e devem também possuir experiência ou formação na área de desenvolvimento de sistemas.

D) A composição do Grupo Revisor de Código-Fonte somente poderá ser revista a cada dois anos.

E) Os servidores lotados nos tribunais de Justiça estaduais e com mais de 10 anos de experiência na área de TI são considerados membros natos do Grupo Revisor de Código-Fonte.

12. (FGV - 2022 - TJ-DFT - Analista Judiciário - Segurança da Informação) O Comitê de Segurança Cibernética do Poder Judiciário instituiu o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) com diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível. O PPINC-PJ baseia-se em um conjunto de boas práticas de segurança cibernéticas para melhor detectar, conter e eliminar ataques cibernéticos, minimizando eventuais impactos na operação das atividades dos órgãos. De acordo com o Anexo I, da Portaria CNJ nº 162/2021, o princípio crítico da PPINC-PJ que tem foco na formação, na revisão de controles/acessos, nos processos e na disseminação da cultura de segurança cibernética é:

A) priorização;

B) diagnóstico contínuo;

C) formação, capacitação e conscientização;

D) automação;

E) resiliência.

13. (CESPE / CEBRASPE - 2022 - TRT - 8ª Região (PA e AP) - Analista Judiciário - Tecnologia da Informação) De acordo com o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), instituído pela Portaria CNJ n.º 162/2021, o protocolo de prevenção a incidentes cibernéticos criado no âmbito de cada tribunal contemplará um conjunto de princípios críticos que assegurem a construção de sistema de segurança cibernética eficaz. Considerando as informações apresentadas, assinale a opção que contém o princípio que representa o poder de recuperação ou a capacidade de uma organização resistir aos efeitos de um incidente bem como impedir a reincidência secundária do incidente identificado.

A) base de conhecimento de defesa

B) priorização

C) diagnóstico contínuo

D) resiliência

E) automação

Gabaritos

1. D
2. C
3. E
4. B
5. A
6. D
7. B
8. A
9. C
10. A
11. B

12. A
13. D

GABARITOS E COMENTÁRIOS

GABARITOS E COMENTÁRIOS

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.