Sugestões Consulta Pública

Resolução Estratégia Nacional Segurança Cibernética

Nome	Órgão/Empresa	2. Sugestões na Resolução “Estratégia Nacional Segurança Cibernética"	Observações
Bruna Pozzebon	Câmara dos Vereadores de Cabo Frio - RJ	Prezados, parabenizo a iniciativa e o excelente trabalho encampado pela Cibersegurança do Poder Judiciário. Em virtude da lentidão na estratégia nacional em defesa da cibersegurança do país, empreendimento que deve ser um movimento coletivo em todas as esferas dos poderes, seguem mais argumentos pertinentes sobre a necessidade, além e junto ao Poder Judiciário, de incentivarmos a campanha nacional de cibersegurança em nosso país, como ocorre nos E.U.A. Referência: A estratégia Nacional Capacitação em Cibersegurança dos Estados Unidos. Porquê o Brasil não tem? https://cecyber.com/noticias/a-estrategia-nacional-capacitacao-em-ciberseguranca-dos-estados-unidos-por-que-o-brasil-nao-tem/	Sugestão prejudicada. Já há previsão de política de capacitação dentre os anexos submetidos à consulta pública.
Said Ahmad Karfan Neto	TJMT	Parágrafo Único II - segurança física e proteção de dados pessoais e institucionais	Sugestão prejudicada. Já consta do texto original.
Edvaldo Ferreira Chaves	TRT18	Parágrafo único do Art. 1º e inciso I Sugestão: Inverter a ordem, Segurança Cibernética por Segurança da Informação. Conforme definido no Art. 2 do Decreto Nº 9.637, de 26 de dezembro de 2018 da Presidência da República (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm) a Segurança Cibernética é uma	Sugestão parcialmente acolhida. O comitê deliberou incluir no glossário texto indicando claramente que Segurança Cibernética é uma das dimensões da Segurança da Informação.

		dimensão da Segurança da informação, e não o contrário como consta no parágrafo único do Art. 1º da presente minuta.	
Claudson Correia Melo Freitas	TJAL	Art. 3º, sugestão: 1) "A fim de melhorar a segurança cibernética tanto no trabalho quanto na vida pessoal dos servidores do poder judiciário, se faz necessária uma instrução mínima de todos os servidores. Uma vez que, tendo uma mínima instrução sobre o que é a internet, como funciona a internet e o trafego de informações, tal conhecimento garantirá uma melhora, pois evitará que servidores do poder judiciário acessem alguns sites hackers, armadilhas, etc."; 2) "Investir em programas de defesa cibernética, tais como: "VPN's, Proxy's, etc.".	1) Sugestão prejudicada. A capacitação já está prevista na política. 2) Sugestão prejudicada. Já há previsão no texto.
Ana Lucia Lourenço	TJPR	A maioria dos Tribunais, inclusive o Tribunal de Justiça do Paraná já editou resolução em razão da entrada em vigor da LGPD, estabelecendo a criação de Comitê de Segurança da Informação e Proteção de Dados Pessoais. O art. 20 da Resolução proposta pelo CNJ prevê que:" Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir Comitê de Governança de Segurança da Informação (CGS). Sugiro para evitar a duplicidade de comitês com atribuições similares, bem como o conflito de decisões, que seja acrescentado um dispositivo ressalvando a desnecessidade de criação de um novo comitê para os Tribunais que já o instituíram nos moldes da implementação da LGPD	Sugestão rejeitada. Não há imposição de criação de comitê específico. O Tribunal pode optar por atribuir novas competências a comitê já existente.
Felipe Valente da Silva Paiva	Fundação Santiago e Montesuma	Faço menção ao art. primeiro da resolução onde fala sobre segurança dos sistemas , é necessário que seja feito um banco de dados onde o servidor de vocês possam ter um sistema de trava automática para que assim os invasores possam cair sempre em uma ante sala e nunca conseguirem entrar no núcleo onde fica armazenado , pra isso é necessário que haja uma analise por um engenheiro de computação	Sugestão rejeitada. Foge ao escopo da estratégia, por se tratar de sugestão de implementação operacional.

Alessandro Sousa	Dell Technologies	De maneira análoga ao descrito no Art. 11. Inciso VII para os endpoints, incluir um inciso relativo à elaboração de requisitos específicos de segurança cibernética dos equipamentos que compõe o datacenter/nuvem: XII – elaborar requisitos específicos de segurança cibernética relativos aos equipamentos que compõem o datacenter/nuvem, ou seja, equipamentos que processam, armazenam ou trafegam informações sensíveis, tais como equipamentos de rede, de processamento (servidores) e de armazenamento de dados.	Sugestão acolhida. Alterar o inciso VII para: “VII – elaborar requisitos específicos de segurança cibernética relativos aos ativos sob sua jurisdição, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive computadores portáteis e telefones celulares;”
Luiz Antônio Mendes Garcia	CSJT	No Capítulo V, Art 15. "Integram o CGSI-PJ" , vimos sugerir a inserção de um inciso acrescentando um especialista representante do Conselho Superior da Justiça do Trabalho - CSJT como integrante do Comitê Gestor de Segurança da Informação do Poder Judiciário. Muito embora a composição atual do Comitê possua um representante do Tribunal Superior do Trabalho, a Justiça do Trabalho é formada também por 24 Tribunais Regionais do Trabalho, além de contar com um órgão superior de controle, supervisão administrativa e normatização, o CSJT, ao qual se subordinam todos os 24 Regionais. A atual representação da Justiça do Trabalho no Comitê mostra-se incompleta e insuficiente, dadas as características e o porte da justiça trabalhista. Impende ressaltar que, no caso da Justiça Federal, o CJF foi elencado para indicar um representante para o Comitê. De forma análoga e por questões de coerência normativa, mostra-se imperiosa a representação também por parte do CSJT. É o que temos a sugerir.	Sugestão acolhida. Incluir o CSJT como integrante do Comitê Gestor de Segurança da Informação do Poder Judiciário.
Murilo de Barros Carneiro	TRT18	Ao que tudo indica, há um erro material na definição de "Segurança Cibernética" no parágrafo único do art. 1º. Como bem definido no último CONSIDERANDO da minuta, Segurança da Informação é mais amplo que Segurança Cibernética, assim, a definição dada a Segurança Cibernética no referido parágrafo único está equivocada, pois os incisos I, II e III claramente estão relacionadas à Segurança da Informação e não	Sugestão acolhida para incorporar parágrafo único ao artigo que detalhe melhor o escopo da segurança cibernética e suas fronteiras com a segurança da informação: “Parágrafo único. Entende-se por segurança cibernética: I – Temas relacionados à

		à Segurança Cibernética. O equívoco pode trazer grande prejuízo, uma vez que atribuirá à Tecnologia da Informação temas que não são de sua responsabilidade, mas sim de outras áreas, fazendo com que o tema seja relegado por outras instâncias dos Órgãos.	segurança da informação, de uma forma ampla, que sejam essenciais para segurança cibernética.II – segurança física e proteção de dados pessoais e institucionais, nos aspectos relacionados à cibersegurança; III – segurança física e proteção de ativos de tecnologia da informação de forma geral;”

Rivadávia Borges Vianna	TRT18	CAPÍTULO I, art. 1º, Parágrafo único e inciso I MOTIVAÇÃO DAS SUGESTÕES: O termo "segurança cibernética" não está definido no "Anexo VIII - Glossário" e o entendimento do que é, expressado no referido inciso, contradiz de certa forma o último CONSIDERANDO desta minuta de Resolução. Tal entendimento passa uma mensagem invertida em relação ao termo "segurança da informação" utilizado pelo Executivo Federal, em sua Política Nacional de Segurança da Informação, Decreto 9.637/2018, art. 2º, pois aquele Poder, que também é fonte de referência para a construção de componentes da ENSEC-PJ, entende que "segurança cibernética está contida em segurança da informação", podendo ser compreendida como "segurança da informação aplicada ao espaço/ambiente/contexto cibernético" (minha conclusão). O reforço de uma definição clara a respeito desses dois termos também ajudará a compreender o porque da necessidade de criação de diversos Comitês relacionados a segurança da informação, segurança cibernética e proteção de dados pessoais, e o modo em que se harmonizarão seus escopos de trabalho, evitando-se sobreposições, retrabalho e desentendimento. SUGESTÕES: a) Definir no Glossário os termos "segurança da Informação" e segurança cibernética", se possível fazendo a relação entre as ambos e, no que couber, a LGPD (contém/contido ou intersecção, se esta for a ideia). b) Alterar parágrafo único e seu inciso I, que passariam ter a seguinte redação: "Art. 1º ... Parágrafo único. Para efeito desta Resolução, entende-se por segurança cibernética:	Itens a, b e c: Sugestões prejudicadas, pela alteração já realizada em virtude de sugestão anterior. Art. 6 inc IV: Sugestão rejeitada para não restringir escopo. Demais sugestões: Sugestões acolhidas para corrigir os erros materiais.

		I - segurança da informação aplicada ao contexto cibernético; ..." c) Como opção aos itens "a" e "b" acima, que seria o ideal, dever-se-ia clarear a mensagem para todos os níveis de audiência (do leigo ao especialista) especificando o escopo dos termos "segurança da informação" e "segurança cibernética" quando utilizados na ENTIC-JUD, ENSEC-PJ e Res. 363/2021, indicando quando os mesmos se aplicam a dado/informação em meio digital/cibernético ou em outro meio (papel, por exemplo) e ajustar tais resoluções/minutas/portarias/anexos, para que o eventual uso intercalado desses termos dentro dos documentos que compõem a ENSEC-PJ e outros documentos providos pelo CNJ não confundam o leitor. CAPÍTULO III, art. 6º, inciso IV MOTIVAÇÃO e SUGESTÃO: o inciso IV não estabelece o escopo, a exemplo dos demais incisos do mesmo artigo, podendo ser alcançado adicionando-se o seguinte texto ao seu final: "quando a descontinuidade for motivada por ameaça cibernética". CAPÍTULO VI, art. 18, inciso VIII MOTIVAÇÃO DA SUGESTÃO: erro material; SUGESTÃO: substituir "dapolítica" por "da política". CAPÍTULO VI, art. 21, inciso IV MOTIVAÇÃO DA SUGESTÃO: erro material;	

		SUGESTÃO: substituir "a demais" por "as demais". CAPÍTULO VII, art. 25, inciso I, II e III e arts. de 26 a 31. MOTIVAÇÃO DA SUGESTÃO: erro material; SUGESTÃO: alinhar as siglas e/ou nomes dos protocolos àqueles utilizados na minuta de Portaria que aprova os protocolos e manuais de segurança cibernética do PJ.	

Daniel Wobeto	TRE-RS	Art. 21, §2º", I - O Gestor de Segurança da Informação, desvinculado da área de TIC, deve COORDENAR A ETIR. Tenho dúvidas se esse comando é o mais adequado. Aliás, parece que a ENTIC-JUD e a ENSEC-PJ estão promovendo uma inversão de papéis. A ENTIC-JUD determina que o Titular da Área de TIC deve coordenar o Comitê Gestor de Segurança da Informação multidisciplinar. Parece-me que deveria ser o Gestor de Segurançda da Informação o responsável por dar andamento às atribuições desse comitê, multidisciplinar por definição, reafirmando-se o conceito de que Segurança da Informação não é "só TI". Por outro lado, as atividades da ETIR são eminentemente técnicas, ainda que presente o dever de colaboração e comunicação com outras áreas do tribunal. Assim, pondero que deveria ficar a coordenação dessa atividade a cargo da área de TIC. Além disso, o comando normativo aqui questionado pode prejudicar a implementação das ETIR na medida que órgãos demorarem a instituir essa área de segurança ligada à Alta Administração. Por isso, proponho que seja indicado que a ETIR deverá ser coordenada pela área de TIC. Outra alternativa seria simplesmente remover essa indicação de quem comandará a ETIR. Art. 10. Sugiro que se inclua a recomendação de uso de tecnologias para "proteção de senhas de usuários privilegiados". Art. 31. Não encontrei razão para que as recomendações do Art. 31 não estejam incluídas no Art. 10, suprimindo-se esse Art. 31.	Sugestão 1 acolhida para retirar o inciso. Sugestão 2: Sugestão rejeitada para não incluir o inciso para não tornar demasiado específico o texto da estratégia. Como trata-se de questão importante a se mencionar, verificar se há a menção de texto acerca da "proteção de senhas de usuários privilegiados" nos anexos IV, V e VI. Sugestão 3: Sugestão rejeitada. Não se vislumbrou razão para mescla dos artigos.

Thiago da Silva Gilla	TRT8	A sugestão faz referência ao art. 21. Conforme definido, é importante que a estrutura de segurança da informação seja subordinada diretamente à alta administração do órgão e desvinculada da área de TIC. Tal artigo contribui para a transparência da segurança da informação no órgão e permite "independência" em relação a área de TIC. Entretanto, com o Programa Justiça 4.0, haverá aumento da adoção da tecnologia da informação nos serviços prestados pelo judiciário e, proporcionalmente, haverá aumento do número de ataques cibernéticos. É importante que essa estrutura de segurança esteja altamente voltada para a gestão, controle e conformidade. Para isso, a gestão deve ser isolada das atividades de operação de ativos, de forma que a unidade de segurança da informação possa realizar o controle e a conformidade de forma imparcial. Dessa forma, a sugestão é que seja explicitado em parágrafo, no art. 21, que a responsabilidade pela operação de ativos como firewalls, webproxy e antivírus permanece atribuída à área de TIC.	Sugestão acolhida, para alteração do texto do Art. 21 para: “Art. 21. Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir estrutura de gestão de segurança da informação, subordinada diretamente à alta administração do órgão e desvinculada da área de TIC.”

Hetug Sardeiro Porto	TRT5 (Bahia)	Art. 2º, § 2º - Sugestão: Alterar redação para: “O aprimoramento do nível de maturidade é atingido por meio da definição, implementação, monitoramento e melhoria dos controles de tratamento de risco…” Art. 11, V - Dúvida: Esclarecer melhor quais tipos de tecnologia se aplicam. Art. 20 - Sugestão: Acrescentar as seguintes competências ao CGSI: - decidir sobre priorização das ações de segurança da informação; - decidir sobre aceitação de riscos de segurança da informação. Art. 31, III - Dúvida: Considerando que o TRT da 5ª Região não custeia a realização de provas de certificação, exceto em casos excepcionais e devidamente justificados, quem deverá custear as despesas para realização de provas de certificação internacional? Em caso das despesas correrem por conta do órgão, quais as consequências para o profissional que não conseguir aprovação nas provas de certificação? Art. 32, Parágrafo único - Dúvida: O padrão a ser adotado refere-se à AAA (Authentication, Authorization and Accounting) com Single Sign-On? Ou trata-se de padronização do formato de nomes e senhas de usuários?	Sugestão 1: Sugestão rejeitada. Sugere-se a manutenção do texto original Sugestão 2: Sugestão rejeitada. Sugere-se manter o texto inalterado Sugestão 3: Sugestão acolhida para incorporar as sugestões de inclusão de competências, no inciso II, conforme abaixo: “II – propor alterações na política de segurança da informação e deliberar sobre assuntos a ela relacionados, INCLUINDO atividades de priorização de ações e gestão de riscos de segurança;” Sugestão 4: Sugestão rejeitada. A questão deve ser tratada por cada tribunal, considerando sua autonomia administrativa. Sugestão 5: Sugestão rejeitada. A especificidade será tratada por cada tribunal, não cabendo detalhar na estratégia.

Marco Aurélio Barbosa Schaan	TRF4	Capitulo I, Art. 1º, V (Continuidade). Desde 2008 o CJF pede que o TRF4 faça o PCN, até hoje ele não foi elaborado. O CNJ em 2015, faz a mesma solicitação e no PEJF-PETI-PDTI 2015-2020 ele não foi elaborado. Com a pandemia de 2020 e, certamente, com um atraso de alguns meses em relação a OMS, o TRF4 continuou funcionando e julgando processos, mesmo sem ter um PCN ou PCSTIC. Isso é preocupante, pois diante de uma grande pandemia não foi necessário um PCN para a continuidade. Portanto, o referido plano ele fica cada vez mais postergado. O conhecimento tácito de certos servidores ficam restrito a eles. Para se ter um PCN deve ser elaborado com muito cuidado. Agora o CNJ faz uma espécie de PCN para crise cibernética. Pois bem, como não se tem um PCN normal para todas as ocorrências será mais uma solicitação que será feita, mas não na sua totalidade. De 2008, quando o CJF verificou a necessidade de segurança da informação foi solicitado um responsável pela área até hoje não existe. Agora que a guerra cibernética se colocou a frente dos interesses o CNJ pede que se tome as devidas providências que a julgar serão tomadas, mas com que atraso.	Sugestão rejeitada. Não há alterações concretas a serem realizadas no texto.
Deborah Araujo Santos Pondelek	TJPR	Cap. I, VII: incluir "educação e responsabilização pelos danos causados direta ou indiretamente"; Cap VII, Art 23, VII e 24, VII, "e": "prevenção, diagnóstico, tratamento e inovação"; Art.31:"condicionado à efetiva contribuição correspondente ao mesmo período na instituição promotora"; Cap VIII, Art32, caput: "com revisão periódica".	Sugestão 1: Sugestão rejeitada. Não se vislumbra a necessidade de incorporação do texto. Sugestão 2: sugestão parcialmente acolhida. Alterar o Art. 23, V para: “Art 23 - V – educação e inovação como alicerce fundamental para o fomento da cultura em segurança cibernética;” Não se vislumbra necessidade de alteração do art. 24. Sugestão 3: sugestão rejeitada. Não há necessidade de incorporação da sugestão ao texto, já que cada tribunal possui autonomia

			para lidar com o tema, e já há jurisprudência pacificada sobre a matéria. Sugestão 4: Sugestão prejudicada. Já está contemplada no corpo do texto.
Egon Schaden Junior	Associação Nacional de Certificação Digital ANCD	"Art. 31. Cada Tribunal, com exceção do Supremo Tribunal Federal, deverá estabelecer em sua Política de Segurança da Informação ações para: (...) V - utilizar os recursos de soluções de criptografia, ampliando o uso de assinaturas eletrônicas qualificadas nas interações entre os órgãos do Judiciário e destes com os cidadãos, nos termos da Lei 14.063/2020 e demais legislações específicas; (...)" Justificativa: A Lei 14.063/2020, convertida da Medida Provisória 983/2020, suscitou longas e importantes discussões neste Congresso Nacional no que diz respeito ao uso de assinaturas eletrônicas nas interações entre entes públicos da Administração Pública e destes para com seus administrados. Foi após discussões técnicas no Legislativo que a então Medida Provisória, transformada em Projeto de Lei de Conversão, e posteriormente sancionada pela Presidência da República que o tema de assinaturas eletrônicas no poder público tornou-se mais didático e amplo. Apesar das recentes discussões em torno do uso de assinaturas eletrônicas, importa rememorar que as assinaturas qualificadas, portadoras de certificados digitais no padrão ICP-Brasil, portanto mais seguras e íntegras, são utilizadas há bastante tempo, sendo regulamentadas por meio da Medida Provisória 2.200-2/2001. Nesse sentido, uma vez que o objetivo da atual Consulta Pública é a	Sugestão rejeitada. Os anexos IV, V e VI já contemplam as questões relacionadas à criptografia e assinaturas digitais.

		criação de uma Estratégia Nacional de Segurança Cibernética para os órgãos do poder judiciário, principalmente frente a um cenário de recorrentes ataques e ameaças cibernéticas aos sistemas da Justiça do Brasil, é oportuno e prudente que a digitalização de documentos e a assinatura de atos dos órgãos de justiça sejam feitos mediante o uso de assinaturas eletrônicas que garantam maior nível de segurança, integridade e rastreabilidade.	
Valéria Freitas Vargens	TRE-MG	Sugiro eliminar o art. 1º e inserir um glossário com todas as definições no início da Resolução. No art. 8º, informar que a implementação será gradual, por meio de plano de trabalho a ser formalizado por cada órgão, conforme critérios prioritários e art. 40. Especificar melhor o art. 10, ficou muito vago. Quais recomendações do CNJ, são tantas, especificar . Os objetivos da política (PSEC-PJ) expostos no art. 24 parecem se misturar com os objetivos e ações da estratégia (ENSEC-PJ), arts. 6º e 9º;	Sugestão 1: Sugestão acolhida e já incorporada em sugestões anteriores. Sugestão 2: Sugestão rejeitada. A implementação não será gradual, porém definida conforme a priorização do art. 40. Sugestão 3: Sugestão rejeitada. A especificação caberá a cada Tribunal. Sugestão 4: Sugestão rejeitada. Decide-se por manter o texto atual, por não haver contradições no texto.
Diógenes Antônio Tavares Paiva	TRE-PB	Os incisos I, II e III do parágrafo único do Art. 1º devem compor a definição do termo "segurança cibernética" no Anexo VIII – Glossário. Os incisos IV, V, VI, VII e VIII do parágrafo único do Art. 1º não são parte da definição da segurança cibernética, mas se tratam de ações que contribuem para ela. Assim, esse parágrafo poderia ter a seguinte redação: "Contribuem para a segurança cibernética:". Neste caso,	Sugestões 1 e 2: acolhidas e já contempladas nas alterações advindas de sugestões anteriores.

		contendo apenas o conteúdo dos atuais incisos IV, V, VI, VII e VIII. Melhor seria ter o glossário como o Art. 2º no Capítulo I - Disposições Gerais, pois é essencial para o entendimento da norma. O título do Capítulo II pode ser "Da Visão, dos Objetivos e das Ações da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)", suprimindo o Capítulo III atual, pois também trata de objetivos da ENSEC-PJ. Neste caso, o artigo correspondente à visão se tornaria o primeiro do Capítulo II. Os atuais artigos 2º e 6º podem ser fundidos, pois descrevem os objetivos da ENSEC-PJ. Os artigos 26 a 29 são, na verdade, detalhamentos dos incisos do artigo 25, devendo ser parágrafos deste.	Sugestão 3: Sugestão rejeitada. Inviável, já que o glossário aborda termos utilizados em todos os normativos e anexos. Sugestões 4, 5 e 6: Sugestão rejeitada. Alterações redacionais sem alteração substancial de conteúdo.

Paulo Roberto Mendes	TRE-MG	Fazer referência à definição clara e concisa de segurança cibernética no glossário, eliminando o parágrafo único do art. 1º por ser confuso (a segurança é alcançada por meio de ações, mas não é, em si, um conjunto de ações); Eliminar o §1º do art. 2º por ser inútil; No art. 3º, definir melhor o que é “estratégia”, “política”, “diretrizes”, “manual”, “protocolo”, “modelo”, etc, fazendo referência ao glossário; No art. 8º, citar que a implementação será gradual, por meio de plano de trabalho a ser formalizado por cada órgão, conforme critérios prioritários e art. 40; Alguns incisos do art. 9º parecem ser objetivos (ver art. 6º) e não propriamente ações; Especificar melhor o art. 10. Se for o caso, citar o alinhamento deste ato à PSI ou POSIC (política de segurança da informação) do órgão (conforme mencionado no art. 31) e à PGR (política de gestão de riscos corporativos) do órgão; O inciso I do art. 11 se refere ao protocolo do anexo? Se sim, explicitar; Os objetivos da política (PSEC-PJ) expostos no art. 24 parecem se misturar com os objetivos e ações da estratégia (ENSEC-PJ), arts. 6º e 9º; Os arts. 26 a 30 parecem ser detalhamentos dos incisos do art. 25, cabendo ser parágrafos deste ou mesmo transferidos para os respectivos anexos;	Sugestão 1: Sugestão acolhida e já tratada em alteração anterior. Sugestão 2: Sugestão rejeitada. Considera-se importante a manutenção do texto, para restringir o escopo da estratégia e política à segurança cibernética. Sugestão 3: Sugestão rejeitada. Entende-se que as definições do glossário são suficientes, sem necessidade de menção posterior Sugestão 4: Sugestão acolhida e já tratada em sugestão anterior. Sugestão 5: Sugestão rejeitada. Sugestão redacional sem alteração substancial de conteúdo Sugestão 6: Sugestão rejeitada. Não se vislumbra a necessidade de maior detalhamento do artigo. Sugestão 7: Sugestão rejeitada. Não se vislumbra a necessidade de explicitar, já que o art. 11 trata somente de infraestruturas críticas, estando relacionado apenas a parte do protocolo descrita no anexo.

		No art. 32 caberia uma referência ao anexo VI (gerenciamento de identidades); Não há razão para se ter uma política de cultura e educação (PCESC-PJ) de que tratam os arts. de 33 a 37 separada da PSEC-PJ. Juntar numa política única, tratando esses grupos de forma integrada; O capítulo IX (arts. 33 a 37) parece ser redundante com o Anexo VII; Citar que a segurança cibernética complementa e apoia, mas não substitui os quesitos e ações relativas à LGPD (art. 39).	Sugestão 8: Sugestão rejeitada. Sugestão redacional sem alteração substancial de conteúdo.

Alessandra Marques da Silva Thompson	TRE-ES	Capítulo I, art. 1o: Melhor criar um glossário e levar as definições para lá. Os incisos do parágrafo único ficaram confusos... traz um conjunto de ações para definir segurança. Capítulo II, art. 2o, § 1o: eliminar. Sem utilidade. Capítulo II, art. 3o, § 1o: Não consegui discernir a diferença entre a Política e a ENSEC-PJ. No documento todo, isso ficou bem confuso. Capítulo III, arts. 6o e 9o: estão muito parecidos. Não dá para distinguir o que é objetivo do que é ação. Capítulo III, art. 10: esclarecer esse artigo. Talvez, "linká-lo" à execução da PSI do órgão. Capítulo III, art. 11: desceu para um nível tático-operacional, repetindo o que já existe em outras normas. Trata-se de uma política que deve dar DIRETRIZES. Sugiro fazer menção ao Protocolo respectivo. Por exemplo: "Para elevar o nível de segurança das infraestruturas críticas, deve-se executar as ações previstas no Protocolo tal....". Capítulo VI, art. 20: Esse Comitê de Governança de Segurança da Informação (CGSI) é o mesmo Comitê Gestor de Segurança da Informação do art. 40 da ENTIC-JUD (lá já é formado pelos titulares das áreas estratégicas do órgão. Não existem pessoas em mais alto nível que eles. Só o presidente)? O § 1º do artigo 20 diz que "O CGSI será coordenado pela autoridade responsável pela segurança da informação no respectivo órgão do Poder Judiciário, nomeado por seu presidente." Quem? O Gestor de Segurança? Na ENTIC-JUD fala que o Comitê Gestor de Segurança da Informação deve ser presidido pelo Secretário de Tecnologia da Informação e Comunicação (art. 40).	Sugestão 1: Sugestão prejudicada. Já houve deliberação no sentido do aprimoramento do termo “segurança cibernética” no glossário. O art 1º, ademais, será melhor trabalhado a partir de sugestões previamente apresentadas. Sugestão 2: Sugestão rejeitada. O grupo considera necessário manter para explicitar o entendimento do conceito. Sugestão 3: Sugestão rejeitada. Em razão dos vários questionamentos acerca do que seja política ou estratégia, o assunto será melhor avaliado oportunamente, decidindo-se não alterar a estrutura atual do normativo proposto, porém incluindo previsão de atualização revisional em momento oportuno. Adicionalmente, o art 3º conceitua que a estratégia visa a estruturar os objetivos instituídos na política. Sugestão 4: Sugestão rejeitada. As ações são os meios de chegar aos objetivos, pode-se ver isso nos normativos. Sugestão 5: Sugestão rejeitada. Não ficou claro o que é necessário esclarecer.

		Capítulo VI, art. 21: Esse artigo diz que "Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir estrutura de segurança da informação, subordinada diretamente à alta administração do órgão e desvinculada da área de TIC.". E, no § 1º, diz que "O titular da estrutura prevista no caput deste artigo será o gestor de segurança da informação do órgão". Como assim? O CNJ precisa alinhar, primeiro, suas POLÍTICAS. Não há como trabalhar com Políticas que se contradizem. Primeiro, pede para o STI ser o coordenador do Comitê Gestor de SI. Depois, pede pra criar estrutura de Seg. Info fora da TI? Capítulo VII, art. 24: Como trabalhar OKR em tantos objetivos? Eles até se misturam com os objetivos e ações da ENSEC_PJ, dos arts. 6o e 9o. Capítulo VII, arts. 26 a 30: deveriam ser transferidos para os respectivos protocolos (anexos). Capítulo IX, art. 33 a 37: por que não juntar com a Política de Segurança Cibernética do PJ do Capítulo VII? Capítulo XI, art. 39: Fala em criação de grupo de trabalho destinado à elaboração de estudos e propostas voltadas à adequação dos tribunais à Lei n. 13.709/2018 (LGPD). Já está tarde! Ainda vão criar? Ou já criaram? Estamos correndo contra o tempo. Depois, quando sair essas propostas, já estaremos com nossos documentos prontos, tendo que ser revistos para adequação. Trabalho dobrado. Capítulo XI, art. 42: Como assim, "ficam revogadas as Resoluções CNJ n. 360, de 17 de dezembro de 2020; n. 361, de 17 de dezembro de 2020 e n. 362, de 17 de dezembro de 2020"? Acabamos de enviar planos com base nelas. Eles ficam revogados também?	Sugestão 6: Sugestão rejeitada. O grupo considerou necessário já estabelecer algumas ações. Sugestão 7 e 8: Sugestão acolhida para incluir dispositivo revogando os artigos 36 a 41 da Entic que tratam da questão de Segurança. E realizar análise mais ampla na ENTIC para verificar outras eventuais incompatibilidades. Sugestão 9: Sugestão rejeitada. O esclarecimento do conceito de política e estratégia, contida na Sugestão 3, soluciona a dúvida apresentada. Sugestão 10: Sugestão rejeitada. Não há sugestão concreta de alteração do artigo. Sugestão 11: Sugestão rejeitada para manter os artigos 26 a 31. Sugestão 12: Sugestão parcialmente acolhida para manter o art. 33 e transferir os demais artigos (34 a 37) para seu respectivo anexo. Sugestão 13: Sugestão acolhida para excluir o art. 39 em razão da Resolução CNJ 363/2021

			Sugestão 14: Sugestão rejeitada. Sem contribuição para norma.

Juarez de Oliveira	TRE-PR	Artigo 1. Existe um claro conflito entre a ENTIC-JUD e a ENSEC-JUD, sendo que a ENTIC deveria apenas referenciar a ENSEC e não colocar objetivos, como organização de Comitê, PSI, Riscos, ETIR etc. Por exemplo, o artigo 20, que fala do Comitê, se sobrepõe ao artigo 40 da ENTIC, que aliás, equivocadamente em termos de governança, define que o Responsável da TI coordene o Comitê. No artigo 31, que trata da PSI, se sobrepõe ao 39 da ENTIC, que trata do mesmo tema. Já o tema de Continuidade de Serviços faz parte do PCN, que também não deve estar atrelado somente à TI, como previsto na ENTIC. Desta forma considero que é imprescindível que nenhum assunto tenha referencia simultânea nas duas Estratégias. Agora vamos aos artigos que são operacionais e jamais devem constar de uma Estratégia: No artigo 21, o responsável pela ETIR pode ser qualquer servidor, não precisa nem deve ser o Gestor de Segurança, devido a segregação de funções necessária. Este ponto deve ficar em aberto para que cada tribunal defina, de acordo com sua estrutura. O capítulo VIII, que trata da Gestão de usuários não deveria constar da Estratégia e sim das Políticas, fazem parte dos controles previstos nas normas ISO 27001/27002. O artigo 36 é inadequado, já que se trata de Estratégia e não de Política. A Estratégia vale para os gestores, os elaboradores de política, não para o nível operacional. O artigo 37 não precisa detalhar os tipos de ações, apenas a necessidade das campanhas de conscientização. Ainda sobre o artigo 37 , não é necessário uma Política e sim um plano em cada órgão, aí sim, com os devidos detalhamentos e indicadores. Detalhar torna o artigo operacional e uma Estratégia não deve ser operacional. Agora falando dos protocolos previstos no artigo 25: Considero que foi um erro lançar os protocolos antes da Estratégia, tendo em vista que para organizar qualquer ação deste tipo é necessário	Sugestão 1: Sugestão já apreciada em outra proposição. Sugestão 2: Sugestão acolhida. Foi decidido pela remoção do inciso que define o Gestor de SIC como coordenador da ETIR. Sugestões 3 e 4: Sugestões já tratadas em proposições anteriores Sugestão 5: Sugestão rejeitada. Não traz proposições concretas.

		que o tribunal possui estrutura de governança de segurança da informação adequada, o que não ocorre na grande maioria. De qualquer forma, o CNJ está descendo para o nível tático e operacional, o que realmente não é seu escopo institucional. É necessário organizar a gestão, traçar os objetivos cobrar estas entregas. Conceitualmente este modelo está equivocado. Ainda assim, no inciso II, que fala sobre prevenção, não tem sentido, já que a prevenção se faz pela adoção das boas práticas, principalmente da ISO 27001/27002 e CIS controls. Então não é um protocolo, é um SGSI. Já a gestão de crises cibernéticas, prevista no inciso III, está atrelada a um comitê de crise que precisa ser único, que atenda a norma ISO 22301 (Plano de Continuidade de Negócios) ou qualquer evento impactante que impeça as operações e traga um algo nível de indisponibilidade ou risco à organização. Não é possível ter um comitê de crise para ciber, outro para o pcn, outro para uma emergência médica, etc, principalmente porque não será possível saber, em caso de uma emergência, qual comitê acionar. Precisa de um comitê de crise só, e ele será formado na aplicação da ISO 22301, na criação do PCN, que aliás tem quase nenhuma referência nessa ENSEC.	

Eder Santana Freire	TRT20	Alterar os incisos IV a VIII do Art. 1º para que iniciem da seguinte forma: "a condução de ações..." ou "a estruturação de ações..." ou "a tomada de medidas..." Substituir o termo "Judiciário" por "Poder Judiciário", ao longo do texto, como nos seguintes exemplos: Art. 6º, inciso I; Art 9º, inciso III; Art. 12, inciso III; Art. 18, parágrafo único; O termo "Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)" aparece, ao longo do texto, ora com as iniciais maiúsculas, ora com as iniciais minúsculas. Favor verificar; Alguns dispositivos, ao longo do texto, não estão corretamente identados. Ex: Art. 20; Art. 24. Favor verificar. Alterar o Art. 5º para que tenha a seguinte redação: "Os objetivos da ENSEC-PJ são a base para tornar o espaço cibernético do Poder Judiciário mais seguro, confiável, resiliente e inclusivo, e buscam direcionar as ações dos seus órgãos a respeito do tema segurança cibernética" Alterar o incisos do Art. 6º para que tenham a seguinte redação: "III – estabelecer, nos órgãos do Poder Judiciário, a governança de segurança cibernética e fortalecer a gestão e a coordenação integrada das ações relacionadas aos seus processos"; "IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível." Alterar o parágrafo único do Art. 8º para que tenha a seguinte redação: "Parágrafo único. O engajamento da alta administração de cada tribunal é essencial para a consecução das finalidades e das medidas de proteção aos serviços disponibilizados no ambiente digital, sobretudo quando tais medidas implicarem a necessidade de rápida suspensão destes serviços,	Sugestão 1: Sugestão rejeitada.Não muda o sentido do dispositivo. Sugestão 2: Sugestão rejeitada. Não considerada necessária. Sugestões 3 e 4: Sugestões acolhidas para atualização na revisão final. Sugestão 5: Sugestão rejeitada. Não verificada mudança no sentido do dispositivo citado. Sugestão 6: Inciso III: Sugestão rejeitada por não trazer alteração de conteúdo. Dessa forma deve-se manter a redação original do inciso. Inciso IV: Sugestão acolhida para atualização na revisão final. Sugestão 7, 8, 9 e 10: Sugestão rejeitada. Não verificada mudança no sentido do dispositivo citado Sugestão 12: Sugestão acolhida para alterar “CGSI-JUD” para “CGSI-PJ”

		visando a evitar o alastramento de ataque cibernético e a contenção de danos." Alterar a redação do Art. 10. para a seguinte: "Para o fortalecimento das ações de governança cibernética, os órgãos do Poder Judiciário devem..." "Alterar a redação do Art. 11. para a seguinte: "De modo a elevar o nível de segurança das infraestruturas críticas, também caberá aos órgãos do Poder Judiciário: (...) I – estabelecer processos que possibilitem maior eficiência na condução das ações envolvendo intraestruturas críticas, visando à melhoria da capacidade de resposta a incidentes de segurança cibernética e à contínua prestação dos serviços essenciais de cada órgão; (...) III – elaborar e implementar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimentos visando à continuidade e o rápido restabelecimento dos serviços essenciais prestados, incluindo as atividades de comunicação interna e externa; (...) V – utilizar tecnologias que empreguem recursos de inteligência no combate a ameaças cibernéticas em ambientes digitais usados para intercâmbio de informações, tais como fóruns, redes sociais e imageboards, inclusive aqueles não disponíveis na Internet de superfície; VI – providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em meio de armazenamento off-line, e em formato que permita a investigação de incidentes;	

		(...) IX – adotar, no desenvolvimento de novos projetos, práticas e requisitos de segurança cibernética de última geração tais como a implementação de duplo fator de autenticação em sistemas e serviços acessíveis por meio externo.; (...) " "Alterar o Art. 17, inciso III para que tenha a seguinte redação: ""elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação de magistrados, servidores, profissionais terceirizados, estagiários e demais colaboradores atuantes no âmbito dos órgãos do Poder Judiciário;" No art. 18, VIII, inserir o espaço faltante em "dapolícia judiciária" No CAPÍTULO IX, inserir o espaço faltante em "SEGURANÇACIBERNÉTICA" No Art. 40, é mencionado o termo "CGSI-JUD", enquanto nos demais dispostivos da ENSEC-JUD é mencionado o termo "CGSI-PJ". Favor verificar.	

Mateus Cançado Assis	TJMG	Art 1º, incisos II e III - DE “segurança física e proteção de …” - PARA “segurança física e lógica para proteção de …” - Os termos “segurança física” e “proteção” originalmente utilizados podem gerar confusão quanto ao seu significado. Controles físicos e lógicos contribuem para a proteção. Art. 1º, § único, inciso V - DE “... da prestação jurisdicional e administrativa dos órgãos do Poder Judiciário” - PARA “... das atividades fim e administrativas" - Trata-se de uma definição, que fica mais amplamente aplicável se colocada em termos gerais do que em âmbito específico. Todos os outros incisos de definição estão em termos gerais. Art 5º, caput e inciso I - Em ambos é utilizado o termo “inclusivo”. Não entendemos que tornar o ambiente digital/cibernético mais inclusivo seja um objetivo da segurança cibernética e sugerimos suprimir o termo. Ressalte-se que “disponibilidade” é um dos pilares de segurança da informação e significa “propriedade de estar acessível e usável sob demanda a entidades autorizadas”, conforme ISO/IEC 27000:2018, definição 3.7, mas não se deve confundir disponibilidade com inclusão. Art. 11, inciso I - DE “... capacidade de responder de forma satisfatória a incidentes de segurança …” - PARA “... capacidade de prevenir, detectar e responder de forma satisfatória a incidentes de segurança …”; - Deve-se destacar não só a resposta a incidentes, mas, antes dela, a prevenção e a detecção.	Sugestão 1: Sugestão rejeitada. Verificado que não traz impactos relevantes no conceito. Sugestão 2: Sugestão acolhida para atualizar a redação do Art. 1º, § único, inciso V para: “as ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade das atividades fim e administrativas dos órgãos do Poder Judiciário;” Sugestão 3: Sugestão rejeitada. Sem contribuição para o dispositivo. Inclusive condiz com os princípios da política de segurança cibernética estabelecida. Sugestão 4: Sugestão rejeitada. Não acrescenta mudança substancial ao dispositivo. Sugestão 5: sugestão acolhida, com nova proposição ao Art. 11, inciso V, conforme abaixo:

		Art. 11, inciso V - A redação desse inciso está bem confusa e difícil de compreender; o termo "fóruns" deveria ser trocado para "fóruns de discussão"; "tais como deep e dark web" se refere a redes de informação ou a comunidades virtuais na internet? Ficou dúbio. Art. 11, inciso VIII - Incluir o termo “cibernética”: elaborar requisitos específicos de segurança cibernética relacionados com o trabalho remoto. Art. 11, inciso IX - DE “... tais como dupla verificação do acesso externo” - PARA “... tais como técnicas de codificação segura; testes de segurança de aplicações; DevSecOps e entrega contínua segura; segurança específica de contêineres, aplicações móveis, serviços e APIs; Web Application Firewall (WAF); que resultem em mecanismos eficazes de segurança e proteção tais como autenticação segura, protocolos de comunicação seguros, proteção contra injeção e contra Cross-Site Scripting (XSS), monitoramento, registro histórico (logging) e auditoria;” - Com um universo tão amplo de práticas e requisitos de segurança cibernética existentes aplicáveis a projetos, citar apenas a dupla verificação (ou autenticação multi-fator) e somente em acesso externo nos parece um exemplo restritivo e pobre, pouco representativo. Referências: Gartner, Guide to Application Security Concepts, ID G00729065, 29/jul/2020; e OWASP Top Ten https://owasp.org/www-project-top-ten/. Art. 17, inciso V - O CPTRIC-PJ atuará como time técnico apoiando os tribunais na prevenção e correção, em caso de ameaças ou de ataques cibernéticos.	“utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação;” Sugestão 6: sugestão acolhida, com nova proposição ao Art. 11, inciso VIII, conforme abaixo: - Incluir o termo “cibernética”: elaborar requisitos específicos de segurança cibernética relacionados com o trabalho remoto. Sugestão 7: Sugestão rejeitada. O detalhamento técnico está contido no manual específico. Sugestão 8: sugestão parcialmente acolhida. Alterar o Art. 11, inc. V, para remoção do termo “tais como...” em diante. Sugestão 9: Art. 18, inciso VI. Sugestão acolhida para manter apenas a sigla ETIR. Sugestão 10: Sugestão rejeitada. O objetivo é ter uma abertura para a participação dos órgãos citados no dispositivo. Sugestão 11: Sugestão rejeitada. Não há contribuição efetiva ao texto.

		A dúvida é se esse time terá condições reais de apoiar os tribunais nessa missão, dada a vastidão do Judiciário abrangido. É realmente viável? Art. 18, inciso VI - DE “incentivar a criação e a atuação de equipe de tratamento e resposta a incidentes cibernéticos (ETIR) em cada órgão do Poder Judiciário;” - PARA “incentivar a criação e a atuação ETIR em cada órgão do Poder Judiciário;” - Como a sigla ETIR foi definida anteriormente no inc. II do art. 11, não é necessário repetir a definição, a exemplo do inc. I do § 2º do art. 21; mas se for repetir, estava incompleta, deveria ser “equipe de tratamento e resposta a incidentes de segurança cibernética”. Art. 19, inciso V - DE “instituir e implementar Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), que comporá a rede de equipes …” - PARA “instituir e implementar ETIR, que comporá a rede de equipes …” - Como a sigla ETIR foi definida anteriormente no inc. II do art. 11, não é necessário repetir a definição, a exemplo do inc. I do § 2º do art. 21; mas se for repetir, estava incompleta, deveria ser “equipe de tratamento e resposta a incidentes de segurança cibernética”. Art. 23 – Inciso IV - DE “... entre os órgãos da Administração Pública Federal e do meio acadêmico” - PARA “... entre os órgãos do Poder Judiciário, outros órgãos da Administração Pública e do meio acadêmico” - Acreditamos que apenas “órgãos da Administração Pública Federal” deve ter sido inadvertidamente copiado sem adaptação do Decreto nº	Sugestão 12: Sugestão já apreciada em resposta a proposições anteriores. Sugestão 13 a 17: Sugestão já apreciada em resposta a proposições anteriores.

		9.367/2018 que institui a Política Nacional de Segurança da Informação. Art. 24, inciso VII, alínea (d) - Deve-se ter atenção para possíveis conflitos com o disposto na Resolução CNJ nº 363/2021, principalmente em seu Art. 1º, inciso XI. Art. 25, inciso I - Se a estrutura normativa base é ENSEC-PJ (Estratégia), fica incoerente que a PSEC-PJ (Política) tenha como um dos seus instrumentos a Estratégia. Nos parece que deveria ser o contrário, a Política ser um dos instrumentos da Estratégia. Art. 30 - Esse comando (acionar o Comitê de Crise) não deveria estar dentro do PGIC-PJ, ao invés de estar no corpo da Resolução da Estratégia? Art. 32, parágrafo único - DE "... 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." - PARA "... que definirá padrões mínimos a serem adotados, com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas judiciais no Poder Judiciário." - O padrão a ser proposto como Estratégia Nacional pelo CNJ deveria se limitar apenas aos sistemas de processo judicial eletrônico, dada a complexidade e heterogeneidade dos diversos sistemas existentes no Poder Judiciário. Além disso, deveria manter-se em nível mais geral de padrões mínimos. Estudos posteriores poderão indicar detalhes de padrões mínimos viáveis e adequados. Abordar aqui detalhes como login único e interface de interação entra numa seara complexa e de	

		especificidades e idiossincrasias dos órgãos que parece incompatível com o nível de abordagem adequado para a Estratégia. Art. 36, incisos I a IV - PARA “I – magistrados; II – servidores; III – estagiários; IV – terceirizados; e” - Apesar da redação original ter buscado ser mais inclusiva, na redação oficial (norma culta da língua) apenas um gênero já serve para indicar o respectivo significado aplicável, da mesma forma que no caput se usa apenas "usuários" e no inciso V está apenas "colaboradores". Art. 38, caput - Não fica claro o que serão consideradas “ações estratégicas”. O artigo 1º cita várias ações, mas não define nenhuma como estratégica. Art. 38, parágrafo único - DE “Os recursos orçamentários deverão ser discriminados em rubrica específica …” - PARA “Os recursos orçamentários deverão preferencialmente ser discriminados em rubrica específica …” - Na forma impositiva original, nos parece que o comando extrapola a competência de segurança cibernética na medida em que faz determinações de ordem administrativo-orçamentária dos órgãos.	

Portaria Aprovação Protocolos e Manuais

Nome	Órgão/Empresa	3. Sugestões na Portaria “Aprovação Protocolos e Manuais"	
Said Ahmad Karfan Neto	TJMT	– Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ); II – Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRCPJ); III – Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).	Sugestão rejeitada. Não se vislumbra a necessidade de adição das siglas.
Claudson Correia Melo Freitas	TJAL	Art. 1º, III: 1) "Além de investigar, deve-se penalizar os praticantes de crimes cibernéticos. Tal penalização agirá de maneira coercitiva contra os próximos possíveis atos criminosos".	Sugestão rejeitada. Não cabe a penalização em esfera administrativa.
Ana Lucia Lourenço	TJPR	Sugiro a alteração do artigo 4º da Portaria: "Art. 4º Os protocolos e manuais aprovados neste ato serão objeto de atualização a qualquer tempo por indicação do Comitê Gestor de Segurança Cibernética do Poder Judiciário", para constar que as atualizações dos protocolos e manuais poderão ocorrer a qualquer tempo depois de previamente consultados todos os Tribunais que deverão se manifestar no prazo de quinze dias. A sugestão é para não ferir a autonomia dos Tribunais e também para que participem da discussão sobre o conteúdo dos protocolos e manuais, cuja implementação é afeta a todos nós.	Sugestão rejeitada. O CNJ já é, em essência, órgão representativo de todo o Poder Judiciário.
Marco Aurélio Barbosa Schaan	TRF4	Art. 2º, IV (Política de Educação). Quando ocorreu a crise de 2018 e, por consequência, uma escassez de recursos em 2019 para qualquer atividade dos tribunais em geral. O primeiro grande corte foi na capacitação de servidores. Neste PDTI 2018-2020 houve apenas capacitação para gestores, talvez algumas exceções bem definidas podem ter sido tratadas, mas a grosso modo não houve capacitação de servidores e a capacitação de	Sugestão rejeitada. Não há sugestões concretas de alteração.

		gestores ainda não foi verificada sua eficácia. Uma política de Educação, e principalmente se tratando de segurança da informação e proteção de dados, deve ser realizada em sua plenitude e completeza. A melhor política de educação é o comprometimento dos gestores dos tribunais com seus servidores, em especial os da área de TI, para a Transformação Digital que será promovida nos próximos anos. Tendo como a satisfação dos usuários internos e externos como METAS 2021-2026 isso deve estar com o máximo de prioridade. As recentes invasões do STJ e TSE não foram em vão no momento das eleições 2020, mas movidas por vasto conhecimento de pessoas de outras nações, como Portugal onde foi detectado o invasor, e a falta dos nossos servidores em conhecimento.	
Paulo Roberto Mendes	TRE-MG	Eliminar os "considerando" desnecessários ou em duplicidade, como a referência à portaria 242; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação) e à PGR (política de gestão de riscos corporativos), evitando duplicidades, ambiguidades e contradições entre as normas; Citar o necessário alinhamento dos protocolos à arquitetura de processos do órgão; No art. 5º, citar que a implementação será gradual, por meio de plano de trabalho a ser formalizado por cada órgão, conforme critérios prioritários (ver por exemplo a sugestão abaixo de grupos para itens do checklist); Muitos anexos possuem checklist de referência (especialmente anexos IV, V e VI). Melhor construir um único checklist com capítulos ou grupos de cada anexo. Utilizar esse checklist padrão, para ser respondido por todos os órgãos, e não apenas como modelo; Padronizar o checklist para recomendar as práticas por grupo (aplicabilidade de cada controle em relação ao porte da organização, categorizado por Grupo 1, Grupo 2 e Grupo 3, esses grupos fornecem uma forma simples e	Sugestão já apreciada em resposta a proposições anteriores.

		acessível de ajudar as organizações de diferentes portes a direcionar seus recursos com o melhor custo × benefício, alcançando os melhores resultados na busca pela mitigação do risco); Padronizar o checklist para pontuar o nível de aplicação em cada órgão por maturidade (1 – Não observado ou inicial (Fator não foi demonstrado claramente); 2 – Maturidade baixa ou em desenvolvimento (Fator demonstrado claramente, mas não integrado); 3 – Maturidade média ou definida (Fator suficientemente demonstrado, integrado, mas não está medido); 4 – Maturidade alta ou gerenciada (Fator constantemente demonstrado, integrado, gerenciado, mas não possui melhoria contínua); 5 – Melhoria contínua ou otimizada); Incluir medidas organizacionais que apoiem a efetivação de cada um dos controles técnicos elencados no checklist.	
Valéria Freitas Vargens	TRE-MG	Citar o necessário alinhamento dos protocolos à arquitetura de processos do órgão; No art. 5º, citar que a implementação será gradual, por meio de plano de trabalho a ser formalizado por cada órgão, conforme critérios prioritários ; Muitos anexos possuem checklist de referência (especialmente anexos IV, V e VI). Melhor construir um único checklist com capítulos ou grupos de cada anexo. Utilizar esse checklist padrão, para ser respondido por todos os órgãos, e não apenas como modelo. Padronizar os checklist para o uso de todos os tribunais.	Sugestão já apreciada em resposta a proposições anteriores.

Eder Santana Freire	TRT20	Alterar a redação do Art. 5º para que preveja um período de adaptação ("vacatio legis") para a plena aplicação da ENSEC-PJ nos órgãos do Poder Judiciário. A sugestão é de que o período de adaptação seja de, no mínimo 12 meses. Tal medida se mostra necessária, sobretudo, em órgãos que não possuem grandes equipes estruturadas e voltadas especificamente para atender às demandas de Segurança da Informação. Este é o caso do TRT20, que possui apenas um servidor (este que vos fala) dedicado a tais demandas. Por conta dessa carência de pessoal, já estamos enfrentando bastantes desafios para implementação dos novos requisitos introduzidos pela LGPD e pelos Protocolos de Segurança Cibernética do CNJ (Res. 360, 361 e 362/2020). Desse modo, a introdução de um período de adaptação dos órgãos à nova ENSEC-PJ seria certamente bem-vinda.	Sugestão parcialmente acolhida para alterar o início da vigência do normativo para 120 dias da data de publicação, excetuando os anexos I, II e III, que reproduzem normas que já estavam em vigor e cujos prazos de cumprimento já haviam sido extrapolados.
Rivadávia Borges Vianna	TRT18	CONSIDERANDOS MOTIVAÇÃO DA SUGESTÃO: penúltimo CONSIDERANDO está contido no 2º CONSIDERANDO SUGESTÃO: suprimir o penúltimo CONSIDERNDO	Sugestão rejeitada. Os “consideranda” não possuem força normativa.
Juarez de Oliveira	TRE-PR	Nem deveriam existir, são inadequados, foram lançados de forma abrupta e não seguem o modelo de governança existente. Os manuais são operacionais, jamais deveriam ser o escopo do CNJ, a não ser em casos muito específicos onde haja dificuldade de entendimentos.	Sugestão rejeitada. Juízo de oportunidade exercido pela Presidência do CNJ ao criar o presente comitê.

Anexo I – Protocolo de Prevenção de Incidentes

Nome	Órgão/Empresa	4. Sugestões no Anexo I – Protocolo de Prevenção de Incidentes	
Eder Santana Freire	TRT20	Seria interessante que o CNJ possa, posteriormente, editar um procedimento técnico com a recomendação das principais ferramentas a serem utilizadas pelas ETIR dos órgãos do PJ nas fases de prevenção, gerenciamento e investigação de incidentes/crises/ilícitos cibernéticos. A edição deste procedimento poderá, inclusive, contar com a colaboração e participação conjunta das equipes dos Tribunais.	Sugestão rejeitada. Trata-se de sugestão que poderá vir a ser acolhida, mas que não deve interferir na conclusão dos normativos ora elaborados.
Rivadávia Borges Vianna	TRT18	MOTIVO DA SUGESTÃO: além das providências que os TRIBUNAIS devem tomar a respeito do que está contido no material de referência, precisamos consolidar o protocolo em algum documento com o mesmo nome? SUGESTÃO: caso afirmativo, acrescentar um item no texto contendo um modelo paradigma com conteúdo exemplificativo, pois reduzirá esforços repetitivos por parte dos TRIBUNAIS e facilitará o acompanhamento da Governança Nacional.	Sugestão rejeitada. A estratégia contém um conjunto de ações para elevação do nível de maturidade em cada Tribunal, que será gradualmente desenvolvido por meio de protocolos. Considera-se ainda que o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos. Com relação aos “modelos paradigma”. A sugestão foi rejeitada. Trata-se de sugestão que poderá vir a ser acolhida, mas que não deve interferir na conclusão dos normativos ora elaborados.

Marco Aurélio Barbosa Schaan	TRF4	7. Boas Práticas de Segurança Cibernética. 7.5.6 - Lições Aprendidas. Este é o capitulo principal da prevenção de incidentes. Nossa cultura odeia o erro, gosta muito dos elogios e reconhecimento de seus méritos, mas recusa-se a aceitar os erros. Lições Aprendidas só terá validade quando colocarmos nossos erros no papel para todos saberem onde erramos e onde não errar. Lições aprendidas é a melhor prevenção. Os protocolos de prevenção são cheios de lições aprendidas quando gestores cometem erros e estes ficam anotados para que no futuro não se cometam os mesmos erros. Não temos esta cultura e devemos adquiri-la com urgência.	Sugestão rejeitada. Não há proposta de alteração concreta a incorporar ao texto.
Hetug Sardeiro Porto	TRT5 (Bahia)	Item 3.2.1 - Sugestão: Definição de uma base de conhecimento de defesa única para todo o Poder Judiciário, inclusive para servir de mecanismo de comunicação entre as ETIR's de cada órgão.	Sugestão prejudicada. Já há previsão de criação do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC) no texto da Estratégia.
Deborah Araujo Santos Pondelek	TJPR	Item 2.1.1: "risco direto e / ou indireto"; 3.2.2: revisão de controles/acessos"; 3.2.5:" contemplem instrução básica, capacitação técnica, formação ética e disseminação responsável"; 3.2.7:" bem como impedir a reincidência secundária do incidente identificado";	Sugestão 2.1.1: Sugestão acolhida para definir nova redação para o item 2.1.1: "identificar: entendimento organizacional para gerenciar o risco direto e /ou indireto de ataques cibernéticos a sistemas, pessoas, ativos, dados e recursos. Permite ao órgão avaliar os recursos que suportam funções críticas e os riscos relacionados. São medidas de concentração e priorização dos esforços na gestão de ativos, ambiente de negócios, governança, avaliação de riscos e estratégia de gestão de riscos."

			Sugestão 3.2.2: Sugestão acolhida para definir nova redação para o item 3.2.2: “priorização: foco prioritário na formação, na revisão de controles/acessos, nos processos e na disseminação da cultura de segurança cibernética. Contribui para a redução de riscos e para a proteção contra as ameaças mais sensíveis e que encontram viabilidade em sua célere implementação.” Sugestão 3.2.7: Sugestão acolhida para definir nova redação para o item 3.2.7: “resiliência: poder de recuperação ou capacidade de a organização resistir aos efeitos de um incidente, bem como impedir a reincidência secundária do incidente identificado.”
Paulo Roberto Mendes	TRE-MG	Criar um item no checklist padrão referente à adoção do protocolo especificado neste anexo; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação); Citar o alinhamento deste à PGR (política de gestão de riscos corporativos); Citar o necessário alinhamento deste protocolo à arquitetura de processos do órgão.	Sugestão rejeitada. Não há proposta de alteração concreta a incorporar ao texto
Juarez de Oliveira	TRE-PR	Não existe protocolo de prevenção a incidentes. A prevenção a incidentes ocorre pela governança, principalmente pela PSI e pelas normas ISO 27000. Também é necessário constituir estruturas organizacionais com foco em	Sugestão rejeitada. Não há proposta de alteração concreta a incorporar ao texto

		cibersegurança e privacidade, tanta na parte operacional tanto na parte de governança	
Mateus Cançado Assis	TJMG	2.1.2 - DE "... que assegurem a proteção de dados, inclusive pessoais, de ativos de informação; e a prestação de serviços críticos." - PARA "... que assegurem a proteção de dados, inclusive pessoais, e de ativos de informação, bem como a prestação de serviços críticos." - A redação original estava confusa, creio que a sugestão a torna mais clara. 3.2.3 - DE "... compreensão abrangente para magistrados e magistradas, servidores e servidoras, colaboradores e colaboradoras, prestadores e prestadoras de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança..." - PARA "... compreensão abrangente para magistrados, servidores, colaboradores, prestadores de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança..." - Apesar da redação original ter buscado ser mais inclusiva, na redação oficial (norma culta da língua) apenas um gênero já serve para indicar o significado aplicável, da mesma forma que o termo "auditores" presente no mesmo trecho. Tal generalização já estava presente na Portaria CNJ 292. 3.2.5 - DE "formação e capacitação: processos formais de educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação e a instrução para todos os atores …" - PARA "formação, capacitação e conscientização: processos formais de	Sugestão 2.1.2: Sugestão acolhida para atualizar a redação do item 2.1.2 para: "proteger: desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, e de ativos de informação, bem como a prestação de serviços críticos." Sugestão 3.2.3: Sugestão acolhida para atualizar a redação do item 3.2.3 para: "instrumentos de medição e métricas: definição e estabelecimento de métricas comuns que fornecem linguagem compartilhada e de compreensão abrangente para magistrados, servidores, colaboradores, prestadores de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança. Permite...." Sugestão 3.2.5: Sugestão acolhida para atualizar a redação do item 3.2.5 para: "formação, capacitação e conscientização: processos formais de educação continuada com a inclusão em planos de

		educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação, a conscientização e a instrução para todos os atores..." 3.2.6 - DE "... para que as organizações obtenham medições confiáveis, escaláveis e contínuas. Tal processo está correlacionado com os resultados almejados por meio dos instrumentos de controle e de métricas." - PARA "... para que as organizações obtenham controles e medições confiáveis, escaláveis e contínuas." - Recomendamos abordar também os controles, além das medições na automação. Com relação ao trecho "Tal processo está correlacionado com os resultados almejados por meio dos instrumentos de controle e de métricas", entendemos que todos os princípios e processos estão, de certa forma, correlacionados com os resultados almejados. Dessa forma, sugerimos a retirada desse trecho do item 3.2.6. 3.2.7 - DE "... poder de recuperação ou capacidade de a organização resistir aos efeitos de um incidente" - PARA "... poder de recuperação ou capacidade de resistência da organização aos efeitos de um incidente" 4 - DE "Gestão de Incidentes de Segurança da Informação" - PARA "Gestão de Incidentes de Segurança Cibernética" - Consoante com a definição do parágrafo único do art. 1º da minuta de Resolução, o termo "segurança cibernética" é mais amplo e contempla também segurança da informação, de forma que com a alteração proposta a	capacitação que contemplem a disseminação, a formação, a conscientização e a instrução para todos os atores..." Sugestão 3.2.6: Sugestão rejeitada. Verificado que não tem impactos relevantes no conceito. Sugestão 3.2.7: Sugestão rejeitada. Verificado que não tem impactos relevantes no conceito. Sugestão 4: Sugestão acolhida para atualizar a redação do item 4 para: "Gestão de Incidentes de Segurança Cibernética" Sugestão 4.1: Sugestão acolhida para atualizar a redação de "A gestão de incidentes de segurança da informação" para "A gestão de incidentes de segurança cibernética". Sugestão de alteração rejeitada: "contendo as fases de preparação, monitoramento, detecção, análise, notificação, resposta e lições aprendidas."

		gestão de incidentes atinge maior amplitude, coerente com o escopo da presente norma. 4.1 - DE “A gestão de incidentes de segurança da informação é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.” - PARA “A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituída formalmente, contendo as fases de preparação, monitoramento, detecção, análise, notificação, resposta e lições aprendidas.” - Além de adotar “segurança cibernética” ao invés de “segurança da informação” (idem item 4), nos parece fundamental que hajam mais fases, em especial, preparação, monitoramento, notificação e lições aprendidas, à luz da norma ABNT NBR ISO/IEC 27002:2013 16.1.1.a (procedimentos da gestão de incidentes de segurança da informação) e, quanto à fase para a atualização das lições aprendidas, a exemplo dos itens 7.3 e 7.5.6 do próprio documento. Entendemos também que a toor riagem está inclusa na análise e pode ser suprimida, notando que também não aparece na NBR ISO 27002. Contudo, deve-se considerar se é desejada coerência com o Cyber-Resilience Framework do IDC referenciado no item 30.1 do Manual de Prevenção e Mitigação (Anexo V da minuta de Portaria) e que se alinha às funções básicas definidas nos subitens do item 2.1 do PPINC-PJ (Anexo I). Uma consolidação e consistência com conceitos e referências diversos auxiliará os órgãos a um entendimento e aplicação inequívocos e eficazes. 5.2 - DE “... solicitar apoio multidisciplinar que abranja as áreas: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias,	Verificado que não traz impactos relevantes no conceito. Sugestão 5.2: Sugestão acolhida para atualizar a redação do item para “... solicitar apoio multidisciplinar para responder aos incidentes de segurança de maneira adequada e tempestiva, em áreas como: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras.” Sugestão 7.5.1: Sugestão acolhida para atualizar a redação do item “preparação: processo que envolve as equipes de tratamento a incidentes e respostas. Trata-se de resposta metódica, contemplando ferramentas forenses de análise e custódia, planejamento sobre como responder e notificar cada incidente de segurança, identificação de cadeia de comando em situação de crise, processos de educação e de formação.”

		comunicação, controle interno, segurança institucional, entre outras, necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva." - PARA "... solicitar apoio multidisciplinar para responder aos incidentes de segurança de maneira adequada e tempestiva, em áreas como: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras." - Sugestão de melhoria na redação, deixando a citação de áreas para o final. 7.5.1 - DE "... contemplando ferramentas forenses de análise e custódia, identificação de cadeia de comando em situação de crise, processos de educação e de formação." - PARA "... contemplando ferramentas forenses de análise e custódia, planejamento sobre como responder e notificar cada incidente de segurança, identificação de cadeia de comando em situação de crise, processos de educação e de formação." - Sugerimos incluir na fase de preparação o planejamento adequado para a resposta e notificação dos incidentes. 7.5.3 - DE "visa a garantir que o incidente não cause mais danos, por meio da adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa, devendo os utilitários isolar a fonte de um ataque e determinar o momento de aplicação de ferramenta forense passiva construída para remoção de malware das redes de produção ou para a	Sugestão 7.5.3: Sugestão acolhida para alterar a redação para: "visa a garantir que o incidente não cause mais danos. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa incluindo, dentre outros, a imediata comunicação prevista na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSECPJ) e seus anexos, o isolamento da fonte do ataque, a aplicação de ferramentas forenses para remoção de malware das redes de produção, a limitação de transferências de dados desnecessárias e a adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises Cibernéticas."

		limitação de transferências de dados desnecessárias.” - PARA “visa a garantir que o incidente não cause mais danos. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa e inclui o isolamento da fonte do ataque, a aplicação de ferramentas forenses para remoção de malware das redes de produção, a limitação de transferências de dados desnecessárias e a adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises Cibernéticas.” - A primeira frase menciona busca da garantia para que um incidente não cause mais danos, “por meio da adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises”. Entendemos que apenas os mecanismos de comunicação, embora muito importantes após a identificação de um incidente, não são suficientes para garantir que o incidente não cause mais danos, como sugere a primeira frase na redação original. Partindo disso, foi proposta uma melhoria geral do texto.	

Anexo II – Protocolo de Gerenciamento de Crises

Nome	Órgão/Empresa	5. Sugestões no Anexo II – Protocolo de Gerenciamento de Crises	
Rivadávia Borges Vianna	TRT18	MOTIVO DA SUGESTÃO: além das providências que os TRIBUNAIS devem tomar a respeito do que está contido no material de referência, precisamos consolidar o protocolo em algum documento com o mesmo nome? SUGESTÃO: caso afirmativo, acrescentar um item no texto contendo um modelo paradigma com conteúdo exemplificativo, pois reduzirá esforços repetitivos por parte dos TRIBUNAIS e facilitará o acompanhamento da Governança Nacional.	Sugestão rejeitada. A estratégia contém um conjunto de ações para elevação do nível de maturidade em cada Tribunal, que será gradualmente desenvolvido por meio de protocolos. Considera-se ainda que o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos. A segunda sugestão será objeto de avaliação posterior na medida em que a criação de “modelo paradigma” não estava no escopo inicial e nem é essencial à aprovação dos presentes normativos.
Eder Santana Freire	TRT20	Seria interessante que o CNJ possa, posteriormente, editar um procedimento técnico com a recomendação das principais ferramentas a serem utilizadas pelas ETIR dos órgãos do PJ nas fases de prevenção, gerenciamento e investigação de incidentes/crises/ilícitos cibernéticos. A edição deste procedimento poderá, inclusive, contar com a colaboração e participação conjunta das equipes dos Tribunais.	Sugestão rejeitada. O detalhamento técnico não é um dos objetivos ENSEC-PJ. As ações e detalhes técnicos são particulares de cada órgão. Ademais, não há proposta de alteração concreta a incorporar ao texto

Marco Aurélio Barbosa Schaan	TRF4	6.2 Para a identificação das lições aprendidas e a elaboração de relatório final, devem ser objeto de avaliação: h) a coordenação da crise, liderança das equipes e gerenciamento de informações. Minha sugestão é igual ao item anterior, ou seja, como não temos um PCN ao implantar um gerenciamento de crise teremos muitos problemas, principalmente na veracidade das informações no gerenciamento de informações.	Sugestão rejeitada. Tratar do tema "Plano de Continuidade de Negócios" é importante, e sugere-se a discussão do tema em pauta futura do Comitê. Não se vislumbra necessidade de alteração no texto presente.
Juarez de Oliveira	TRE-PR	Não existe protocolo para gerenciamento de crises descolado da governança. O gerenciamento de crises está previsto na norma ISO 22301 (PCN). Conceitualmente qualquer tratamento sobre o tema, principalmente sobre a criação do comitê de crises deveria seguir o PCN, que aliás a maioria dos tribunais não tem. Foi tratado de forma inadequada na resolução 211 e persiste desta forma na ENTIC e na ENSEC.	Sugestão rejeitada. Tratar do tema "Plano de Continuidade de Negócios" é importante, e sugere-se a discussão do tema em pauta futura do Comitê. Não se vislumbra necessidade de alteração no texto presente.
Natália Harsanyi de Oliveira	HarsanyiInsight	2. Identificação de Crise Cibernética. 2.2 4. - 4.1	Sugestão rejeitada. Não há proposta de alteração concreta a incorporar ao texto.
Paulo Roberto Mendes	TRE-MG	Criar um item no checklist padrão referente à adoção do protocolo especificado neste anexo; Integrar o Plano de Gestão de Incidentes Cibernéticos ao Plano de Riscos do órgão; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação); Citar o alinhamento deste à PGR (política de gestão de	Sugestão rejeitada. Não há proposta de alteração concreta a incorporar ao texto.

		riscos corporativos); Citar o necessário alinhamento deste protocolo à arquitetura de processos do órgão.	
Mateus Cançado Assis	TJMG	4.1, alínea e Um Programa de Gestão da Continuidade de Serviços deve contemplar a categorização, o estabelecimento dos procedimentos de resposta, bem como o apoio às equipes, não apenas nos casos de incidentes cibernéticos graves. Desta forma, sugerimos retirar o termo “graves” no final do item. 5.5 DE “A sala de situação ... e estar próxima a um local onde se possa fazer declarações públicas à imprensa ...” PARA “A sala de situação ... e estar preferencialmente próxima a um local onde se possa fazer declarações públicas à imprensa ...” 6.4 DE “Deve ser elaborado Relatório de Comunicação de Incidente de Segurança em Redes Computacionais …” PARA “Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética …” Para maior coerência com a terminologia definida e utilizada nas normas, é recomendável utilizar o termo	Sugestão 4.1, alínea e: Sugestão acolhida. Nova proposição para o item 4.1, alínea e: “categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos;” Sugestão 5.5: Sugestão acolhida. Nova proposição para o item 5.5: “A sala de situação é o local a partir do qual serão geridas as situações de crise, devendo dispor dos meios necessários (ex.: sistemas de áudio, vídeo, chamadas telefônicas) e estar preferencialmente próxima a um local onde se possa fazer declarações públicas à imprensa e com acesso restrito ao Comitê de Crise e a outros entes eventualmente convidados a participar das reuniões.” Sugestão 6.4: Sugestão acolhida. Nova proposição para o item 6.4: “Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, bem como o plano

		“segurança cibernética” ao invés de “segurança em redes computacionais”.	de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados. Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.”

Anexo III – Protocolo de Investigação de Ilícitos Cibernéticos

Nome	Órgão/Empresa	6. Sugestões no Anexo III – Protocolo de Investigação de Ilícitos Cibernéticos	
Rivadávia Borges Vianna	TRT18	MOTIVO DA SUGESTÃO: além das providências que os TRIBUNAIS devem tomar a respeito do que está contido no material de referência, precisamos consolidar o protocolo em algum documento com o mesmo nome? SUGESTÃO: caso afirmativo, acrescentar um item no texto contendo um modelo paradigma com conteúdo exemplificativo, pois reduzirá esforços repetitivos por parte dos TRIBUNAIS e facilitará o acompanhamento da Governança Nacional.	Sugestão rejeitada. A sugestão será objeto de avaliação posterior na medida em que a criação de “modelo paradigma” não estava no escopo inicial e nem é essencial à aprovação dos presentes normativos.
Hetug Sardeiro Porto	TRT5 (Bahia)	Item 2.8 - Dúvida: Esclarecer melhor o termo "remotamente". A recomendação é que os registros de auditoria sejam também armazenados em outro servidor, centralizado e/ou off-site?	Sugestão rejeitada. Não há proposta de alteração concreta a incorporar ao texto. Quanto ao termo “remotamente”, pode ser tanto em outro servidor centralizado e/ou off-site, a critério do órgão.
Paulo Roberto Mendes	TRE-MG	Criar um item no checklist padrão referente à adoção do protocolo especificado neste anexo; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação); Citar o alinhamento deste à PGR (política de gestão de riscos corporativos); Citar o necessário alinhamento deste protocolo à arquitetura de processos do órgão.	Sugestão rejeitada. Não há proposta de alteração concreta a incorporar ao texto.

Mateus Cançado Assis	TJMG	2.5. - DE “Os sistemas e as redes de comunicação de dados devem ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:” - PARA “Os sistemas e as redes de comunicação de dados devem ser monitorados, registrando-se, QUANDO POSSÍVEL, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:” 4.1, 4.3, 4.4, 4.5 e 4.7 - Considerar padronizar a terminologia utilizada neste conjunto de normas, alterando DE “Segurança em Redes Computacionais” PARA “Segurança Cibernética”. 4.4, alínea h - Entendemos que o Termo de Custódia original deve ser anexado ao Relatório. Se não for esse o entendimento, deve-se adicionar “cópia do”.	Sugestão 1: Sugestão rejeitada. No texto já consta o termo “minimamente”. Sugestão 2: Sugestão acolhida. A redação dos itens 4.1, 4.3, 4.4, 4.5 e 4.7 deve ser alterada para “Segurança Cibernética”. Sugestão 3: Sugestão rejeitada. Não se vislumbra necessidade de alteração no texto. Os termos de custódia originais, via de regra, já são eletrônicos.
Juarez de Oliveira	TRE-PR	Não é necessário esse protocolo. Cada órgão deve executar suas políticas, configurar seus ativos para armazenar os logs de forma adequada, conforme previsto na ISO 27001 e treinar seus servidores técnicos para apoiar eventuais investigações de incidentes.	Sugestão rejeitada. O juízo de conveniência e oportunidade já foi exercido pela Presidência do CNJ na Portaria 242/2020.
Eder Santana Freire	TRT20	Revisar o item 2.1 para que, no lugar dos "ativos de informação" restrinja a necessidade de ajuste dos horários para os "recursos de TIC" ou para os "ativos de tecnologia da informação". Isto porque o ajuste dos horários não se aplica a ativos de informação não tecnológicos (informações armazenadas em papel, por exemplo). Lembrando que o termo "ativo", em sua concepção mais ampla, de acordo	Sugestão 1: Sugestão acolhida. A redação dos itens 2, 2.1 e 2.2 deve ser alterada para “Ativos de Tecnologia da Informação”.

		com os padrões de boas práticas, refere-se a "tudo aquilo que tem valor para a organização." Seria interessante que o CNJ possa, posteriormente, editar um procedimento técnico com a recomendação das principais ferramentas a serem utilizadas pelas ETIR dos órgãos do PJ nas fases de prevenção, gerenciamento e investigação de incidentes/crises/ilícitos cibernéticos. A edição deste procedimento poderá, inclusive, contar com a colaboração e participação conjunta das equipes dos Tribunais.	Sugestão 2: Sugestão rejeitada. As ações e detalhes técnicos são particulares de cada órgão. Não há proposta de alteração concreta a incorporar ao texto

Anexo IV – Manual de Proteção de Infraestrutura

Nome	Órgão/Empresa	7. Sugestões no Anexo IV – Manual de Proteção de Infraestrutura	
Bruna Pozzebon	Câmara dos Vereadores de Cabo Frio - RJ	A respeito da Proteção de dados - 10.3 Permitir apenas o acesso de cloud storage e\ou provedores de e-mail autorizados. É sabido e preocupante - "Incêndio destrói servidores da maior empresa de computação em nuvem da Europa" - a fragilidade de servidores e serviços terceirizados em nuvem. Nesse sentido, sugerimos pela grande quantidade de informação do Poder Judiciário a necessidade de investimento e desenvolvimento de serviços próprios em nuvem. Referência: https://www.cnnbrasil.com.br/tecnologia/2021/03/10/incendio-destroi-servidores-da-maior-empresa-de-computacao-em-nuvem-da-europa	Sugestão rejeitada. O emprego uso de serviços em nuvem é admitida pela Resolução CNJ 335/2020, sendo baseada nela a nova política de governança e gestão do processo judicial eletrônico.
Eder Santana Freire	TRT20	Observar que uma nova versão do framework Cis Controls (v 8.0) será disponibilizada no mês que vem (maio/2021): https://www.cisecurity.org/controls/v8/ Desse modo, recomendo que avaliem se não vale a pena aguardar pela divulgação desta nova versão, para que o manual seja publicado já com as devidas atualizações.	Sugestão rejeitada. Nada impede os tribunais adotem a versão mais recente, na medida em que se trata, nos presentes normativos, de “requisitos mínimos”. A orientação da comunidade que mantém o SisControl é da manutenção do uso da versão 7.1, considerada efetiva e usável, sem prejuízo de uma migração ao longo do tempo para a versão 8: “*We believe that Version 8 of the CIS Controls is the best we have ever produced. But we appreciate that enterprises who are actively using prior versions of the CIS Controls as a key part of their defensive strategy*

			might be reluctant to move to Version 8. Our recommendation is that if you are using Version 7 or Version 7.1, you are following an effective and usable security plan; but over time you should consider moving to Version 8. If you are using Version 6 (or earlier), our recommendations is that you should start to plan a transition to Version 8 as soon as practical."
Hetug Sardeiro Porto	TRT5 (Bahia)	Item 7.3 - Sugestão: Padronizar os níveis de maturidade/aplicabilidade em todos os manuais de referência, preferencialmente utilizar o padrão dos demais manuais, ou seja, 5 níveis de maturidade.	Sugestão rejeitada. Não se vislumbra a necessidade de detalhamento da aplicabilidade em níveis de maturidade.
Paulo Roberto Mendes	TRE-MG	Definir melhor se isto é um "manual", uma "política", um "modelo", uma "referência" ou uma "norma" a ser cumprida; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação); O item "finalidade e escopo" está misturando assuntos dos itens "campo de aplicação" e "referências normativas"; Utilização de checklist padrão, para ser respondido por todos os órgãos, e não apenas como modelo; Padronizar o checklist para pontuar o nível de aplicação em cada órgão por maturidade (1 – Não observado ou inicial (Fator não foi demonstrado claramente); 2 – Maturidade baixa ou em desenvolvimento (Fator demonstrado claramente, mas não integrado); 3 – Maturidade média ou definida (Fator suficientemente demonstrado, integrado, mas não está medido); 4 – Maturidade alta ou gerenciada (Fator constantemente demonstrado, integrado, gerenciado, mas não possui melhoria contínua); 5 – Melhoria contínua ou otimizada); Incluir medidas organizacionais que apoiem a efetivação de cada um dos controles técnicos elencados no checklist.	1ª. Sugestão. Sugestão rejeitada. A Portaria que deverá aprovar o normativo estabelece que seus anexos são de observância obrigatória. Não há espaço, portanto, para interpretação divergente, no sentido de tratar-se de mera recomendação. 2ª. Sugestão. Sugestão rejeitada. O comentário acerca do item "finalidade e escopo" misturar assuntos dos itens "campo de aplicação" e "referências normativas" não foi compreendido. 3ª. Sugestão. Sugestão rejeitada. A sugestão de inclusão de medidas organizacionais que apoiem a efetivação de cada um dos controles técnicos elencados no checklist interfere no "como" cada órgão irá trabalhar para alcançar os níveis de controle.

			4ª. Sugestão. Sugestão rejeitada. A sugestão de inclusão de medidas organizacionais que apoiem a efetivação de cada um dos controles técnicos elencados no checklist interfere no “como” cada órgão irá trabalhar para alcançar os níveis de controle.
Marco Aurélio B. Schaan	TRF4	Capacidade de recuperação de dados e proteção de dados. O primeiro está ligado a PCN e se existe ele não é normatizado. A proteção de dados iniciou-se recentemente e está seguindo as determinações do CNJ.	Sugestão rejeitada. Colaboração na compreendida como sugestão, mas como mera crítica.
Juarez de Oliveira	TRE-PR	Situações operacionais devem ser avaliadas pelas equipes operacionais, durante a execução das políticas definidas pelos comitês. Elaborar esse tipo de procedimento não é atribuição do CNJ e pode levar a mais dúvidas ainda por parte das equipes técnicas. Este manual não deve existir.	Sugestão rejeitada. O juízo de legalidade, conveniência e oportunidade já foi exercido pela Presidência do CNJ na Portaria 242/2020.
Mateus Cançado Assis	TJMG	2.1.1 a 2.1.11 - Como se trata de uma simples enumeração descritiva de seções do documento, sugerimos que seja usada a numeração em alíneas “a” a “k”. 3, alínea d - DE “Norma técnica Gestão de Riscos de Segurança da Informação associada às recomendações constantes da norma NBR ISO/IEC 27005:2019” - PARA “Recomendações constantes da norma técnica ABNT NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação” 3, alínea e - DE “Framework – CIS Controls – Versão 7.1, https://www.cisecurity.org/”	Sugestões parcialmente acolhidas com o objetivo de realizar uma validação geral do texto para eventuais correções.

		- PARA “CIS Controls Framework – Versão 7.1, Center for Internet Security (CIS), https://www.cisecurity.org/controls/” 3, alínea f - DE “Framework – National Institute of Standards and Technology (NIST) – Versão 1.1, https://www.nist.gov/cyberframework/framework” - PARA “NIST Cybersecurity Framework – Versão 1.1, National Institute of Standards and Technology (NIST), https://www.nist.gov/cyberframework/framework” 6, todos os subitens - Os subitens fazem menção a uma “Política de Segurança da Informação e das Comunicações – POSIC”. Seria importante estabelecer uma relação clara e direta entre tal política e os instrumentos estabelecidos nos arts. 22 (Política de Segurança Cibernética do Poder Judiciário – PSEC-PJ) e 31 (Política de Segurança da Informação de cada Tribunal) da minuta de Resolução.	

Alessandro Sousa	Dell Technologies	Na tabela constante no item 8 do sumário - Checklist para utilização dos Controles Mínimos Recomendados, incluir os seguintes pontos: Gerenciamento contínuo de vulnerabilidade ID 3.7 – Utilizar ferramenta que possua tecnologias avançadas de inteligência como Inteligência Artificial, Machine Learning e algoritmos de deep learning, entre outros a fim de garantir melhor identificação do ataque e priorização de alertas - NIST CSF Proteger/ Detectar – aplicável para todos os Grupos ID 3.10 – Utilizar ferramenta que utilize Inteligência Integrada contra ameaças a fim de possibilitar uma melhor detecção - NIST CSF Proteger – aplicável para todos os Grupos ID 3.11 – Utilizar ferramenta que permita que os eventos de segurança e o conhecimento dos incidentes da solução sejam compartilhados para possibilitar a manutenção do ambiente face a novos ataques - NIST CSF Proteger – aplicável para todos os Grupos ID 3.12 – Utilizar ferramenta que gerencie de forma unificada o monitoramento de ameaças nos endpoints, servidores e aplicações Web - NIST CSF Proteger – aplicável para todos os Grupos ID 3.13 – Utilizar ferramenta que verifique cada equipamento por meio da rede para identificação de vulnerabilidades possibilitando controle da gestão de mudanças nas configurações aprovadas e implementadas pela equipe técnica - NIST CSF Proteger – aplicável para todos os Grupos ID 3.14 – Utilizar ferramenta que permita a integração com outras tecnologias de Inteligência - NIST CSF Detectar – aplicável para todos os Grupos ID 3.15 – Utilizar ferramenta que apresente as informações na forma de um Workflow de fácil entendimento e intuitivo - NIST	Sugestão rejeitada. Insiste-se em trabalhar apenas com os controles do próprio SisControl, mantendo a estratégia que já vem sendo adotada de manter controles que possam garantir a exequibilidade e efetividade do normativo proposto levando em conta o conhecimento sobre o contexto do Judiciário. Sugestão poderia levar, ademais, a direcionamentos em eventuais contratações por parte dos tribunais.

		CSF Detectar – aplicável para todos os Grupos ID 3.16 – Utilizar ferramenta cujos alertas emitidos sejam direcionados ao contexto do ataque, p.ex discriminando usuário e endpoint atingido, possibilitando uma visualização rápida e clara dos eventos - NIST CSF Detectar – aplicável para todos os Grupos ID 3.17 – Utilizar ferramenta que permita análise do comportamento das aplicações possibilitando avaliação sequencial dos eventos - NIST CSF Detectar – aplicável para todos os Grupos ID 3.18 – Utilizar ferramenta que possibilite registro com correlação automática de eventos de segurança - NIST CSF Detectar – aplicável para todos os Grupos ID 3.19 – Utilizar ferramenta que permita que seus alertas e vulnerabilidades sejam mapeados de acordo com o framework de ataque do MITRE - NIST CSF Detectar – aplicável para todos os Grupos ID 3.20 – Utilizar ferramenta que realize escaneamentos inteligentes e automáticos em todos os componentes da rede - NIST CSF Detectar – aplicável para todos os Grupos ID 3.21 – Utilizar ferramenta que permita priorização da correção de vulnerabilidade - NIST CSF Detectar – aplicável para todos os Grupos ID 3.22 – Utilizar ferramenta que possibilite atuação pró ativa e de maneira a auxiliar o time de Segurança na preparação para resposta a possíveis incidentes - NIST CSF Recuperar – aplicável para todos os Grupos Configuração segura para hardware e software em dispositivos móveis, laptops, estações de trabalho e servidores ID 5.5 – Utilizar equipamentos (laptops e estações de trabalho) que possuam verificação da integridade com assinatura	

		criptografada do firmware durante o Boot - NIST CSF Proteger – Todos os Grupos ID 5.6 – Utilizar equipamentos (laptops e estações de trabalho) que realizem auto-recuperação do Firmware em caso de falha, ataque ou códigos maliciosos (NIST 800-193) através de uma cópia segura no próprio hardware - NIST CSF Proteger/Detectar – aplicável para todos os Grupos ID 5.7 – Utilizar equipamentos (laptops e estações de trabalho) que possuam solução de software do fabricante para verificações e atualizações contínuas de Firmwares, BIOS\UEFI e Drivers, permitindo busca na internet ou restringir a busca a um repositório na rede interna de forma centralizada e automatizada - NIST CSF Proteger – aplicável para todos os Grupos ID 5.8 – Utilizar equipamentos (laptops e estações de trabalho) que implementem travamento de configuracões de BIOS de acordo com as necessidades especificas do órgão requerente através de senhas master - NIST CSF Proteger – aplicável para todos os Grupos ID 5.9 – Utilizar equipamentos (laptops e estações de trabalho) que permitam acesso remoto apenas com consentimento do usuário, sinalização gráfica do acesso e gravação de log's para efeito de auditoria - NIST CSF Proteger/ Detectar/ Recuperar – aplicável para todos os Grupos ID 5.10 – Utilizar equipamentos (laptops e estações de trabalho) que permitam salvar as configurações da BIOS em um arquivo a ser carregado em todos os equipamentos do mesmo modelo facilitando implementação de políticas de segurança - NIST CSF Proteger/ Detectar/ Recuperar – aplicável para todos os Grupos ID 5.11 – Utilizar equipamentos (laptops e estações de trabalho) que permitam configuracão da BIOS remota e distribuição em massa, com software incluído para alterar ordem de inicialização,	

		senhas, configurações etc. e limpeza do disco rígido - NIST CSF Proteger – aplicável para todos os Grupos ID 5.12 – Utilizar equipamentos (laptops e estações de trabalho) que possuam solução de software para criptografia do disco, diretórios e arquivos específicos com gerenciamento centralizado das chaves e controle de aplicação da política, permitindo gerenciar recuperação dos dados em caso de falha - NIST CSF Proteger/ Recuperar – aplicável para todos os Grupos ID 5.13 – Utilizar equipamentos (laptops e estações de trabalho) que possuam chip de criptografia com certificado FIPS 140-2 - NIST CSF Proteger/ Recuperar – aplicável para todos os Grupos ID 5.14 – Utilizar equipamentos (laptops e estações de trabalho) que permitam implementar duplo fator de autenticação biométrico com no mínimo: - Desktops: Leitor de Impressão Digital integrado ao mouse - Notebooks: Leitor de impressão digital e/ou webcam com infravermelho compatível com a tecnologia de reconhecimento facial - NIST CSF Proteger – aplicável para todos os Grupos ID 5.15 – Utilizar equipamentos (laptops e estações de trabalho) que permitam utilizar travas e/ou cadeados contra abertura física - NIST CSF Proteger/ Detectar – aplicável para todos os Grupos ID 5.16 – Utilizar equipamentos (laptops e estações de trabalho) que permitam habilitar/desabilitar portas USB pela BIOS - NIST CSF Proteger/ Detectar – aplicável para todos os Grupos ID 5.17 – Utilizar equipamentos (laptops) reconhecidos como seguro pelo fornecedor do Sistema Operacional (Microsoft Secure-Code) - NIST CSF Detectar – aplicável para todos os Grupos ID 5.18 – Instalar solução de software anti-malware para monitorar e inibir ameaças de baseada em comportamento e	

		inteligência artificial em todos equipamentos - NIST CSF Detectar – aplicável para todos os Grupos ID 5.19 – Instalar solução de software EDR para proteção, detecção e resposta a ataques no nível do Sistema Operacional com emissão de relatórios de análise de risco - NIST CSF Detectar – aplicável para todos os Grupos ID 5.20 – Utilizar equipamentos de processamento de dados (servidores) que permitam verificação da integridade da BIOS/UEFI através de assinatura criptográfica imutável gravada em hardware (Root of Trust) - NIST CSF Proteger – aplicável para todos os Grupos ID 5.21 – Utilizar equipamentos de processamento de dados (servidores) que permitam autenticação dos módulos de firmware e sistema operacional durante a inicialização (Chain of Trust) a partir de Root of Trust em hardware e apoiada pelo UEFI Secure Boot - NIST CSF Proteger – aplicável para todos os Grupos ID 5.22 – Utilizar equipamentos de processamento de dados (servidores) com discos SED (Self-Encrypting Drives) com criptografia com criptografia FIPS 140-2 - NIST CSF Proteger – aplicável para todos os Grupos ID 5.23 – Utilizar equipamentos de processamento de dados (servidores) que permitam utilizar funcionalidade guarda de chaves (Secure Key Management) - NIST CSF Proteger – aplicável para todos os Grupos ID 5.24 – Utilizar equipamentos de processamento de dados (servidores) com discos com suporte a ISE (Instant Secure Erase) - NIST CSF Proteger – aplicável para todos os Grupos ID 5.25 – Utilizar equipamentos de processamento de dados (servidores) que possuam barreiras físicas (bezels, trancas, restrição de acesso, etc) - NIST CSF Proteger – aplicável para todos os Grupos	

		ID 5.26 – Utilizar equipamentos de processamento de dados (servidores) que possuam sensores, alarme e log de abertura de gabinete - NIST CSF Proteger – aplicável para todos os Grupos ID 5.27 – Utilizar equipamentos de processamento de dados (servidores) que permitam Habilitar/Desabilitar Portas USB pela BIOS - NIST CSF Proteger – aplicável para todos os Grupos ID 5.28 – Utilizar equipamentos de processamento de dados (servidores) que possuam solução de gerenciamento para executar verificações automáticas e contínuas dos níveis/versões de todos os firmwares e BIOS/UEFI disponíveis e checar a conformidade com o padrão institucional críticas e identificar eventuais CVE's - NIST CSF Detectar – aplicável para todos os Grupos ID 5.29 – Utilizar equipamentos de processamento de dados (servidores) que possuam verificação de integridade de HW (measured boot) e BIOS a partir de técnicas com Intel TXT e chip TPM 2.0 - NIST CSF Detectar – aplicável para todos os Grupos ID 5.30 – Utilizar equipamentos de processamento de dados (servidores) que possuam auto-recuperação de cópia de segurança da BIOS/UEFI, em área protegida no hardware do servidor, ao detectar código malicioso durante inicialização - NIST CSF Recuperar – aplicável para todos os Grupos	

Alessandro Sousa	Dell Technologies	Na tabela constante no item 8 do sumário - Checklist para utilização dos Controles Mínimos Recomendados, incluir os seguintes pontos: Defesas contra malware ID 8.9 – Utilizar solução de software anti-malware para monitorar e inibir ameaças baseadas em comportamento e inteligência artificial em todos os equipamentos de processamento de dados e endpoints - NIST CSF Proteger/ Detectar – aplicável para todos os Grupos Capacidade de recuperação de dados ID 9.6 – Utilizar equipamentos/soluções de backup que possuam verificação da integridade da BIOS/UEFI através de assinatura criptográfica imutável gravada em hardware (Root of Trust) - NIST CSF Proteger – aplicável para todos os Grupos ID 9.7 – Utilizar equipamentos/soluções de backup que possuam autenticação dos módulos de firmware e sistema operacional durante a inicialização (Chain of Trust) a partir de Root of Trust em hardware e apoiada pelo UEFI Secure Boot - NIST CSF Proteger – aplicável para todos os Grupos ID 9.8 – Utilizar equipamentos/soluções de backup que realizem criptografia dos dados em repouso (Data at Rest – D@RE) com certificação FIPS 140-2 - NIST CSF Proteger – aplicável para todos os Grupos ID 9.9 – Utilizar equipamentos/soluções de backup que possuam funcionalidade de guarda de chaves (Secure Key Management) - NIST CSF Proteger – aplicável para todos os Grupos ID 9.10 – Utilizar equipamentos/soluções de backup que garantam imutabilidade dos dados através de recursos de WORM (Write Once Read Many) certificado SEC 17a-4(f) para garantir que os dados não serão alterados ou excluídos - NIST CSF Proteger – aplicável para todos os Grupos	Sugestão rejeitada. Insiste-se em trabalhar apenas com os controles do próprio SisControl, mantendo a estratégia que já vem sendo adotada de manter controles que possam garantir a exequibilidade e efetividade do normativo proposto levando em conta o conhecimento sobre o contexto do Judiciário. Sugestão poderia levar, ademais, a direcionamentos em eventuais contratações por parte dos tribunais.

		ID 9.11 – Utilizar equipamentos/soluções de backup que garantam imutabilidade dos dados mesmo em caso onde o cibercriminoso altere/adiante a data do sistema para poder alterar/excluir os arquivos protegidos (System Clock Hardening Protection) - NIST CSF Proteger – aplicável para todos os Grupos ID 9.12 – Utilizar equipamentos/soluções de backup que utilizem recurso de dupla autenticação (2FA – Two Fator Authentication) para executar atividades administrativas de exclusão no equipamento - NIST CSF Proteger – aplicável para todos os Grupos ID 9.13 – Utilizar equipamentos/soluções de backup que realizem leitura e gravação no equipamento através de API com controle de acesso através de usuário e senha, não utilizando compartilhamento CIFS/NFS ou montagem do disco/volume no servidor de backup - NIST CSF Proteger – aplicável para todos os Grupos ID 9.14 – Utilizar equipamentos/soluções de backup que possuam suporte de arquitetura com isolamento via Air Gap para impedir a propagação do ataque cibernético no momento da sincronização entre os sistemas em rede segregada - NIST CSF Proteger – aplicável para todos os Grupos ID 9.15 – Utilizar equipamentos/soluções de backup que utilizem barreiras físicas (bezels, trancas, restrição de acesso, etc) a fim de restringir o acesso ao equipamento e seus componentes - NIST CSF Proteger – aplicável para todos os Grupos ID 9.16 – Utilizar equipamentos/soluções de backup que possuam sensores, alarme e log de abertura de gabinete/ rack - NIST CSF Proteger – aplicável para todos os Grupos ID 9.17 – Utilizar equipamentos/soluções de backup que utiizem recursos de segurança e autenticação seguindo padrões internacionais de segurança NIST SP 800-171 - NIST CSF Proteger	

		– aplicável para todos os Grupos ID 9.18 – Utilizar equipamentos/soluções de backup que estejam em conformidade com padrões de segurança internacionais conforme descrito no DISA STIG como referência - NIST CSF Proteger – aplicável para todos os Grupos ID 9.19 – Utilizar equipamentos/soluções de backup que realizem identificação da corrupção de dados, incluindo criptografia, ransomware, destruição e corrupção lenta dos arquivos copiados - NIST CSF Detectar – aplicável para todos os Grupos ID 9.20 – Utilizar equipamentos/soluções de backup que possuam ferramentas forenses e façam uso de métodos analíticos de aprendizado de máquina (Machine Learning) para encontrar arquivos corrompidos e diagnosticar o vetor de ataque a partir da imagem de backup - NIST CSF Detectar – aplicável para todos os Grupos ID 9.21 – Utilizar equipamentos/soluções de backup que realizem varredura no conteúdo completo dos arquivos (full-content) incluindo metadados a fim de identificar uma alteração maliciosa - NIST CSF Detectar – aplicável para todos os Grupos ID 9.22 – Utilizar equipamentos de backup que possuam sistema de proteção utilizando snapshots internos que permitam melhorar a segurança dos dados e índices a fim de permitir a recuperação para um momento anterior ao incidente - NIST CSF Recuperar – aplicável para todos os Grupos ID 9.23 – Utilizar equipamentos/soluções de backup que realizem cópia lógica periódica das informações para segundo sítio preservando os dados originais - NIST CSF Recuperar – aplicável para todos os Grupos ID 9.24 – Utilizar equipamentos/soluções de backup que permitam restaurar e iniciar de maneira imediata a execução de uma máquina virtual instantaneamente, diretamente a partir do	

		seu repositório de backup, sem necessidade de recuperação dos dados para o ambiente de produção - NIST CSF Recuperar – aplicável para todos os Grupos ID 9.25 – Utilizar equipamentos/soluções de backup que possuam a funcionalidade de recuperação instantânea (Instant Recovery) que permita recuperar múltiplas VMs simultâneas a partir do repositório de backup desduplicado - NIST CSF Recuperar – aplicável para todos os Grupos Proteção de dados ID 10.7 – Utilizar equipamentos de armazenamento de dados que realizem autenticação de acesso individual com integrações aos protocolos LDAP e AD - NIST CSF Proteger – aplicável para todos os Grupos ID 10.8 – Utilizar equipamentos de armazenamento de dados que garantam a imutabilidade de informações através de tecnologia WORM (Write Once Read Many) onde os dados não sejam sobrescritos / alterados - NIST CSF Proteger – aplicável para todos os Grupos ID 10.9 – Utilizar equipamentos de armazenamento de dados que transmitam dados de forma criptografada entre soluções ou sítios - NIST CSF Proteger – aplicável para todos os Grupos ID 10.10 – Utilizar equipamentos de armazenamento de dados que possuam tecnologia de Proteção de Dados Air-Gap com bloqueio de acesso a solução secundária, imediatamente após a realização de cada cópia de segurança - NIST CSF Proteger – aplicável para todos os Grupos ID 10.11 – Utilizar equipamentos de armazenamento de dados que adotem padrão de criptografia de dados em repouso FIPS 140-2 - NIST CSF Proteger – aplicável para todos os Grupos ID 10.12 – Utilizar equipamentos de armazenamento de dados que realizem provisionamento de funcionalidade de guarda e	

		gerenciamento de chaves criptográficas (Secure Key Management) - NIST CSF Proteger – aplicável para todos os Grupos ID 10.13 – Utilizar equipamentos de armazenamento de dados que realizem provisionamento de discos/drives com suporte a ISE (Instant Secure Erase) - NIST CSF Proteger – aplicável para todos os Grupos ID 10.14 – Utilizar equipamentos de armazenamento de dados que possuam barreiras físicas (bezels, trancas e cadeados, restrições de acesso) - NIST CSF Proteger – aplicável para todos os Grupos ID 10.15 – Utilizar equipamentos de armazenamento de dados que possuam sensores, alarmes e logs de abertura de gabinetes e chasssis - NIST CSF Proteger – aplicável para todos os Grupos ID 10.16 – Utilizar equipamentos de armazenamento que protejam os dados em caso de roubo dos mesmos por meio de tecnologia de criptografia em repouso - NIST CSF Proteger – aplicável para todos os Grupos ID 10.17 – Utilizar equipamentos de armazenamento de dados que permitam proteção geográfica dos dados com distribuição ou Replicação dos dados - NIST CSF Proteger – aplicável para todos os Grupos ID 10.18 – Utilizar equipamentos de armazenamento de dados que realizem copia lógica periódica das informações para segundo sítio preservando os dados originais - NIST CSF Recuperar – aplicável para todos os Grupos ID 10.19 – Utilizar equipamentos de armazenamento de dados que realizem cópia contínua para segunda solução ou sítio preservando todas as características originais de segurança e metadados das informações - NIST CSF Recuperar – aplicável para todos os Grupos	

Anexo V – Manual Prevenção e Mitigação

Nome	Órgão/Empresa	8. Sugestões no Anexo V – Manual Prevenção e Mitigação	
Marco Aurélio Barbosa Schaan	TRF4	21.Processo de Gestão de Riscos de Segurança da Informação. A gestão de risco ainda não funciona plenamente dentro da gestão de TI, portanto, a Gestão de Riscos de Segurança da Informação tem o papel preponderante de implantar definitivamente a Gestão de Riscos.	Sugestão rejeitada. Não há proposta concreta de alteração.
Hetug Sardeiro Porto	TRT5 (Bahia)	Item 13.1 a) - Sugestão: O processo de gestão de riscos de segurança da informação deve ser parte integrante de todos processos organizacionais, não só dos processos de Tecnologia da Informação e Comunicação (TIC), alinhando-se à Resolução (Art. 21). Item 15.1 c) - Sugestão: A unidade responsável pela Gestão de Segurança da Informação do órgão como um todo, não só de TIC, alinhando-se à Resolução (Art. 21). Item 16 - Sugestão: Utilizar a mesma nomenclatura empregada na Resolução (Art. 20), qual seja, Comitê de Governança de Segurança da Informação (CGSI). Item 16.1 - Sugestão: Utilizar a mesma nomenclatura empregada na Resolução (Art. 20), qual seja, Comitê de Governança de Segurança da Informação (CGSI). Alinhar essas competências com as mesmas previstas na Resolução (Art. 20).	Item 13.1 a): Sugestão rejeitada. Talvez fosse interessante, mas a parte de GR foi construída sobre a norma NBR ISO 27005. Item 15.1 c): Sugestão rejeitada em razão da rejeição da proposição anterior. Item 16 e 16.1: Sugestão parcialmente acolhida para que se proceda o alinhamento da nomenclatura e, caso constatada duplicação de texto, remoção do anexo. Item 17: Sugestão rejeitada conforme comentários aos itens 13.1 a) e 15.1 c). Item 17, IV: Sugestão acolhida para que se proceda a correção na sigla. Item 18: Sugestão rejeitada conforme comentários aos itens 13.1 a), 15.1 c) e 17.

		Item 17 - Sugestão: As competências previstas devem ser de todas as unidades dirigentes do órgão, não somente de TIC, alinhando-se à Resolução (Art. 21). Item 17, IV - Dúvida: A que se refere a sigla CGETI? Não seria CGSI? Item 18 - Sugestão: Unidade responsável pela Gestão de Segurança da Informação do Órgão, não somente de TIC, alinhando-se à Resolução (Art. 21). Item 33.1 d) - Sugestão: Alterar redação para: "O acesso lógico aos ativos…"	Item 33.1 d): Sugestão acolhida para que se proceda a correção.
Paulo Roberto Mendes	TRE-MG	Definir melhor se isto é um "manual", uma "política", um "modelo", uma "referência" ou uma "norma" a ser cumprida; Citar os alinhamentos às normas e modelos de referência, mas deixar as descrições deles no glossário; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação); Citar o alinhamento deste à PGR (política de gestão de riscos corporativos); Como o processo de riscos de segurança da informação é bem similar ao de riscos corporativos (na verdade devendo ser um subconjunto específico daqueles riscos), concentrar apenas nas possíveis diferenças ou especificidades relativas a este tipo de risco, sem descrever um processo completo; Na parte de auditoria de riscos, referenciar os materiais disponibilizados pelo TCU, a exemplo da planilha com o roteiro	1ª. Sugestão: Sugestão rejeitada. Quanto a definir se se trata de um "manual", uma "política", um "modelo", uma "referência" ou uma "norma" a ser cumprida, tenha-se em mente que a portaria que deverá aprovar o normativo estabelece que seus anexos são de observância obrigatória. Não há espaço, portanto, para interpretação divergente, no sentido de tratar-se de mera recomendação. 2ª. Sugestão: Sugestão rejeitada. Em relação aos comentários referentes à similitude entre os riscos da segurança da informação e dos riscos corporativos, concorda-se com a visão do colaborador. Contudo, tal não impede que se mantenha a descrição do processo de uma forma mais ampla apenas pelo fato de não

		de auditoria de gestão de riscos, o manual de avaliação de maturidade em gestão de riscos, o referencial básico de gestão de riscos, a política de gestão de riscos e os apêndices com os critérios para avaliação de maturidade em gestão de riscos e a matriz de planejamento de auditoria em riscos; Incluir exemplos mais extensivos de design para resiliência cibernética; Referenciar melhor (fazer um link) do framework de resiliência cibernética com os protocolos dos anexos I, II e III; Utilização de checklist padrão, para ser respondido por todos os órgãos, e não apenas como modelo; Padronizar o checklist para recomendar as práticas por grupo (aplicabilidade de cada controle em relação ao porte da organização, categorizado por Grupo 1, Grupo 2 e Grupo 3, esses grupos fornecem uma forma simples e acessível de ajudar as organizações de diferentes portes a direcionar seus recursos com o melhor custo × benefício, alcançando os melhores resultados na busca pela mitigação do risco); Incluir medidas organizacionais que apoiem a efetivação de cada um dos controles técnicos elencados no checklist.	contemplar todas as categorias de riscos de um processo corporativo. 3ª. Sugestão. Sugestão rejeitada. Com relação à utilização de checklist padrão, para ser respondido por todos os órgãos, trata-se mais de uma questão de formatação, pois trata-se do mesmo conjunto de controles. 4ª. Sugestão. Sugestão rejeitada por se entender que os grupos herdados do Siscontrol, em sua versão 7.1, são os mais adequados para o checklist em questão. 4ª. Sugestão. Sugestão rejeitada. Quanto à inclusão de medidas organizacionais que apoiem a efetivação de cada um dos controles técnicos elencados no checklist, salientou-se que, ao assim fazer, estar-se-ia interferindo na forma de cada órgão irá trabalhar para alcançar os controles almejados.
Juarez de Oliveira	TRE-PR	Situações operacionais devem ser avaliadas pelas equipes operacionais, durante a execução das políticas definidas pelos comitês. Elaborar esse tipo de procedimento não é atribuição do CNJ e pode levar a mais dúvidas ainda por parte das equipes técnicas. Este manual não deve existir.	Sugestão rejeitada. O juízo de legalidade, conveniência e oportunidade já foi exercido pela Presidência do CNJ na Portaria 242/2020.
Eder Santana Freire	TRT20	Avaliar a disponibilização, a todos os órgãos do Poder Judiciário, de cópias atualizadas e licenciadas das normas mencionadas no manual (tendo em vista que as normas publicadas pela ABNT, por exemplo, são de acesso restrito, e precisam ser adquiridas para uso e aplicação regular).	Sugestão rejeitada por fugir ao escopo da presente normatização, embora possa ser recomendada oportunamente. Salientou-se que o TST dispõe dos documentos, que poderiam ser disponibilizados aos TRTs.

Mateus Cançado Assis	TJMG	1.1 - DE “a empresa” - PARA “o órgão” (“... orientações que se adequam melhor ao cenário em que O ÓRGÃO se encontra atualmente…”), ou ainda o termo “instituição” a exemplo do item análogo “3.0.1” (sic) no Manual de Gestão de Identidade (Anexo VI). 2.1 - Incluir o URL de referência: “A publicação está disponível para uso gratuito por qualquer pessoa ou organização, em https://attack.mitre.org/” 3.1 - Considerando que as normas técnicas da ABNT e ISO podem implicar em custos que dificultem o acesso por órgãos com menor disponibilidade orçamentária, é interessante adicionar nota (rodapé) como: “A versão original da norma ISO/IEC 27000:2018 está publicamente disponível em https://standards.iso.org/ittf/PubliclyAvailableStandards/.” 6.1 - DE “... em complemento às diretrizes descritas na ABNT NBR ISO 19011:2012” - PARA “... em complemento às diretrizes descritas na norma ABNT NBR ISO/IEC 19011:2018” 9 - DE “NIST SP 800-160 v2” - PARA “NIST SP 800-160 Vol. 2” - A abreviatura “v2” induz incorretamente a “versão 2”, quando de fato é “Volume 2.	Sugestões parcialmente acolhidas. Trata-se de pontuações referentes a formatação e inclusão de dados faltantes, cabendo uma revisão referente aos pontos citados e outros pontos não mencionados que também possam ser aprimorados.

		9.1 - DE “Esta publicação é usada em conjunto …” - PARA “A publicação NIST Special Publication 800-160, Volume 2 (Desenvolvendo Sistemas Cyber Resilientes: Uma - - Abordagem de Engenharia de Segurança de Sistemas) é usada em conjunto …” 9.2 - DE “Ele pode ser visto como …” - PARA “Pode ser visto como …” 11.5 - DE “... (publicado por meio da norma NBR 31.000) …” - PARA “... (publicado por meio da norma ABNT NBR ISO 31000:2018) …” - Como esta norma não é citada anteriormente nas referência, é recomendável definir sua identificação completa para maior clareza e precisão. Notas de rodapé 13, 14 e 15, respectivas aos itens 27.1, 28.1 e 29.1 - DE “... v2 …” - PARA “... Vol. 2 …” (vide apontamento para item 9 acima) - Além disso, os itens 28.1 e 29.1 poderiam referenciar a mesma nota de rodapé 13, ao invés de criar notas de rodapé idênticas. Notas de rodapé 17 e 18 - Poderiam ser unificadas em uma só e reusadas nas referências nos respectivos textos, notando que a 18 está mais completa pois cita URL da fonte.	

Anexo VI – Manual Gerenciamento Identidade Acesso

Nome	Órgão/Empresa	9. Sugestões no Anexo VI – Manual Gerenciamento Identidade Acesso	
Paulo Roberto Mendes	TRE-MG	Definir melhor se isto é um “manual”, uma “política”, um “modelo”, uma “referência” ou uma “norma” a ser cumprida; Citar os alinhamentos às normas e modelos de referência, mas deixar as descrições deles no glossário; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação); Utilização de checklist padrão, para ser respondido por todos os órgãos, e não apenas como modelo; Padronizar o checklist para recomendar as práticas por grupo (aplicabilidade de cada controle em relação ao porte da organização, categorizado por Grupo 1, Grupo 2 e Grupo 3, esses grupos fornecem uma forma simples e acessível de ajudar as organizações de diferentes portes a direcionar seus recursos com o melhor custo × benefício, alcançando os melhores resultados na busca pela mitigação do risco); Incluir controles dos outros modelos de referência no checklist, se for o caso, e não apenas do CIS Controls; Incluir medidas organizacionais que apoiem a efetivação de cada um dos controles técnicos elencados no checklist.	1ª Sugestão. Sugestão rejeitada. Quanto a definir se se trata de um “manual”, uma “política”, um “modelo”, uma “referência” ou uma “norma” a ser cumprida, tenha-se em mente que a portaria que deverá aprovar o normativo estabelece que seus anexos são de observância obrigatória. Não há espaço, portanto, para interpretação divergente, no sentido de tratar-se de mera recomendação. 2ª. Sugestão. Sugestão rejeitada. Quanto à deixar as descrições dos modelos de referência no glossário, entendeu-se tratar-se de questão formal, que não altera o conteúdo material do documento. 3ª. Sugestão. Sugestão rejeitada. Quanto ao alinhamento com a PSI, trata-se de item já apreciado em ponderações anteriores. 4ª. Sugestão. Sugestão rejeitada. Quanto à questão da utilização do checklist, trata-se de item já apreciado em ponderações anteriores. 5ª. Sugestão. Sugestão rejeitada. Não haveria problemas em padronizar o checklist por grupo, mas nem sempre o tamanho da organização ou orçamento implica na necessidade de um maior nível de gestão de identidades e

			controles de acessos. A maior parte dos controles não está relacionada a investimento financeiro, mas a processos de trabalho. E isto está mais relacionado à maturidade e visão de segurança do que a outra coisa. Questão já apreciada em sugestões anteriores 6ª. Sugestão. Sugestão rejeitada. Quanto aos itens do checklist, trata-se de questão já apreciada em sugestões anteriores. 7ª. Sugestão. Sugestão rejeitada. Quanto às outras medidas organizacionais, a questão já foi tratada em sugestões anteriores
Juarez de Oliveira	TRE-PR	Situações operacionais devem ser avaliadas pelas equipes operacionais, durante a execução das políticas definidas pelos comitês. Elaborar esse tipo de procedimento não é atribuição do CNJ e pode levar a mais dúvidas ainda por parte das equipes técnicas. Este manual não deve existir.	Sugestão rejeitada. O juízo de legalidade, conveniência e oportunidade já foi exercido pela Presidência do CNJ na Portaria 242/2020.
Eder Santana Freire	TRT20	Observar que uma nova versão do framework Cis Controls (v 8.0) será disponibilizada no mês que vem (maio/2021): https://www.cisecurity.org/controls/v8/ Desse modo, recomendo que avaliem se não vale a pena aguardar pela divulgação desta nova versão, para que o manual seja publicado já com as devidas atualizações.	Sugestão rejeitada por já ter sido avaliada anteriormente em outra proposição.
Mateus Cançado Assis	TJMG	2 - Os parágrafos estão incorretamente numerados como 3.0.1 e 3.0.2. Deveriam ser 2.0.1 e 2.0.2. 9, coluna “Referencial” da tabela, todas as linhas	2 e 9: Sugestões parcialmente acolhidas para que se proceda a correção e realizar uma validação geral.

		- DE “CIS Control 7.1” - PARA “CIS Controls v7.1”	

Anexo VII – Política de Educação e Cultura

Nome	Órgão/Empresa	10. Sugestões no Anexo VII – Política de Educação e Cultura	
Adriano Meirelles Borba	TRE-MT	Sugiro que seja fortemente incentivada a orientação dos servidores quanto a aspectos básicos de segurança digital, tanto em equipamentos profissionais quanto pessoais (já que os celulares e PCs pessoais têm sido largamente utilizados também para o trabalho, tornando-se uma possível porta de entrada para invasores). Adicionalmente, poderia ser melhor fomentada também a capacitação dos servidores para manuseio de diversas ferramentas auxiliares de produtividade, como Excel e PowerPoint (por favor, nada de LibreOffice ou outros alternativos menos eficazes). Essa promoção poderia, na prática, se dar com a promoção de um ou dois eventos anuais de participação obrigatória dos servidores, via EAD com tutoria, visando reforçar aspectos de segurança e privacidade digitais (visando a aplicação prática desses conceitos no dia a dia de trabalho), e outros cursos EAD diversos para capacitação em aplicações auxiliares (aplicativos do Office, navegadores, Canva, etc), de caráter opcional e sem tutoria, com cômputo de carga horária para registro individual como ação de treinamento	Sugestões rejeitadas. As sugestões serão contempladas pelos Planos de Capacitação elaborados pelos órgãos ou mesmo nas ações concretas efetivamente realizadas. As sugestões referem-se mais a aspectos operacionais e aspectos de execução, não cabendo no âmbito da presente proposta de Política.

		realizada. Dada a abrangência dos temas, a fim de otimizar o planejamento e execução, tais cursos poderiam ser criados e coordenados pelo CNJ, ou pela corte superior de cada esfera envolvida (TSE para Eleitoral, STJ para as Justiças Estaduais e TRFs, TST para a Justiça do Trabalho, etc.).	
Ana Lucia Lourenço	TJPR	No 3.1.1.Compete às Escolas de Formação, aos Centros de Educação e Capacitação e às demais unidades administrativas responsáveis pela capacitação de magistrados e magistradas e de servidores e servidoras do Poder Judiciário", sugiro incluir as Escolas Associativas, e também um item recomendando o não afastamento do servidor ou magistrado de suas funções para participação dos cursos, dado o grande acúmulo de feitos em tramitação em todos os tribunais do país e também a excessiva cobrança de metas a que todos estão submetidos.	Sugestão rejeitada. Deverão estar contempladas todas as Escolas e unidades que detenham a efetiva competência para a realização de ações de capacitação previstas nesta Política. A participação de outras entidades deve ficar a cargo dos normativos vigentes em cada órgão. Quanto às regras de afastamento ou não afastamento, caberá a cada ação específica fixar os critérios e condições de participação.
Marco Aurélio Barbosa Schaan	TRF4	Não é implementado pelo TRF4	Sugestão rejeitada. Não se compreendeu a intenção de proposta enviada, mais parecendo-se a uma crítica.

Hetug Sardeiro Porto	TRT5 (Bahia)	Item 2.1.3 - Sugestão: Melhorar a redação da expressão: “carga horária mínima de capacitação não superior a 1 (um) ano”. Não seria “não inferior a 1 (ano) ano”?	Sugestão acolhida, para simplificação do texto. Proposta de redação: “2.1.3. Cada órgão do Poder Judiciário deverá estabelecer uma carga horária mínima de capacitação, podendo as ações previstas neste Manual serem efetuadas em diversas cargas horárias e níveis de formação, assim divididas:”
Paulo Roberto Mendes	TRE-MG	Definir melhor se isto é um “manual”, uma “política”, um “modelo”, uma “referência” ou uma “norma” a ser cumprida; Citar o alinhamento deste à PSI ou POSIC (política de segurança da informação); Trabalhar com trilhas de capacitação por público alvo, criando perfis específicos, ao invés de listar todos os assuntos sem maiores orientações; Trabalhar com trilhas de maturidade (mastery model), mostrando a sequência de capacitações para o aumento de maturidade em determinado tema, escolhendo o repertório de etapas a partir das seguintes alternativas: SFIA (7 níveis), Dreyfus (5 níveis), Shu-ha-ri (3 níveis), Tuckman (4 níveis) ou outra adequada; Associar os temas à competências a serem desenvolvidas por perfil; Não associar competências à áreas que podem ter atribuições diversas nos órgãos. Por exemplo: em alguns órgãos a Gestão de Pessoas é responsável pelo desenvolvimento e capacitação dos colaboradores e colaboradoras, desde a gestão do plano até o pagamento dos cursos contratados; em outros órgãos a Escola Judiciária é responsável pela formulação do plano e contratação e pagamento dos cursos, treinamentos, eventos.	1ª. Sugestão. Sugestão rejeitada. Questão já apreciada em proposições anteriores. 2ª. Sugestão. Sugestão rejeitada. O alinhamento das ações de capacitação estão explicitamente vinculados a outras Políticas, Planos e Normas vigentes nos órgãos. Não há necessidade de especificar. 3ª. Sugestão. Sugestão rejeitada. Quanto às trilhas de maturidade, trata-se de assunto voltado à elaboração dos Planos de Capacitação e à operacionalização das ações. Quanto às demais sugestões, também são rejeitadas em razão de também se referirem a aspectos de planejamento e operacionalização.

Juarez de Oliveira	TRE-PR	Situações operacionais devem ser avaliadas pelas equipes operacionais, durante a execução das políticas definidas pelos comitês. Elaborar esse tipo de procedimento não é atribuição do CNJ e pode levar a mais dúvidas ainda por parte das equipes técnicas. Esta política nem deveria existir, apenas um plano em cada tribunal.	Sugestão rejeitada. O juízo de legalidade, conveniência e oportunidade já foi exercido pela Presidência do CNJ na Portaria 242/2020.
Eder Santana Freire	TRT20	Seria interessante que o CNJ pudesse desenvolver um programa nacional de capacitação em segurança da informação e proteção de dados, direcionado às equipes técnicas de todos os órgãos do Poder Judiciário. Tal programa poderia abranger ações de treinamento e capacitação nas diversas disciplinas e tecnologias que envolvem o tema da segurança cibernética, e poderia contar com a participação ativa de servidores, especialistas nestas matérias, que atuariam como instrutores e monitores. As ações poderiam ser realizadas em ciclos periódicos e agrupadas em eixos temáticos, com a disponibilização de vagas para representantes de todos os órgãos que compõem o PJ.	Sugestão rejeitada. As sugestões referem-se a aspectos de planejamento e operacionalização. Em termos de Política, mantém-se a proposta de redação como está na minuta.
Mateus Cançado Assis	TJMG	1.1.1 e adiante - A sigla "PCESC-PJ" é introduzida sem definição formal prévia. Supõe-se ser a própria Política de educação e cultura em segurança cibernética do Poder Judiciário, mas a sigla natural seria "PECSC-PJ". A definição inicial "Política de educação e cultura em segurança cibernética do Poder Judiciário (PECSC-PJ)" (ou PCESC-PJ como está) deveria estar definida na primeira ocorrência, em 1.1.1. 1.3.1	1.1.1. Sugestão parcialmente acolhida para que se aprecie a questão durante a revisão final da minuta. 1.3.1 sugestão acolhida. Para melhor entendimento da sigla no decorrer da leitura do texto, sugere-se a inclusão da definição da sigla PECSC-PJ em sua primeira aparição no texto. 1.4.1 sugestão acolhida. Retirar o item 1.4.1

		- O tópico redefine desnecessariamente a abrangência do que é “segurança cibernética” que já está definida no parágrafo único do art. 1º da minuta de Resolução. 1.4.1 - Apontamento idêntico ao feito para o Art. 36, incisos I a IV, da minuta de Resolução (vide acima).	

Anexo VIII – Glossário

Nome	Órgão/Empresa	11. Sugestões no Anexo VIII – Glossário	
Waldir Costa Sola	TRF3	II –aumentar a resiliência às ameaças cibernéticas; IV –permitir a manutenção e continuidade dos serviços ou o seu restabelecimento em menor tempo possível resiliência significa "o seu restabelecimento em menor tempo possível" em minha opinião o item II e IV são redundantes e eu removeria o item II	Sugestão rejeitada. Não se refere ao Glossário, mas sim aos incisos do art. 6º da Minuta. Não é pertinente.
Paulo Roberto Mendes	TRE-MG	Alinhar este glossário às definições em normas (ISO 27000, etc) e modelos de referência em riscos e segurança da informação (COSO, COBIT, etc), mantendo as referências e fontes; Incluir definição clara e concisa de segurança cibernética; Incluir aqui, eliminando dos outros manuais, as descrições dos modelos de referência (por exemplo, CIS Controls, MITRE ATT&CK, ISO 27000, ISO 31000, NIST SP 800-53, etc).	Sugestão rejeitada. Não houve uma sugestão de redação. Ademais, a proposta não é compatível com os objetivos estritos do presente glossário.
Juarez de Oliveira	TRE-PR	O maior problema tem sido a confusão entre cibersegurança, constante em alguns trechos, e segurança da informação.	Sugestão rejeitada. Não se refere ao glossário e não houve sugestão de redação. Trata de esclarecimento terminológico que já foi objeto de apreciação.

Mateus Cançado Assis	TJMG	2 - DE “Agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) …” - PARA “Agente responsável pela ETIR …” - Como a sigla ETIR é definida no item 27 do glossário, pode ser utilizada apenas a sigla; mas se for repetir a definição, estava incorreta, deveria ser “Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética”.	Sugestão acolhida para corrigir o item 2 do glossário para que se compatibilize com o item 27.

Sugestões de cunho geral

Nome	Órgão/Empresa	12. Sugestões de cunho geral:	
Elson Correia de Oliveira Neto	TJAC	A Minuta Resolução Estratégia Segurança Cibernética Poder Judiciário, está com seu texto excelente e praticamente pronto a meu ver. Sugeriria, apesar de já previsto, que ficasse mais claro o envolvimento da alta administração com a Estratégia Segurança Cibernética Poder Judiciário, bem como com outras estratégias, como a ENTIC-JUD. Me parecesse que a alta administração de um modo geral, enxerga essas estratégias como demandas diretas do CNJ para os setores de Tecnologia da Informação, simplesmente isso, quando na verdade elas têm como principal objetivo, o conjunto envolvimento da alta administração dos órgãos judiciais e seus setores de Tecnologia da Informação, aplicando as melhores práticas de gestão de TI e de Segurança da	Sugestões acolhidas e já incorporadas ao texto

		Informação no caso desta Estratégia Nacional Segurança Cibernética.	
Ana Lucia Lourenço	TJPR	A principal porta de entrada das ameaças virtuais está nas falhas de segurança nos e-mails corporativos de modo que sugiro que tal questão deve ser abordada nos manuais. No que se refere a alocação de recursos financeiros para a segurança cibernética em todos os Tribunais seria interessante fazer um questionário investigativo sobre quanto e como cada um dos Tribunais da Federação disponibiliza neste enfrentamento para evitar que recursos sejam aplicados na contramão da política ora instituída.	Sugestão rejeitada. Trata-se de sugestões de cunho operacional, razão pela qual não se vislumbra razão para alteração dos textos produzidos
Felipe Valente da Silva Paiva	Fundação Santiago e Montesuma	Faço menção ao art. primeiro da resolução onde fala sobre segurança dos sistemas , é necessário que seja feito um banco de dados onde o servidor de vocês possam ter um sistema de trava automática para que assim os invasores possam cair sempre em uma ante sala e nunca conseguirem entrar no núcleo onde fica armazenado , pra isso é necessário que haja uma análise por um engenheiro de computação	Sugestão rejeitada. Foge ao escopo da estratégia, por se tratar de sugestão de implementação operacional.

Marco Aurélio Barbosa Schaan	TRF4	Quando falamos de Transformação Digital e satisfação do usuário interno e externo a primeira conclusão é que os projetos definidos no papel, o planejamento, tenha alinhamento completo com as Metas definidas a nível nacional. A Política de Educação deve ser tratada como um referencial para atingir as METAS nacionais e regionais. Como o Judiciário não ambiciona lucro como uma empresa de capital privado a satisfação do usuário deve ser o principal meio de medir os objetivos a serem alcançados. O que gera certo temor, pois trata-se de mera política.	Sugestão rejeitada. O comentário não apresenta sugestão de alteração do texto.
Deborah Araujo Santos Pondelek	TJPR	Considero o esforço na implementação da ETIR, bem como a prática dos princípios norteadores da segurança cibernética essenciais para compensar quaisquer danos causados direta ou indiretamente. No entanto, convém buscar ferramentas eficientes que impeçam a reincidência secundária, tornando-se desnecessário novo procedimento preventivo do incidente previamente identificado.	Sugestão rejeitada. O comentário não apresenta sugestão de alteração do texto
Paulo Roberto Mendes	TRE-MG	Simplificar a resolução, definido diretrizes mais objetivas, conforme sugestão do checklist único nas observações acima.	Sugestão rejeitada. Sugestões específicas tratadas em comentários anteriores.

Juarez de Oliveira	TRE-PR	Está ocorrendo uma grande confusão com a mistura de enfoques na ENTIC e na ENSEC ao mesmo tempo. Primeiro de tudo isso precisa ser revisto. Se existirá uma ENSEC, ela precisa ser referenciada diretamente na ENTIC, que não deve tratar desse assunto, a não ser no nível de planejamento orçamentário. Não é possível duas Estratégias versarem sobre o mesmo assunto. O Plano de Continuidade de Negócios está muito mal referenciado nas duas Estratégias e não deve estar sobre a égide da área de tecnologia da informação e sim sobre a alta administração. O comitê de crise precisa ser único e não de cibersegurança, isso não existe na literatura nem na vida real. O CNJ precisa se atentar apenas a Estratégia (objetivos, estruturas organizacionais, orçamentos, metas, etc). A parte operacional é um desdobramento disso, e só vai lograr êxito se os tribunais tirarem a governança de segurança da informação e proteção de dados de dentro das áreas de TI e subirem para a alta administração, deixando para a TI a parte operacional efetivamente, no que lhe couber. Tendo dito isto e já pelo que expus sobre os capítulos da ENSEC, acho que primeiramente se precisa de uma Estratégia mais clara exequível e de médio e longo prazos.	Sugestões parcialmente acolhidas. Será realizado um alinhamento entre as possíveis concorrências existentes entre a ENTIC e a ENSEC. No mais, não há sugestões concretas de alteração nos textos produzidos.
Eder Santana Freire	TRT20	Atuo na área de Segurança da Informação do TRT da 20ª Região, e encaminho algumas breves contribuições a respeito da consulta pública que definirá a Estratégia e a Governança Cibernéticas do Poder Judiciário. Tendo em vista as diversas demandas de segurança da informação que estamos recebendo (sobretudo aquelas advindas da LGPD), e com a proximidade do fim do prazo concedido para envio das respostas, não pude me debruçar	Agradecemos a participação.

		sobre os documentos da forma que gostaria (tanto que só pude fazê-lo hoje, neste Sábado de Aleluia, e de forma superficial). Mas espero que as poucas contribuições que trago (ou, ao menos parte delas) possam ser úteis ao processo de revisão dos documentos. Permaneço à disposição para continuar contribuindo, bem como para participar de eventual fórum nacional de discussão a respeito do tema governança em segurança cibernética, caso me seja dada a oportunidade.	
Diógenes Antônio Paiva	TRE-PB	Não se trata de sugestões, mas elogio ao elevado nível técnico e detalhamento cuidadoso dos protocolos propostos.	Agradecemos a participação.