RELATÓRIO DE MONITORAMENTO

I. IDENTIFICAÇÃO	
Nº do Processo	Proad nº 95/2019
Nº da Ordem de Serviço	01/2019
Unidade Auditada	Secretaria de Tecnologia da Informação e Comunicação
Seção Responsável pela Auditoria	Seção de Auditoria de Gestão Administrativa e Patrimonial – SAGAP
Objeto da Auditoria	Gestão e Governança de tecnologia da informação e comunicação, estabelecida no TRT 7ª Região, notadamente ***o processo de implantação da Gestão de Riscos de TIC e a estratégia de tratamento de incidentes de segurança de TIC***
Tipo de Auditoria	Conformidade

II. CONSTATAÇÕES

Constatação nº 1

Descrição sumária:

Ausência de apuração dos indicadores relacionados ao Objetivo 3 (Implementar a gestão de Riscos de TI) do Plano Estratégico de TIC - PETIC 2015-2020.

Determinação 1.1:

1.1 Elaborar proposta de revisão dos indicadores e metas definidos no PETIC 2015-2020 referente ao objetivo 3: "Implementar a gestão de riscos de TI."

Providências adotadas:

Manifestação da SETIC:

A recomendação 1.1 foi deliberada pelo Comitê de Governança de TIC na reunião de 16/05/2019.

As soluções críticas de TIC, para efeito o mapeamento de riscos, bem como as metas de 2019 e 2020 foram definidas.

Ata da reunião do CGTIC de 16/05/2020 (ver item 2 da pauta) :

https://proad.trt7.jus.br/proad/pages/pdfprint/DOCUMENTO%20-%20Ata%20da%20Reuni%C3%A3o%20do%20Comit%C3%AA%20de%20Governan%C3%A7a%20de%20TIC%20de%2016-05-2019.pdf?nrSequencial=40&numeroProtocolo=6057&numeroAno=2017&

Análise de auditoria:

O Despacho da Presidência é de 22/10/2019. A Ata mencionada na manifestação da SETIC se refere a uma reunião ocorrida em 16/5/2019, portanto, anterior. Nessa reunião, fora aprovada a proposta de revisão dos indicadores e metas do objetivo 3 (PETI 2015-2020) "implementar a gestão de riscos de TI".

Recomendação:

Não há.

Prazo:

Não se aplica.

Constatação nº 2

Descrição sumária:

Ausência de plano de ação contendo cronograma para mapeamento dos riscos de processos.

Determinação 2.1:

2.1 Elaborar Plano de Ação e cronograma para o mapeamento de riscos dos processos essenciais de TIC.

Providências adotadas:

Manifestação da SETIC:

Embora não tenha sido lavrado um documento chamado plano de ação, tal planejamento é o próprio estabelecimento dos indicadores, que englobam escopo e metas com prazo para cumprimento.

O plano de ação foi executado, cujo resultado é evidenciado pelo Doc. 36, que é o plano de tratamento de riscos, bem como indicadores correspondentes foram atualizados.

Ato contínuo às definições decorrentes da recomendação 1.1, foram realizadas análise de riscos em 2019 e 2020. Nas reuniões de avaliação da estratégia esses indicadores foram apresentados ao Comitê de Governança de TIC e publicados no site institucional, conforme indicado abaixo.

- REUNIÃO DE ANÁLISE DA ESTRATÉGIA DE TIC - 04/12/2019

https://www.trt7.jus.br/files/institucional/governanca_ti/planejamento_estrategico/RAE-2015-2020/Raetic-04-12-2019.PDF

Na página 22 (painel de bordo) temos a apresentação dos indicadores relativos ao objeto 3, junto aos demais.

Nas páginas 40 e 41 a visualização detalhada dos indicadores.

- REUNIÃO DE ANÁLISE DA ESTRATÉGIA DE TIC - 07/12/2020

https://www.trt7.jus.br/files/institucional/governanca_ti/planejamento_estrategico/RAE-2015-2020/ApresentacaoRAE-07-12-2020.pdf

Na página 8 (painel de bordo) temos a apresentação dos indicadores relativos ao objeto 3, junto aos demais.

Nas páginas 14 e 15 a visualização detalhada dos indicadores.

Na página 31 temos a visualização dos sistemas alvos para a gestão de riscos.

Análise de auditoria:

A Determinação trata do *mapeamento de riscos de processos essenciais de TIC* e pode ser considerada atendida, tendo em vista a apresentação dos indicadores nos documentos de registro das reuniões de análise da estratégia de TIC**.** As reuniões aludidas na manifestação da unidade auditada ocorreram em dezembro de 2019 e em dezembro de 2020, ou seja, após o Despacho da Presidência (de 22/10/2019). O Doc. 36 se refere ao Plano de Tratamento de Riscos de TIC.

Recomendação:

Não há.

Prazo:

Não se aplica.

Determinação 2.2:

2.2 Definir ferramenta para apoiar a implantação da gestão de riscos na TIC.

Providências adotadas:

Manifestação da SETIC:

Desde 2019, quando iniciamos a gestão de riscos dos sistemas considerados críticos, foram utilizados documentos de texto e planilhas eletrônicas na plataforma de colaboração do TRT7, atualmente Google, pela simplicidade e facilidade de uso.

Evidência:

-Plano de tratamento de riscos 21/22

https://docs.google.com/document/d/1qPgtaTKQDDF4O54Esg5n668L1401LeFQpEUWEFmoSuU/edit?usp=sharing

-Planilha com a análise de risco SIGEP 2021

https://docs.google.com/spreadsheets/d/10d_mOuvflj3tTKUzfA2v7MFo7MZuSpUVfBH84RA5JoQ/edit?usp=sharing

Agora em 2022, tendo o TRT7, ao menos na área de segurança da informação, ter realizado 1 ciclo completo de análise risco, que contemplou a identificação dos ativos de TIC, das vulnerabilidades, das ameaças, da determinação do nível de risco inerente, seleção do tratamento, avaliação dos controles existes e implementados neste período, além de cálculo do risco residual, entendeu-se que há maturidade para adoção de uma ferramenta capaz de otimizar tal processo e agregar novos controles, assim a ferramenta definitiva está em fase de licitação.

Evidência:

PROAD 1770/2021 - Pregão realizado em 20/1/2022. Neste momento (25/01) a licitação está em fase de análise da documentação técnica da ferramenta ofertada pela licitante vencedora da etapa de lances.

Análise de auditoria:

A Determinação encontra-se atendida, tendo em vista a definição da ferramenta de apoio na implantação da gestão de riscos cuja aquisição tramita presentemente na fase licitatória.

O desempenho e a efetividade dessa ferramenta serão apurados em futura ação de auditoria.

Recomendação:

Não há.

Prazo:

Não se aplica.

Constatação nº 3

Descrição sumária:

Ausência de Plano de Continuidade de Serviços Essenciais de TI ou Gestão de Continuidade de TIC (Ato TRT7 n. 02/2017).

Determinação 3.1:

3.1 Concluir os testes do plano de contingência do PJe, o que demanda a solução, por parte da Administração, da questão da necessidade da realização do trabalho em dias não úteis.

Providências adotadas:

Manifestação da SETIC:

Elencamos como providências no contexto dos testes de contingência:

1) Edição do Ato TRT7 nº 23/2020, que atualizou o Ato TRT7 nº 02/2017 que estabelece a Norma Complementar, com as diretrizes para o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações, para inclusão dos parâmetros de ponto (RPO) e tempo de recuperação (RTO), que estabelecem as expectativas de negócio para tolerância a perda de dados e o tempo necessário para executar o sistema no ambiente de contingência, respectivamente.
PROAD: 8353/2019
ATOS:
https://www.trt7.jus.br/files/atos_normativos/atos_presidencia/2020/BD_ATO_PRESI_23-2020.pdf

https://www.trt7.jus.br/files/atos_normativos/atos_presidencia/2017/BD_ATO_PRESI_02-2017.pdf

2) Finalizamos, com sucesso, em 21/05/2021, um teste de restauração do banco de dados do PJe a partir do backup diferencial em fita, que constitui a principal estratégia para viabilizar a execução do plano de continuidade operacional do PJe em caso de desastre no data center principal. Neste período, como não envolveu a execução da totalidade do PCO, não foi necessário paralisar o ambiente principal, assim não houve necessidade de atuação fora do horário de expediente. As ações encontram-se documentadas no chamado EL-1834[1] e nos chamados relacionados.
3) Na reunião conjunta do Núcleo de Apoio à Gestão de TIC com a Divisão de Infraestrutura de TIC ocorrida em 07/12/2021 (doc. 49 do PROAD 864/2021) deliberou-se por priorizar e retomar as atividades, a partir de 24/01/2022, para preparação e execução novo teste de contingência, neste caso de todas as etapas. Assim, será oportunamente encaminhado à Administração superior o pedido de autorização para trabalho fora do horário de expediente (ainda neste primeiro semestre).
4) Atualizamos em dezembro de 2021 [2] as licenças da solução de virtualização de servidores (VMware). Com exceção dos servidores de banco de dados e de backup, todos os demais são virtualizados utilizando essa tecnologia. Tal infraestrutura, atualmente, é essencial para a realização dos testes de contingência, bem como para a entrada em produção do PJe no ambiente de contingência (instalado no Fórum Autran Nunes) em casa de pane severa no ambiente principal (sala-cofre localizada do Anexo II do complexo sede).

[1] Identificação no sistema de chamados (Jira) internamente utilizado pela SETIC.
[2] Contrato TRT7 nº 43/2021

Análise de auditoria:

Determinação ainda a ser atendida, de acordo com a informação da unidade auditada quanto à retomada das atividades com vistas à realização de um teste englobando todas as etapas do PCO (Plano de Continuidade Operacional) ainda no mês de janeiro de 2022.

Recomendação:

Manter a Determinação.

Prazo:

60 dias

Determinação 3.2:

3.2 Elaborar Plano de Recuperação de Desastres para conclusão da Gestão de Continuidade de TIC, pelo menos para o PJe.

Providências adotadas:

Manifestação da SETIC:

Para evitar qualquer interpretação não alinhada entre os servidores da SETIC ou qualquer pessoa envolvida nos processos de auditoria e gestão é oportuno reforçar que um Plano de Recuperação de Desastres (PRD) foca nos ativos, ou seja, nos elementos que garantem a infraestrutura básica (tais como no-breaks, links de comunicação de dados), software (de virtualização, por exemplo) e nos dados (ativos de informação), já o

Plano de Continuidade Operacional (PCO) tem como foco os processos, no caso do TRT7, os processos de negócio ofertados pelo sistema PJe.

Em que pese a importância do PRD, por questões de capacidade operacional, o foco de atuação até o presente momento foi o PCO, essencialmente porque o TRT7 dispõe de um ambiente de contingência no Fórum Autran Nunes capaz de rodar os processos do PJe por muito tempo (ou até mesmo definitivamente) em caso de danos significativos e de longo prazo no ambiente principal. Desta forma, os procedimentos de recuperação podem seguir um fluxo normal de planejamento, aquisições por licitação (quando for o caso), implementação e testes. Todos os ativos de TIC, do tipo software, envolvidos no ambiente principal, referente à sustentação do PJe, estão em garantia e/ou possuem suporte, assim, em muitos casos o PRD destes ativos é simplesmente reinstalação. Todos os ativos de TIC, do tipo hardware, envolvidos no ambiente principal, referente à sustentação do PJe, estão em garantia e/ou possuem suporte, assim, em muitos casos o PRD destes ativos é simplesmente acionar a garantia ou disparar procedimento de compra quando for o caso. Quanto aos ativos de informação, todos são objetos de backup, segundo a política vigente, portanto o PRD é restaurar os dados por meio das cópias de segurança do PJe (disponíveis no Fórum Autran Nunes).
Em síntese, os PRD´s dos ativos de TIC do PJe não foram formalmente registrados em documento com este propósito, mas as ações tipicamente necessárias estão sendo executadas.

De qualquer forma, dentro do contexto da continuidade de implementação do plano de contingência, neste ciclo do PDTIC 2021/2022, os PRD´s dos ativos que sustentam o PJe serão formalizados.

Análise de auditoria:

Conforme a manifestação da unidade auditada, não há um PRD elaborado. Portanto, a Determinação não foi atendida.

Recomendação:

Manter a Determinação.

Prazo:

60 dias

Determinação 3.3:

3.3 Apresentar cronograma para elaboração de Planos de Contingência para os demais serviços essenciais, além do PJe.

Providências adotadas:

Manifestação da SETIC:

Na reunião do Comitê de Governança de TIC de 29/08/2018 [1], restou definido que seria construído um plano de contingência operacional apenas para o PJe, o que foi realizado, conforme já informado por ocasião da auditoria.

No PDTIC vigente, período 2021/2022 o Comitê de Governança de TIC deliberou por criar o plano de continuidade operacional para os seguintes sistemas: PJe e Acesso ao SIAFI [2].

[1] Ata reunião do Comitê de Governança de TIC de 29/08/2018 (doc. 19 do PROAD 6057/2017): https://proad.trt7.jus.br/proad/pages/pdfprint/DOCUMENTO%20-%20Ata%20do%20CGTIC%20de%2029-08-2018.pdf?nrSequencial=19&numeroProtocolo=6057&numeroAno=2017&

[2] Anexo VII do PDTIC 2021/2022, ver página 17

https://www.trt7.jus.br/files/institucional/governanca_ti/plano_diretor/2021/AnexoVII-PDTIC-2021-2022-AnaliseDeDesempenho.pdf

Análise de auditoria:

A Ata mencionada na manifestação acima se refere a reunião do CGTIC ocorrida em 29/8/2018, antes, portanto, do Despacho da Presidência com a Determinação em tela, datado de 22/10/2019.

Com efeito, em que pese o Anexo VII do PDTIC 2021/2022 apresentado, a Determinação não se encontra atendida, haja vista a inexistência de cronograma para elaboração de Planos de Contingência para os demais serviços essenciais, além do PJe.

Recomendação:

Manter a Determinação.

Prazo:

30 dias

Constatação nº 4

Descrição sumária:

Descumprimento de periodicidade de reunião conjunta do CGSI (Comitê Gestor de Segurança da Informação) com a CSI (Comissão de Segurança Institucional).

Determinação 4.1:

4.1 Promover reuniões conjuntas periódicas do CGSI e da CSI, conforme definido na Res. TRT7 nº 278/2017, ou avaliar a conveniência de alterar a norma nesse aspecto.

Providências adotadas:

Manifestação da SETIC:
A política de segurança da informação foi revista em 2020 e o aspecto objeto da determinação 4.1 foi revisto, conforme artigo reproduzido abaixo.

Resolução Normativa nº 14/2020

> Art. 13. O CGSI se reunirá ordinariamente pelo menos duas vezes por ano, e de forma extraordinária, quando se fizer necessário.
>
> § 1º As deliberações do CGSI serão consignadas em ata e encaminhadas ao Comitê de Governança de TIC para aprovação.

§ 2º O CGSI poderá convidar para participar das reuniões, sem direito a voto, representantes de outras unidades, órgãos, entidades públicas ou organizações da sociedade civil, a fim de colaborar na execução dos trabalhos a serem realizados.

https://www.trt7.jus.br/files/atos_normativos/resolucoes/2020/BDRESOLUONORMATIVATRT7N14-2020.pdf

As atas do Comitê Gestor de Segurança da Informação estão registradas no PROAD 954/2021, entretanto, em razão da matéria, por decisão do referido Comitê, o conteúdo das reuniões não são divulgados, pois podem expor vulnerabilidades e fraquezas do Tribunal, podendo ser exploradas por pessoas mal intencionadas, motivo pelo qual os documentos do supracitado PROAD estão marcadas para acesso restrito.

Análise de auditoria:

A Resolução Normativa TRT7 n. 14/2020 atende ao propósito da Determinação quanto à revisão da periodicidade e da participação das reuniões do CGSI.

Evidencia-se o cumprimento do novo dispositivo ao longo de 2021. O PROAD nº 954/2021 traz as Atas das reuniões do Comitê Gestor de Segurança da Informação.

Recomendação:

Não há.

Prazo:

Não se aplica.

Constatação nº 5

Descrição sumária:

Falta de ação institucional de sensibilização, conscientização e capacitação em segurança da informação de TIC.

Determinação 5.1:

5.1 Estabelecer plano de ação para a sensibilização, conscientização e capacitação, referentes à segurança da informação, dos usuários no âmbito do TRT7.

Providências adotadas:

Manifestação da SETIC / NGTIC:
O NGTIC juntamente com a Ejud realizaram, nos exercícios de 2020/2021, os seguintes cursos com intuito de capacitar magistrados e servidores em Segurança da Informação - SI.
.LGPD no Poder Judiciário

https://www.trt7.jus.br/escolajudicial/index.php?option=com_content&view=article&id=1139&Itemid=181

.Lei geral de Proteção de Dados

https://www.trt7.jus.br/escolajudicial/index.php?option=com_content&view=article&id=1139&Itemid=181

-Segurança da Informação para Servidores - Turma 1

https://www.trt7.jus.br/escolajudicial/index.php?option=com_content&view=article&id=1163&Itemid=181
-Segurança da Informação para Servidores - Turma 2

https://www.trt7.jus.br/escolajudicial/index.php?option=com_content&view=article&id=1184&Itemid=181cle&id=1163&Itemid=181

Por meio de notícias na intranet/extranet foram fornecidas dicas importantes para sensibilizar e conscientizar magistrados e servidores em SI. Segue relação de notícias (necessário estar autenticado):

-Segurança da informação: conheça dicas importantes para proteger seus dados e não cair em golpes virtuais - 20/4/2020

https://extranet.trt7.jus.br/index.php?option=com_content&view=article&id=4152:seguranca-da-informacao-conheca-dicas-importantes-para-proteger-seus-dados-e-nao-cair-em-golpes-virtuais&catid=8&Itemid=117

-Segurança da Informação: Gabinete de Segurança da Informação do TRT/CE faz alerta contra site fraudulento - 02/06/2021

https://extranet.trt7.jus.br/index.php?option=com_content&view=article&id=4640:gabinete-de-seguranca-da-informacao-do-trt-ce-faz-alerta-contra-site-fraudulento&catid=8&Itemid=117

-Alerta de segurança: cuidado com e-mail falso -10/05/2021

https://extranet.trt7.jus.br/index.php?option=com_content&view=article&id=4610:alerta-de-seguranca-cuidado-com-e-mail-falso&catid=8&Itemid=117

-Alerta de golpe: TRT/CE não envia boletos solicitando pagamento - 15/06/2021

https://extranet.trt7.jus.br/index.php?option=com_content&view=article&id=4653:alerta-de-golpe-trt-ce-nao-envia-boletos-solicitando-pagamento&catid=8&Itemid=117

Análise de auditoria:

As ações listadas pela SETIC, relativas à sensibilização, conscientização e capacitação dos servidores e magistrados, evidenciam o esforço deste Tribunal em aprimorar a segurança da informação. No entanto, deve ser observada a necessidade de ações sistemáticas, nos anos vindouros, baseadas em planejamento efetivo e coordenado, para o atendimento do propósito da Determinação.

Recomendação:

Não há.

Prazo:

Não se aplica.

Constatação nº 6

Descrição sumária:

Não cumprimento integral pelo NGTIC (Núcleo de Apoio à Gestão de TIC e Segurança da Informação) e pela ETIR (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais) de suas atribuições, no que concerne a esse ponto de controle.

Determinação 6.1:

6.1 Adotar providências para o integral cumprimento das atribuições do NGTIC e da ETIR, conforme o Ato nº 152/2018 (tratamento de incidentes de segurança).

Providências adotadas:

Manifestação da SETIC:
O Núcleo de Apoio a Gestão de TIC e Segurança da Informação vem desempenhando as atribuições previstas no Ato nº 152/2018, em especial a implantação da gestão de incidentes de segurança e a conscientização Institucional em SI, conforme informação descrita na manifestação da determinação 5.1.
Como evidência seguem atuações recentes do NGTIC e da ETIR em incidentes de Segurança:

Data do incidente	Atuações recentes
29/06/2021	PROAD 3736/2021 - Incidente 24893 - Ataque ao site Institucional
15/06/2021	PROAD 3729/2021 - Incidente 24759 - Boleto falso em nome do TRT7

Há ainda diversas atuações do NGTIC relacionadas diretamente com a prevenção de incidentes de segurança da informação, em constante contato com o Comitê Gestor de Segurança da Informação, tais atuações podem ser constatadas por meio dos documentos presentes no PROAD 954/2021, tais como documentos 19, 20, 21, 23 e 24;

Análise de auditoria:

A unidade auditada aduz evidências quanto ao cumprimento do Ato nº 152/2018 (tratamento de incidentes de segurança), contemplando as ações pertinentes. Oportuno enfatizar que a tempestividade dessas ações é fundamental para a sua efetividade, assim como para a prevenção e mitigação dos danos em eventuais tentativas de violação dos sistemas de TIC.

Recomendação:

Não há.

Prazo:

Não se aplica.

Constatação nº 7

Descrição sumária:

Falta de divulgação quanto ao procedimento para registro de incidentes de segurança de TIC.

Determinação 7.1:

7.1 Estabelecer plano de ação (incluindo cronograma) para as implementações pendentes ao cumprimento integral do que dispõe o Ato nº 152/2018, incluindo ações para que os usuários de TIC possam conhecer os canais de registro e operacionalizá-los adequadamente.

Providências adotadas:

Manifestação da SETIC/NGTIC:

A implementação que estava pendente no momento da auditoria foi executada ainda em 2019, conforme detalhado abaixo.

-Foi criado em **abril de 2019**, no sistema de registros de chamados de TIC do TRT7, um canal específico para o registro de incidentes de segurança da informação, conforme figura abaixo:

-Em 26/04/2019 foi publicada a notícia "Incidentes de Segurança da Informação: saiba como identificar e prevenir".

Em 16/9/2019 a notícia acerca do canal para registro de ocorrência ou suspeita de ocorrência de incidentes de segurança foi republicada na intranet/extranet para reforçar a necessidade de uso do canal.
https://extranet.trt7.jus.br/index.php?option=com_content&view=article&id=3782:sti-explica-como-identificar-e-prevenir-incidente-de-seguranca-da-informacao&catid=8&Itemid=117

Adicionalmente temos no sistema de chamados um vídeo explicativo de como registrar chamados. Este vídeo encontra-se disponível na Intranet, dentro da página inicial da Central de serviços de TI.

https://intranet.trt7.jus.br/files/publicacoes/videos/assyst_02_abrir_chamado.mp4

Análise de auditoria:

As providências adotadas são importantes para tornar o controle e o tratamento de incidentes mais eficazes. Nesse sentido, a Determinação está atendida. No entanto, cabe reforçar o caráter dinâmico dessas ações, a serem sistematicamente revistas, atualizadas e aprimoradas para assegurar a continuidade operacional dos recursos de TIC, indispensáveis na cadeia processual desenvolvida neste Tribunal.

Recomendação:

Não há.

Prazo:

Não se aplica.

Informação nº 2

Descrição sumária:

Normativos internos em desacordo com a estrutura organizacional do TRT7 (item 9, 10 e 11 da TRT7.SCI.SCGAP nº 01/2019).

Determinação:

Apresentar minuta de normativos necessária aos ajustes na Resolução TRT7 nº 278/2017 e no Ato TRT7 Nº 106/2018, conforme sugestão constante da Informação nº 2 (*do Relatório de Auditoria*).

Providências adotadas:

Manifestação da SETIC:

Em 22/6/2020 foi publicada a RESOLUÇÃO NORMATIVA TRT7 Nº 14/2020 - com as revisões e ajustes necessários à POSIC em substituição a Resolução TRT7 nº 278/2017.

Foram publicados a RESOLUÇÃO NORMATIVA TRT7 Nº 11/2021 e o ATO TRT7.GP. Nº 71/2021 referente à Política e ao plano de Gestão de Riscos do TRT7 que abrangerá todas as unidades, inclusive a SETIC.

Assim, o Ato TRT7 nº 106/2018 será revisto para alinhamento aos novos normativos. A minuta da revisão está pronta e será submetida à apreciação superior nos próximos dias.
Análise de auditoria: Determinação atendida, tendo em vista a documentação apresentada.
Recomendação: Não há.
Prazo: Não se aplica.

III. CONCLUSÃO

No Relatório de Providências, foram listadas as 10 determinações, no âmbito de 7 constatações, além de uma determinação decorrente de informação constante do Relatório de Auditoria, para manifestação da unidade auditada.

Nesta fase, pela análise das providências em face das determinações exaradas, considera-se que 8 determinações foram ou estão sendo satisfatoriamente atendidas. Remanescem, portanto, 3 determinações para efetivas providências de controle sistemático nas contratações futuras:

Determinação 3.1: *Concluir os testes do plano de contingência do PJe, o que demanda a solução, por parte da Administração, da questão da necessidade da realização do trabalho em dias não úteis*.

Novo prazo sugerido para o cumprimento: 60 dias

Determinação 3.2: *Elaborar Plano de Recuperação de Desastres para conclusão da Gestão de Continuidade de TIC, pelo menos para o PJe*.

Novo prazo sugerido para o cumprimento: 60 dias

Determinação 3.3: *Apresentar cronograma para elaboração de Planos de Contingência para os demais serviços essenciais, além do PJe*.

Novo prazo sugerido para o cumprimento: 30 dias

Responsáveis pela Elaboração:

assinado eletronicamente
Anísio de Sousa Meneses Filho
Analista Judiciário

assinado eletronicamente
Rossini de Sousa Maciel
Coordenador de Serviço da SAGAP

Data: 24/3/2022

Responsável pela Coordenação: *assinado eletronicamente* **Rossini de Sousa Maciel** Coordenador de Serviço da SAGAP
Data: 31/03/2022

Revisão:	**Aprovação:**
assinado eletronicamente **Michel Cavalcante Pinto** Secretária de Auditoria Interna	*assinado eletronicamente* **Michel Cavalcante Pinto** Secretária de Auditoria Interna
Data: 31/03/2022	**Data: 31/03/2022**