



## RELATÓRIO SINTÉTICO

Auditoria no processo de gestão de riscos de tecnologia da informação e comunicações no TRT 24ª Região

COORDENADORIA DE AUDITORIA INTERNA  
RELATÓRIO Nº 2/2020 – PROCESSO Nº 20170/2019  
JULHO DE 2020

# RELATÓRIO SINTÉTICO

---

## OBJETIVO

Este trabalho teve como escopo verificar e avaliar a efetiva adoção e execução dos subprocessos do Processo “Gerenciar Riscos de TIC”, bem como sua adequação às melhores práticas vigentes.

---

## AVALIAÇÃO DO GERENCIAMENTO DE RISCOS

Por meio da análise preliminar do processo de trabalho objeto desta auditoria, observou-se que a lista geral dos ativos críticos e processos críticos não distingue ativos primários e de suporte, razão pela qual foi recomendado que a administração avalie a possibilidade de revisar e reeditar a PORTARIA TRT/GP/DG Nº 61/2020, que revogou a Portaria TRT/GP/DGCA Nº 176/2016 (Política de Segurança da Informação) para contemplar a classificação de ativos em críticos e não críticos (ou de suporte), conforme preceitua a Norma ABNT ISO-NBR-27005/2008 - Gestão de Riscos de TI – no Anexo B.

---

## ACHADOS DE AUDITORIA E RECOMENDAÇÕES

### 1) AUSÊNCIA DE DESIGNAÇÃO FORMAL DOS RESPONSÁVEIS PELOS ATIVOS DE TIC E SUAS DEVIDAS ATRIBUIÇÕES

#### RECOMENDAÇÃO

- Sejam designados formalmente os responsáveis pelos ativos de TIC, estabelecendo seus papéis e responsabilidades no gerenciamento de riscos de TIC responsável.

### 2) MANUTENÇÃO DE RESPONSÁVEIS POR ATIVOS MESMO APÓS O SEU DESLIGAMENTO

#### RECOMENDAÇÃO

- Adote procedimentos de controle para, doravante, manter atualizada a gestão dos ativos e respectivos responsáveis, com vistas a evitar responsabilização indevida por qualquer incidente de TIC a servidor do quadro ou já desligado, bem como possíveis fraudes.

## CONCLUSÃO

Nos últimos anos a Justiça do Trabalho, visando padronizar e otimizar processos de trabalho, vem adotando soluções padronizadas de gestão de riscos de TIC. A principal ferramenta utilizada até o momento é o Risk Manager. Porém, segundo informações da Coordenadora da CTIC, esse software foi descontinuado e, no momento, está em curso o processo de contratação, em nível nacional, de um novo software para substituí-lo. Em função desse momento de transição, há que se considerar que para que essa nova solução seja efetivada nos Tribunais, deve-se levar em conta todo o tempo de contratação, treinamento e implantação para sua utilização, o que pressupõe a necessidade de elaboração de um plano de ação para sua consecução.

Efetuada as análises propostas, constatou-se que a classificação dos ativos para fins de gerenciamento de riscos deve ser efetuada sob os preceitos do Anexo B da Norma ABNT ISO-NBR-27005/2008 - Gestão de

Riscos de TI. Essa atividade pressupõe uma revisão, para adequação a essa Norma ABNT, da Portaria TRT/GP/DG nº 61/2020 (Política de Segurança da Informação) e TRT/GP/DG Nº 070/2019 (Política de Gestão de Riscos de Tecnologia de Informação e Comunicações).

A revisão, que se propõe, nas portarias acima descritas, deve designar os responsáveis por cada ativo e suas devidas atribuições quanto à sua produção, desenvolvimento, manutenção, utilização, integridade e valoração, e, ainda, se o responsável por cada ativo é a chefia do setor onde se localiza o ativo, se é o setor de infraestrutura da CTIC, etc. E isso deve estar refletido nos controles do software a ser adquirido.