Tribunal Regional do Trabalho
24ª Região | Mato Grosso do Sul

RELATÓRIO SINTÉTICO

Auditoria no processo de segurança da informação com ênfase na política e processos de controle de acessos

COORDENADORIA DE AUDITORIA INTERNA
RELATÓRIO Nº 1/2020 – PROCESSO Nº 6773/2018
FEVEREIRO DE 2020

RELATÓRIO SINTÉTICO

OBJETIVO

Este trabalho teve como escopo verificar e avaliar a efetiva adoção de subprocessos do Processo DSS05 do COBIT 5 - Gerir Serviços de Segurança e também a aderência à norma ABNT ISO 27002.

AVALIAÇÃO DO GERENCIAMENTO DE RISCOS

Foi identificada situação de risco causada pela ausência de segregação de funções no processamento da folha de pagamento.

ACHADOS DE AUDITORIA E RECOMENDAÇÕES

1) INSUFICIÊNCIA DE REGISTROS PARA AS OPERAÇÕES DOS USUÁRIOS COM DIREITOS DE ADMINISTRADOR DO SISTEMA (DATA BASE ADMINISTRATOR - DBA)

RECOMENDAÇÕES

- Implante perfis individuais de acesso ao banco de dados pelos administradores (DBA's) visando evitar a utilização de senha única.
- Adote, doravante, na definição das Regras do Negócio de cada sistema, regras detalhadas para trilhas de auditoria (log's), para todos os acessos ao Banco Oracle por usuários com privilégio de administrador, onde fique registrado, além da data e hora do acesso, também a íntegra dos comandos executados.

2) PERMANÊNCIA DE DIREITO DE ACESSO A SISTEMAS POR COLABORADOR JÁ DESLIGADO DO TRT

RECOMENDAÇÕES

- Determine a periodicidade necessária e efetue levantamento para verificar a existência de ex-colaboradores que continuam com direito de acesso a sistemas, efetuando a sua exclusão, caso constatadas situações positivas.
- Estabeleça controles internos a fim de assegurar que o desligamento de colaboradores seja comunicado pelos gestores de contratos à Coordenadoria de Gestão de Pessoas imediatamente após o término do vínculo.

3) FALTA DE ASSINATURA DO TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

RECOMENDAÇÕES

A recomendação efetuada no relatório preliminar foi atendida pela administração.

4) INSUFICIÊNCIA DE INFORMAÇÕES DE CONTROLE NAS TRILHAS DE AUDITORIA

RECOMENDAÇÕES

- Doravante, na definição da arquitetura de cada sistema, registre clara e detalhadamente todos os campos passíveis de alteração que constarão das trilhas de auditoria (log's) de cada sistema, gravando

os conteúdos anteriores e posteriores a movimentações que causem alterações nos mesmos. Convém que para essas definições seja consultada a Coordenadoria de Auditoria Interna.

5) AUSÊNCIA DE HISTÓRICO NA TABELA "REQUISIÇÕES" DO SISTEMA SCMP, QUANTO A EXCLUSÕES E RETORNO DE MATERIAL AO ALMOXARIFADO

RECOMENDAÇÕES

- Implante no sistema SCMP as funções "Estorno de Requisição" e "Devolução ao Almoxarifado" para permitir a alteração na composição dos itens ou quantitativos nas requisições demandadas pelo Setor de Almoxarifado, ocasionada por erro em seu lançamento e possíveis devoluções ao almoxarifado.
- Encaminhe, como sugestão, as recomendações "a", "b", "e" e "f" do Relatório de Auditoria nº 1/2020 ao Comitê Gestor dos sistemas "nacionais" para considerá-las nas definições de regras de negócio nos sistemas em elaboração/manutenção, como os sistemas "SCMP" e "FOLHAWEB", os quais são oriundos deste TRT.

CONCLUSÃO

Nos últimos anos a Justiça do Trabalho, visando padronizar e otimizar procedimentos de trabalho, vem desenvolvendo sistemas informatizados com status de "sistema nacional", que serão implantados em todos os regionais. Este Regional atualmente contribui com essa iniciativa liderando três projetos nacionais: os sistemas FOLHAWEB (Folha de Pagamento), SCMP (Material e Patrimônio) e Escola Judicial.

Nesta auditoria optou-se por limitar o escopo a verificar se as práticas de segurança da informação relativas a controle de acesso adotadas no TRT estão de acordo com a norma ISO-27002 e o habilitador "Informação" do Cobit 5 e, também, se no desenvolvimento de sistemas informatizados é observado o princípio da segregação de funções, no qual fique claramente bem detalhado o que cada ator pode fazer em cada função do sistema.

Para testar essas duas indagações do escopo, escolheu-se esses dois sistemas (FOLHAWEB e SCMP) no intuito de contribuir com a depuração dos mesmos, visto que ambos têm o status de "nacionais".

Efetuadas as análises propostas, constatou-se que as principais causas motivadoras da ocorrência dos achados desta auditoria recaem, em primeira análise, na inobservância da Norma ABNT ISO 27002, no que tange a segurança da informação, e do manual Boas Práticas em Segurança da Informação – 4ª edição – TCU – 2012. E, em segunda análise, na escassez de pessoal especializado na infraestrutura necessária.

Dentre as justificativas apresentadas pela área auditada, há que se considerar o agravamento da situação pela diminuição da força de trabalho consequente do aumento da inativação de servidores lotados nas Coordenadorias envolvidas, sem que haja reposição da correspondente força de trabalho, dificultando a adoção de procedimentos relevantes de controle, como a segregação de função para maior segurança e também a atualização dos procedimentos de segurança nos acessos unívocos aos bancos de dados.