



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO



RELATÓRIO DE AUDITORIA		RA – SACI – SMAAAG 004/2017	
Referência/Assunto:	Auditoria da Gestão da Segurança da Informação		
Processo nº:	50.070/2017		
Unidade Auditada:	Secretaria de Tecnologia da Informação		
Equipe de Auditoria:	Avany Gomes da Cunha Cavalcanti (líder) Sílvio Ramos da Silva		

Introdução

Trata-se de relatório de auditoria realizada em cumprimento ao Plano Anual de Auditoria – PAA 2017, aprovado pela Presidência deste Tribunal (Protocolo TRT6 nº 5.960/2016), e que teve como objetivo verificar os níveis de segurança referentes à disponibilidade, confiabilidade, integridade e autenticidade das informações de Tecnologia da Informação.

Verifica-se uma preocupação crescente da Administração Pública com a temática Segurança da Informação, que possui como principais normativos o Decreto nº 3505/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, e alterações posteriores, e a Instrução Normativa nº 01 do Gabinete de Segurança Institucional/PR que estabelece orientações para a Gestão de Segurança da Informação e Comunicações para implementação pelos órgãos e entidades da Administração Pública Federal.

No âmbito do Poder Judiciário, tem-se a Resolução do Conselho Nacional de Justiça (CNJ) nº 211/2015, que ao instituir a Estratégia Nacional de TIC do Poder Judiciário (2015/2020), assegura o dever de elaborar e aplicar política, gestão e processo de segurança da informação em todos os níveis da instituição, tema introduzido por meio da Resolução CNJ nº 90/2009, que motivou, em julho/2012, o estabelecimento das primeiras diretrizes para a implantação da Gestão de Segurança da Informação (GSI) para adoção pelos órgãos do Judiciário Brasileiro.

A nível institucional, destaque-se a existência do Programa de Consolidação da Cultura Organizacional em Segurança da Informação que integra o Projeto nº 11 do Planejamento Estratégico do TRT6 (2015-2020), o que reflete o seu alinhamento com as diretrizes do Conselho Nacional de Justiça.

A matéria se encontra disciplinada, neste Regional, por meio da Resolução Administrativa TRT nº 30/2009 e dos Atos-TRT-GP números 314/2013, 408/2013, 153/2014 e 198/2016, que constituem nos critérios adotados na presente auditoria. Considerou-se, ainda, o Código de Práticas para a Gestão de Segurança da Informação - ABNT NBR ISO/IEC 27002:2005, apenas no que concerne a boas práticas de 2005 que permanecem vigentes, tendo em vista a atualização do normativo em 2013. Destaque-se que o referido manual é adotado pelo Tribunal de Contas da União como norma técnica de auditoria de segurança da informação, consoante publicação "Boas práticas em segurança da informação" (4ª versão, 2012) daquela Corte de Contas, e que serviu de referência para a elaboração do documento de Política de Segurança da Informação deste TRT6.

Assinatura



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

A execução do trabalho de auditoria aconteceu no período de 30/01/2017 a 10/08/2017, ultrapassando o período inicialmente estabelecido em decorrência de ajustes que se revelaram necessários na amplitude da auditoria.

Como técnicas de auditoria foram utilizadas a indagação escrita, o exame documental, entrevista e a inspeção *in loco*.

A fim de verificar o nível de aderência às normas estabelecidas, basearam-se os exames pelas seguintes questões de auditoria:

1. A Política de Segurança da Informação (PSI) do TRT6, aprovada pelo Ato – TRT - nº 314/2013, contempla as diretrizes e os princípios que norteiam a gestão de segurança da informação e seus respectivos responsáveis?
2. O TRT6 promove ações permanentes de divulgação da Política e disseminação da cultura em segurança da informação em toda a organização?
3. As normas internas que disciplinam o controle de acesso, tratamento de incidentes, gestão de ativos e gestão de riscos de segurança da informação atendem às boas práticas vigentes e estão efetivamente em uso?
4. Há um Plano de Continuidade do Negócio formalmente estabelecido?

Para início dos trabalhos, expediu-se o Comunicado de Auditoria CA-SACI-SMAAAG nº 001/2017 (Protocolo TRT6 nº 50070/2017) dando ciência da auditoria à Secretaria de Tecnologia da Informação, em cumprimento à Resolução nº 171/2013 do Conselho Nacional de Justiça.

Com a finalidade de subsidiar a auditoria, encaminhou-se à unidade auditada a Requisição de Documentos e Informações, RDI-SACI-SMAAAG nº 005/2017, em 07/04/2017, por meio eletrônico, contendo questionário de auditoria que abordou os seguintes temas: Política de Segurança da Informação – Documento; Divulgação e Disseminação da Cultura em Segurança da Informação; Controle de Acesso; Tratamento de Incidentes; Gestão de Ativos; Gestão de Riscos de Segurança da Informação e Plano de Continuidade do Negócio.

A Secretaria de Tecnologia da Informação teceu o pronunciamento em 12/05/2017, inclusive com envio eletrônico da documentação comprobatória respectiva, e ainda, em 28/06/2017 e 13/07/2017, por ocasião das visitas à Seção de Gestão da Segurança da Informação da Divisão de Gestão e Governança de TI daquela Secretaria.

Considera-se que as informações prestadas pela unidades foram elucidativas.

Cumprir informar que os pronunciamentos e documentos recebidos encontram-se disponíveis na pasta I:\2a Instancia\Pres\SACI\trib.saci\ AUDITORIAS_CNJ 171\AUDITORIAS 2017\GESTAO DA SEGURANCA DA INFORMACAO DE TI_PAA 2017.

Achados de Auditoria

Concluída a análise preliminar, os possíveis achados de auditoria foram noticiados à Secretaria de Tecnologia da Informação por meio da RDI SACI nº 014/2017 (Protocolo nº 51.853/2017), para ciência e manifestação, que, por sua vez, remeteu os esclarecimentos adicionais em 1º/08/2017 (Ofício TRT6-STI nº 046/2017).



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

Apresenta-se, a seguir, a consolidação dos achados de auditoria, os esclarecimentos prestados pela unidade auditada, bem como pelos responsáveis de unidades envolvidas, e as considerações da equipe de auditoria:

Achado 1: Política de controle de acesso parcialmente estruturada.

Nos exames realizados constatou-se que inexistiu um procedimento formal de registro e de cancelamento de usuário para garantir e revogar acessos nos sistemas de informações e serviços.

Identificou-se, ainda, que não há estabelecimento de procedimentos de controle de atualização de privilégio de acesso aos ativos de informação em caso de mudança nas atribuições e/ou lotação de usuários, inclusive via geração de relatórios gerenciais pelos sistemas, e que qualquer alteração de acesso depende de comunicação da unidade de Gestão de Pessoas.

Verificou-se, inclusive, a ausência de envio imediato da informação (e definição de responsáveis) de desligamento, aposentadoria ou movimentação de magistrados, servidores, estagiários e aprendizes para fins de ajustes das credenciais de acesso, bem como, não há realização de análise crítica, em intervalos regulares e por meio de processo formal, dos direitos de acesso dos usuários.

Constatou-se, ainda, que o sistema de gerenciamento de senhas não obriga a troca periódica de senhas, e que o registro de acesso (trilha de auditoria) para uso de utilitários de sistemas está restrito apenas ao PJe, não contemplando outros sistemas relevantes.

Por fim, observou-se que o processo de trabalho referente a controle de acessos não se encontra mapeado.

As ocorrências acima contrariam os dispostos no Ato TRT-GP nº 408/2013, Anexo, I, itens 5.2, 5.4, 5.5, 7.1.1, 7.1.3, 8, 9.1.3, 9.3, 9.5, Ato TRT-GP nº 314/2013, item 5.6 e Ato-TRT-GP nº 157/2014.

A situação restou evidenciada no pronunciamento da unidade auditada em resposta à RDI-SACI nº 05/2017, ao informar que a implementação do controle está prevista com a execução do Projeto de Acesso ao Ambiente Virtual do TRT6, que se encontra em fase de planejamento e com previsão de implementação até dezembro/2017.

Esclarecimento dos responsáveis: Acerca do achado, a STI teceu o seguinte pronunciamento:

No que se refere ao PJe, principal sistema do TRT, a regulamentação e procedimentos formais estão definidos na Resolução CSJT nº 185, de 24 de Março de 2017, Seção II, que trata do ACESSO ao Sistema.

Para os demais sistemas que a STI fornece o acesso, atualmente já existe a participação da área de gestão de pessoas, que avisa através de chamado a entrada de um integrante no Tribunal, demandando a criação de e-mail institucional, *login* e senha de rede. Além disso, está em execução o Projeto de Acesso de Ambiente Virtual do TRT6, com o final previsto para dezembro de 2017, o qual está tentando padronizar e formalizar o processo para credenciamento e descredenciamento de usuários para garantia e revogação



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

de acessos, já tendo sido realizado o mapeamento de uma versão inicial do processo para controle de acesso.

A unidade informou, ainda, que estes procedimentos deverão ser implementados após a implantação do SIGEP quando será verificada a viabilidade de automatizar os privilégios de acesso ou a notificação aos gestores do sistema.

Quanto à análise crítica, a STI esclareceu que o Ato TRT nº 385/2013 de 16/08/2013 institui os Gestores da Informação dos Sistemas de Tecnologia da Informação deste Tribunal. Dentre as suas responsabilidades está a de definir os privilégios, perfis e direitos de acesso dos usuários às funcionalidades e às informações disponibilizadas pelos sistemas e soluções de Tecnologia da Informação. No entanto, não existe processo definido para que os gestores realizem a análise crítica dos direitos de acesso dos usuários.

A unidade informou, ainda, que se encontra em elaboração uma minuta disciplinando o uso de senhas no Regional que abordará, além da periodicidade da troca obrigatória da senha, questões relacionadas a sua qualidade. Esse procedimento deverá ser proposto ao Comitê Gestor de Segurança da Informação - CGSI para ser executado em até 3 meses.

No que concerne aos registros de acesso (trilha de auditoria), a STI esclareceu que devido ao processo de nacionalização dos sistemas, os registros devem ser deliberados pelos comitês gestores nacionais para a implementação nos referidos sistemas. Em relação aos demais sistemas, em razão da quantidade de sistemas estratégicos e a complexidade da implementação, deve ser avaliada a possibilidade de atender à solicitação somente para os sistemas que venham a ser classificados como críticos.

Por fim, quanto ao mapeamento do processo de trabalho, a STI informou que o projeto de Acesso ao Ambiente Virtual levará em conta o estabelecido no inciso V do Art. 4º do Ato GP 385/2013, quanto à responsabilidade dos gestores de informação dos sistemas em definir os privilégios, perfis e direitos de acesso dos usuários às funcionalidades e às informações disponibilizadas pelos sistemas e soluções de Tecnologia da Informação.

Avaliação da manifestação: Verifica-se a existência de projeto "Acesso ao Ambiente Virtual do TRT6", em via de elaboração e com previsão de execução até 19/12/2017, que objetiva estabelecer um processo de gestão de acessos no âmbito deste Regional.

Em que pese a normatização do acesso do PJe ocorrer por meio da Resolução CSJT nº 185/2017, observa-se a necessidade de se atentar para os procedimentos de descredenciamento de perfis quando o usuário se desvincular da unidade jurisdicional, preocupação que também deve permear nos demais sistemas e serviços.

Com o intuito de atender aos normativos internos e boas práticas existentes, convém que o processo em tramitação contemple o universo de sistemas de informações e serviços existentes (por exemplo, Sistema de Diárias e de Folha de Pagamento), priorizando os mais relevantes e vulneráveis. Convém, ainda, que o processo estabeleça previsão acerca da responsabilidade do administrador de ativo de verificar e adequar periodicamente as permissões de acesso e promover revogações quando cabíveis.

No que concerne à troca periódica de senhas, tem-se que se encontra em elaboração proposta de normativo a ser submetido ao Comitê Gestor de Segurança da Informação, com previsão de implementação ainda no corrente ano, fato que tornará regular o procedimento em questão.

Apesar da previsão de implantação do SIGEP, entende-se que o processo de comunicação das ocorrências de desligamento da Secretaria de Gestão de Pessoas para a STI



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

deve ser assegurado enquanto não se efetive o funcionamento do referido Sistema, e com isso findar o acesso de usuários não mais autorizados aos sistemas.

Por fim, verifica-se que a unidade comunga com a realização de estudo da viabilidade de promover a ampliação dos registros dos acessos (trilhas de auditoria) para sistemas considerados críticos, a fim de possibilitar a detecção de eventuais inconsistências e, dessa forma, assegurar um controle efetivo dos acessos dos usuários aos sistemas e ambiente de TI.

O não fortalecimento dos procedimentos de controle de acesso resultará em maior vulnerabilidade do ambiente tecnológico.

Achado 2: Processo de gestão de incidentes de segurança da informação insuficientemente divulgado.

Constatou-se que o canal de notificação de incidentes de segurança da informação necessita de maior divulgação, e, por conseguinte, que os usuários deste TRT não se encontram suficientemente cientes da responsabilidade de notificar evento de segurança da informação com celeridade, bem como instruídos a registrar e notificar observação suspeita de fragilidade em sistemas ou serviços de TI. Tais fatos encontram-se em desacordo com o disposto no Ato TRT-GP nº 153/2014, Anexo, III, item 4.

A situação restou evidenciada no pronunciamento da unidade auditada em resposta à RDI-SACI nº 05/2017, ao informar que o canal precisa ser mais divulgado. Por ocasião da visita realizada à unidade em 28/06/2017, esclareceu-se que apesar do canal estar disponibilizado, há necessidade de se promover ações de conscientização e capacitação dos usuários em geral, que ainda não possuem nível de maturidade para utilizá-lo. Afirmou-se, ainda, que atualmente o canal está voltado basicamente aos usuários internos da STI que, em situações pontuais onde ocorra a detecção de um incidente potencial, emite alerta aos demais usuários para utilizar o canal para registro de eventual e específica ocorrência.

Esclarecimento dos responsáveis: Em resposta ao mapa de achados, a STI prestou os seguintes esclarecimentos:

- O Ato TRT-GP nº 153/2014, anexo, parte III determina que os incidentes de segurança da informação deverão ser reportados à ETIR por meio do e-mail incidenteseg-1@trt6.jus.br;
- O procedimento para divulgação do e-mail para reportar incidentes à ETIR está divulgado na intranet na página da Seção de Gestão da Segurança da Informação;
- Em ações de divulgação, como a ocorrida no dia 13 de Junho, o e-mail para notificação de incidentes foi divulgado;
- Como oportunidade de melhoria, será formatada uma mensagem padrão para envio nos alertas de segurança da informação como parte integrante do plano de comunicação da STI, contendo informações e *links* para página com instruções de preenchimento e formulário estruturado para envio da notificação de incidentes.

Avaliação da manifestação: Verifica-se que, em seu pronunciamento preliminar, a STI sinaliza para a necessidade de maior divulgação do canal de comunicação disponível na página da intranet deste TRT, e de se promover ações de capacitação para o uso adequado desse meio.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

Em resposta ao presente achado, a STI renovou os procedimentos já estabelecidos no âmbito deste TRT e, visando o aprimoramento do processo de registro de incidentes de segurança da informação, apresentou propositura de ação de melhoria por meio da emissão de alertas de segurança da informação, que já se encontra inserido no Plano de Comunicação da Secretaria.

Convém destacar que o Ato TRT-GP nº 314/2013 prevê a criação de um Plano de Comunicação e Conscientização em Segurança da Informação. Entretanto, não há sinalização para a construção de documento específico, uma vez que a unidade considera que ações voltadas ao tema estão sendo contempladas no Plano de Comunicação (PC) da STI, que está em fase de elaboração, cuja minuta está prevista pra ser submetida ao Comitê de Governança para aprovação, para posterior publicação, ainda no corrente ano.

Ressalte-se que, em análise à minuta disponibilizada do PC da STI, observou-se que inexistente tópico específico que contemple, de forma permanente, a temática segurança da informação.

A subutilização do canal de notificação de incidentes pelos usuários de redes computacionais restringe a obtenção de êxito na execução do processo de gestão de incidentes, comprometendo a sua celeridade e efetividade.

Achado 3: Procedimentos de controle visando à quantificação e monitoração dos incidentes parcialmente estruturados

Verificou-se que não há o estabelecimento de procedimentos estruturados para manusear diferentes tipos de incidentes de segurança da informação, tais como código malicioso e violações de confidencialidade. Observou-se, ainda, que há geração parcial de trilhas e/ou evidências de auditorias possíveis de serem coletadas e protegidas nos sistemas de informação deste TRT6, uma vez que a funcionalidade encontra-se implementada apenas para o PJe. Constatou-se, inclusive, que não ocorrem de maneira regular e ordenada o envio de registros de ações de emergência para a direção e as análises críticas. Tais ocorrências contrariam o disposto na Resolução Administrativa TRT nº 30/2009, art. 9º; Ato-TRT-GP nº 314/2013, 7.3; Ato-TRT-GP nº 408/2013, item 8; Ato TRT-GP nº 153/2014, Anexo, III (itens 7.2.3, 8 e 9); e Ato-TRT-GP nº 157/2014.

A situação restou evidenciada no pronunciamento da unidade auditada, em resposta à RDI-SACI-SMAAAG nº 05/2017, ao informar que os controles ainda não estão sendo implementados de forma estruturada e que os registros de ocorrências não são usados para fins gerenciais e, ainda, que não há um fluxo definido de ações após o registro.

Esclarecimento dos responsáveis: Em sua manifestação, acerca do achado a unidade auditada informou que, como oportunidade de melhoria, "serão estabelecidos procedimentos para melhor estruturar os controles para quantificação e monitoramentos dos diferentes tipos de incidentes de segurança da informação".

No tocante à geração parcial de trilhas, a STI informou o seguinte:

Devido ao processo de nacionalização dos sistemas, este registro deve ser deliberado pelos comitês gestores nacionais para a implementação nos referidos sistemas.

Em relação aos demais sistemas, face à grande quantidade de sistemas estratégicos e à complexidade da implementação do controle, deve ser avaliada a possibilidade de atender a solicitação somente para os sistemas a serem classificados como críticos.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO



Quanto ao processo de comunicação dos registros de ações de emergência, a unidade esclareceu que "houve somente uma única ocorrência de alto impacto neste Regional, e a mesma foi de conhecimento da administração [...]" e que, apesar da gravidade, ocorreu a normalização da prestação jurisdicional nas Varas do Trabalho do Recife após 24 horas do incidente e sem nenhuma perda de dados, em razão dos procedimentos de backup que haviam sido realizados com sucesso.

Avaliação da manifestação: Constata-se que a unidade auditada corrobora o achado, e apresenta ação de melhoria visando dotar o sistema de procedimentos de controles mais efetivos, o que inclui a possibilidade de ampliação de trilhas e/ou evidências de auditoria possíveis de serem coletadas e protegidas em sistemas considerados críticos, além do PJe.

Destaque-se que a adoção de medidas estruturadoras (o que inclui o estabelecimento de rotina para comunicação dos registros de incidentes à alta administração) minimizará a ocorrência de ação prejudicial na rede de computadores, evitando danos ao sistema de segurança da informação de TI que poderiam afetar negativamente a prestação de serviços e comprometer o alcance da missão institucional.

Achado 4: Inventário dos ativos da informação realizado parcialmente, pendente de classificação e sem responsável explicitamente identificado

Constatou-se que o inventário de ativos de informação encontra-se estruturado apenas quanto aos ativos de infraestrutura, bem como não há classificação dos ativos de informação, nem designação de proprietário responsável para os mesmos, contrariando o disposto no art. 5º da Resolução Administrativa TRT nº 30/2009, Ato-TRT-GP nº 314/2013, item 5.1, Ato-TRT-GP nº 153/2014, Anexo, I (item 4.2) e II (item 5).

A situação restou evidenciada no pronunciamento da unidade auditada, em resposta à RDI-SACI-SMAAAG nº 05/2017, ao informar que apenas os ativos de infraestrutura estão inventariados. Informação ratificada em visita realizada em 28/06/2017, para coleta de informações complementares.

Esclarecimento dos responsáveis: Preliminarmente, a STI informou que o inventário está em processo de estruturação. Entende que convém que o levantamento e a classificação dos ativos de informação, a nível institucional, seja feito pelo responsável da unidade que produz a informação e, por ser uma atividade bastante extensa, a atividade requer uma demanda grande de pessoal, o que estaria incompatível com a atual capacidade laborativa da Seção de Gestão de Segurança da Informação, que conta com três servidores em sua estrutura.

Em relação ao achado, a STI esclareceu que os ativos de microinformática são gerenciados em sistema próprio de patrimônio com responsabilidade atribuída.

Quanto às ações referentes à classificação da informação, informou que estão sendo tratadas pela Presidência.

No que concerne à inexistência de designação de proprietário responsável para os ativos de informação, a unidade de Tecnologia e Informação esclareceu que "o gerenciamento dos equipamentos e a responsabilização é feita por meio do sistema de inventário institucional."

Avaliação da manifestação: O documento que institui a Política de Segurança da Informação do TRT6, Resolução Administrativa TRT nº 30/2009, dispõe que "toda informação gerada no Tribunal será classificada, em termos de valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento". O Ato TRT-GP-nº 314/2013 (Anexo), por sua vez, conceitua ativos de informação como sendo "os meios de armazenamento, transmissão e

Assinatura 7



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso”. Estabelece, ainda, no rol de diretrizes, que os ativos de informação deverão ser identificados e classificados [...], devendo ser atribuído um responsável explicitamente identificado.

Consoante o Ato-TRT-GP nº 153/2014, é de responsabilidade do gestor da informação “definir procedimentos, critérios de acesso e classificar as informações [...]”, sob sua gestão, produzidas ou custodiadas pelo Tribunal. O normativo ainda dispõe que “a Presidência do Tribunal estabelecerá, por intermédio de Portaria, os controles para tratamento da informação classificada, correspondentes a cada grau de confidencialidade, integridade e disponibilidade, respectivamente” e, ainda, os prazos para a efetiva implementação dos controles. Entretanto, em consulta ao sítio institucional, verificou-se que ainda não ocorreu a publicação da referida Portaria.

Esta Seção corrobora a unidade auditada quanto à amplitude da implementação do inventário (identificação e classificação dos ativos de informação, com a atribuição respectiva do responsável), que extrapola as competências da Secretaria de Tecnologia da Informação, uma vez que envolve toda a instituição.

A realização plena de inventário dos ativos de informação, com a devida classificação e designação de responsável, farão com que os ativos recebam um nível adequado de proteção, minimizando riscos às atividades e serviços do Tribunal.

Achado 5: Procedimentos de controle referentes à gestão de ativos parcialmente estruturados

Verificou-se que o processo de trabalho para classificação e tratamento de informações não se encontra mapeado. Constatou-se que inexistente cronograma definido para a realização dos testes de restauração de cópias de segurança, e que os testes de restauração de cópias de segurança não vêm sendo realizados regularmente. Por fim, observou-se que não há implementação de controles de forma estruturada para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.

As ocorrências acima contrariam o disposto no Ato-TRT-GP nº 408/2014, Anexo, V (itens 6.1, 6.2 e 8.1), Ato-TRT-GP nº 157/2014, art.1º e Ato-TRT-GP nº 201/2016, art. 2º.

A situação restou evidenciada no pronunciamento da unidade auditada, em resposta à RDI-SACI-SMAAAG nº 05/2017, ao informar que os controles citados não foram implementados, que as restaurações de cópias são feitas sob encomenda e que a classificação de informação a nível dos recursos de TI ainda não está implementada.

Esclarecimento dos responsáveis: Acerca do presente achado, a STI esclareceu que as ações referente à classificação da informação estão sendo tratadas pela Presidência, o que inclui o mapeamento do processo de trabalho. Acrescentou, ainda, que a frequência com que as restaurações são realizadas minimiza a necessidade de um cronograma prévio e que adotará um calendário de testes regulares de recuperação de dados a fim de manter a regularidade dos testes. Enfatizou que “embora não estejam obedecendo a um cronograma prévio, os testes realizados estão garantindo a qualidade das cópias de segurança” e que “100% das solicitações por restaurações foram atendidas com sucesso”.

Avaliação da manifestação: Considerando que a condução do processo de classificação e tratamento de informação corre pela alta administração, convém que a unidade responsável promova o mapeamento do processo de trabalho, a fim de permitir o estabelecimento de



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

procedimentos de controle pela STI visando garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.

Quanto à necessidade de se firmar um cronograma para realização de testes de restauração de cópias de segurança, a unidade de Tecnologia da Informação sinaliza para a adoção de um calendário de testes.

CONCLUSÃO

Feitos os exames e identificados os achados, apresentam-se os apontamentos acerca das questões de auditoria formuladas pela equipe de auditoria:

1ª. QUESTÃO DE AUDITORIA: A Política de Segurança da Informação (PSI) do TRT6, aprovada pelo Ato – TRT - nº 314/2013, contempla as diretrizes e os princípios que norteiam a gestão de segurança da informação e seus respectivos responsáveis?

Inicialmente, convém destacar que se considerou como norte para a construção da presente questão, as diretrizes, critérios e procedimentos para elaboração, institucionalização e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades na Administração Pública Federal, dispostas na Instrução Normativa 03/IN01/DSIC/GSIPR, que recomenda, dentre outros, definição de estrutura organizacional específica, instituição de Gestor de Segurança da Informação, de Comitê de Segurança da Informação e Comunicação, e de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

A IN01 dispõe, ainda, acerca de elementos a serem contemplados no normativo interno, tais como: escopo, conceitos e definições, referências legais e normativas, princípios, diretrizes gerais (que trate, ao mínimo, sobre os seguintes temas: tratamento da informação, tratamento de incidentes de rede, gestão de risco, gestão de continuidade; auditoria e conformidade, controles de acesso, uso de e-mail e acesso a internet), penalidades, competências, responsabilidades e atualização (previsão de revisão periódica da política).

A Política de Segurança da Informação do TRT6 foi instituída pela Resolução Administrativa TRT nº 30/2009 e pormenorizada pelo Ato-TRT-GP nº 314/2013. O normativo contempla todos os elementos elencados pela Instrução Normativa, supracitados, e estabelece diretrizes gerais dos temas mínimos recomendados, proporcionando uma abordagem mais específica por meio das seguintes normas complementares: Ato-TRT-GP nº 408/2013 (que trata do acesso lógico, do uso de senhas, das estações de trabalho, de software e rede, do acesso à internet, do correio eletrônico, da geração/restauração de cópias de segurança); Ato-TRT-GP nº 153/2014 (tratamento de incidentes, proteção contra códigos maliciosos, controle de acesso físico e tratamento da informação) e Ato-TRT-GP nº 198/2016 (Gestão de Risco de Tecnologia da Informação).

O normativo dispõe, ainda, sobre as responsabilidades da Presidência, do Comitê Gestor de Segurança da Informação e das unidades administrativas envolvidas direta ou indiretamente na gestão da segurança de informação, sugerindo, assim, o comprometimento da alta administração com a PSI.

A política interna prevê, ainda, a elaboração de Plano Diretor de Segurança da Informação. Atualmente, verifica-se que as ações em segurança da informação estão inseridas no Plano Diretor de Tecnologia da Informação e Comunicação.

No que diz respeito à estrutura organizacional, o TRT6 possui em sua composição unidade de apoio administrativo responsável pela gestão da segurança da

9



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

informação denominada Seção de Gestão de Segurança da Informação, subordinada à Divisão de Gestão e Governança de Tecnologia da Informação, por sua vez vinculada à Secretaria de Tecnologia da Informação, nos termos do Art. 9º, III, da RA-TRT nº 30/2009. Consoante o disposto no Ato TRT GP nº 434/2016, a Seção tem como objetivo principal "apoiar o estabelecimento de programa de gestão de segurança e gestão de riscos de TI, em conformidade com as normas e padrões nacionais e internacionais, adotando as melhores práticas de governança da segurança da informação". A unidade conta com três membros, sendo que um deles também integra a equipe responsável pela condução do PJe junto ao CNJ.

O Comitê de Segurança da Informação do TRT6 está formalmente estabelecido por meio da RA-TRT nº 30/2009, e suas competências especificadas pelo Ato-TRT-GP 314/2013.

No que concerne ao Comitê Gestor de Segurança da Informação do TRT6, a institucionalização ocorreu por meio do Ato-TRT-GP nº 311/2013.

Quanto à instituição de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR do TRT6, constata-se sua formalização por meio da Portaria TRT-DG nº 145/2016.

Por fim, tem-se que a Gestão da Política de Segurança da Informação e Normas Complementares possui processo de trabalho formalizado por meio da Portaria DG nº 138/2016.

Conclui-se, portanto, que os normativos contemplam diretrizes e procedimentos mínimos que possibilitam um ambiente tecnológico eficiente e seguro, a fim de favorecer as atividades jurisdicionais e administrativas deste Tribunal.

2ª QUESTÃO DE AUDITORA: O TRT6 promove ações permanentes de divulgação da Política e disseminação da cultura em segurança da informação em toda a organização?

Inicialmente, convém destacar que no rol dos projetos estratégicos do Planejamento Estratégico Institucional (PEI), 2015-2020, reside o Programa de Consolidação da Cultura Organizacional em Segurança da Informação, que se encontra em fase de atualização. Alinhado ao PEI, tem-se o Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) do TRT6 2015-2020, aprovado pelo Ato-TRT-GP nº 120/2016, que prevê, dentre outros, a promoção de ações de comunicação em segurança da informação, como forma de atender ao Objetivo 4 – Fortalecer a segurança da informação.

Destaque-se, ainda, o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do TRT6, referente ao biênio 2015-2016 (Ato-TRT-GP nº 134/2016), que contemplou ações de fortalecimento da segurança da informação voltadas para o "projeto de Sensibilização e Conscientização em Segurança da Informação". Tal previsão também está mantida no PDTIC referente ao triênio 2017-2019, com realização de cinco ações de sensibilização e conscientização por ano. Consoante a unidade de TI, no momento, as ações estão sendo executadas de forma reativa, sem definição prévia, mas reconhece ser mais apropriada a adoção de planejamento antecipado, proposto como ação de melhoria pela unidade.

À luz dos registros do Relatório de Atividades do TRT6 no Exercício de 2015, disponível na página institucional, referente à Seção de Gestão de Segurança da Informação/STI, verifica-se que dentre as principais ações realizadas pela unidade estão as seguintes: execução do Projeto Sensibilização e Conscientização em Segurança da Informação, que contemplou atividades como a criação de página na Intranet contendo dicas



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO



em segurança da informação; divulgação via email institucional de normas e práticas de uso adequado dos recursos computacionais; apresentação de palestra para equipe de atendimento aos usuários sobre segurança da informação; e elaboração e divulgação de cartilha sobre o uso de senhas. O Relatório de 2016 apresenta um conjunto de ações de divulgação e conscientização realizadas, a saber: elaboração de cartaz tratando sobre certificado digital distribuído para as varas do trabalho e setores administrativos; ação de divulgação sobre uso seguro do certificado digital na intranet e na página institucional; criação de aulas em vídeo sobre uso de senhas (previsto pra ser disponibilizado em 2017); publicação de cartilha sobre uso do e-mail institucional; e promoção de ação de divulgação no evento "Café com TI" acerca do processo de tratamento de incidentes.

Verifica-se, ainda, que inexistente registro de elaboração de plano específico de Comunicação e Conscientização em Segurança da Informação, nos moldes do disposto no Ato-TRT- nº 314/2013. Entretanto, tem-se a elaboração de minuta do Plano de Comunicação da Secretaria de Tecnologia da Informação, o qual será submetido ao Comitê de Governança para aprovação (previsto para ocorrer no 2º semestre de 2017) para posterior publicação, mas que carece de tópico específico para ações em segurança da informação, sem contemplar, inclusive, as cinco ações previstas no PDTIC 2017-2019.

Constata-se, conforme reportado no Achado de nº 01, que a comunicação com a unidade de Pessoal requer ser aprimorada no processo de gerenciamento de acessos. Verifica-se, ainda, necessidade de se promover maior divulgação do canal de notificação de incidentes de segurança da informação, bem como, de ações de capacitação dos usuários, consoante o disposto no Achado de nº 02. E, por fim, nota-se fragilidade na comunicação dos registros de incidentes à alta administração, considerando o exposto no Achado de nº 03.

Conclui-se, dessa forma, que há um crescente empenho da STI em promover ações de sensibilização e conscientização na Política de Segurança da Informação no âmbito deste Tribunal visando à disseminação da cultura em segurança da informação na instituição, o que enseja a intensificação de ações permanentes de comunicação e de capacitação para a sua consolidação, e que convém estarem destacadas no Plano de Comunicação da STI, caso não se opte pela construção de Plano de Comunicação e Conscientização em Segurança da Informação próprio.

3ª QUESTÃO DE AUDITORA: As normas internas que disciplinam o controle de acesso, tratamento de incidentes, gestão de ativos e gestão de riscos de segurança da informação atendem às boas práticas vigentes e estão efetivamente em uso?

Pauta-se a presente questão em verificar o nível de aderência dos normativos internos referente ao controle de acesso, tratamento de incidentes, gestão de ativos e gestão de riscos de segurança da informação com as boas práticas em segurança da informação dispostas pela ABNT NBR ISO/IEC 27002:2005, e sua efetiva aplicação.

No tocante ao controle de acesso, tem-se que há política formalmente estabelecida tanto para o acesso lógico (que trata dos tipos de usuários, das contas de acesso, da autenticação, das permissões de acesso aos ativos de informação e da penalidade em caso de tentativa de violação, dentre outros), como para o acesso físico (regras de proteção às instalações e os equipamentos de Tecnologia da Informação), atendendo às exigências mínimas de boas práticas em vigor.

Constata-se ainda, que os sistemas adotados são providos de recursos de segurança. Entretanto, verifica-se que procedimentos de gerenciamento de acesso (a exemplo do registro de credenciamento/descredenciamento de usuários, realização de análise



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

crítica de forma regular) necessitam ser formalizados, e procedimentos de controle de acesso ao sistema (a exemplo do sistema de gerenciamento de senhas) necessitam ser aprimorados, consoante o disposto no Achado de nº 01. Espera-se que tais constatações sejam atendidas no Projeto de Acesso Virtual do TRT6, ainda em fase de planejamento, que possui o propósito de "definir e mapear os processos e procedimentos envolvidos no acesso aos serviços de TI, englobando procedimentos automatizados e manuais, definindo perfis de acesso, atividades e responsáveis, incluindo a implantação do processo".

A preocupação em gerenciar os incidentes de segurança da informação está sinalizada na política interna da instituição, que possui Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais formalmente instituída (ETIR), que atua de forma reativa e, segundo o normativo, nos seguintes serviços: tratamento de incidentes de segurança em redes, emissão de alertas e advertências e geração de relatórios mediante estatísticas e análise de tendência, que são executadas de forma concomitante com as funções regulares inerentes a cada membro da equipe.

Tem-se, ainda, que o processo de gestão de resposta a incidentes de segurança da informação está formalizado por meio da Portaria-TRT-GP nº 138/2016 e que o sítio institucional disponibiliza um *link* de acesso ao formulário de registro de incidentes. Entretanto, verifica-se que o canal de notificação requer maior divulgação, e os usuários carecem de capacitação, tal como abordado no Achado de nº 02. Observa-se, ainda, que os procedimentos de controle, objetivando a quantificação e o monitoramento de incidentes, encontram-se parcialmente estruturados, tal como relatado no Achado de nº 03.

No tocante à gestão de riscos de segurança da informação, verifica-se o estabelecimento de normas que definem como os riscos relacionados aos ativos de informação, projetos e processos de TI serão geridos no âmbito do TRT6, bem como a adoção de boas práticas nos procedimentos de controles. Constata-se, ainda, a escolha dos serviços do PJe e Portal Web como prioritários para as ações imediatas da gestão de riscos, continuidade e incidentes, por serem essenciais à atividade fim da instituição. Verifica-se, por fim, previsão de realização de iniciativa "Executar o Sistema de Gestão de Riscos de TI" em 2017 e em 2018 no PDTIC TRT6. 2017-2019, o que revela o comprometimento da unidade de TI com o tema.

Embora existam normativos internos com diretrizes gerais acerca da classificação e tratamento de informações, constata-se que o processo ainda não está formalmente instituído, nem efetivamente implementado, de maneira a tornar-se norma de cumprimento obrigatório.

A execução do processo de gestão de ativos carece de definição de responsabilidade, de um inventário de ativos da informação devidamente estruturado (que deve contemplar além dos ativos de infraestrutura) e, ainda, de classificação. Tais fatos motivaram o Achado de nº 04.

Ainda na gestão de ativos, verifica-se ausência de mapeamento do processo de trabalho e certa fragilidade de procedimentos de controle no processo de geração de cópias de segurança, que resultaram no Achado de nº 05.

Conclui-se que os documentos internos que dispõem de regras de segurança da informação contemplam, em linhas gerais, requisitos mínimos para assegurar proteção adequada aos ativos de informação. Entretanto, verifica-se imprescindível que a administração proceda à classificação plena dos ativos de informação, com brevidade, a fim de permitir a implementação de controles para garantir a proteção adequada das informações.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

4ª. QUESTÃO DE AUDITORIA: Há um Plano de Continuidade do Negócio formalmente estabelecido?

Inicialmente, convém destacar que o Plano de Continuidade de Negócios (PCN) relacionado às ações de tecnologia da informação é um componente do PCN institucional, que, por sua vez, constitui o sistema de Gestão da Continuidade de Negócio.

Tem-se que diretrizes gerais acerca da Gestão de Continuidade de Negócios, a nível institucional, estão dispostas na Resolução Administrativa TRT nº 30/2009. Convém informar que, consoante o Anexo do Ato-TRT-GP Nº 314/2013, compete ao Comitê Gestor de Segurança da Informação o estabelecimento do Sistema de Gestão da Continuidade do Negócio (SGCN) do Tribunal, que compreende, dentre outros, a elaboração e a manutenção do Programa de Gestão de Continuidade de Negócio. Ainda segundo o normativo, cabe à Seção de Segurança da Informação o gerenciamento do Plano de Continuidade do Negócio e o SGCN.

Por meio da Resolução nº 211 de 15 de dezembro de 2015, o Conselho Nacional de Justiça estabelece, dentre os macroprocessos mínimos a serem observados pelas estruturas organizacionais de TIC, o macroprocesso de segurança da informação de continuidade de serviços essenciais.

À luz dos pronunciamentos e documentações disponibilizadas pela STI, constata-se que ocorreu a definição do "Processo de Elaboração de Plano de Continuidade do Negócio em Tecnologia da Informação", no âmbito deste Tribunal, que consiste num conjunto de atividades para servir de guia à elaboração do Plano de Continuidade de Negócios em TI (PCNTI), em atendimento à iniciativa prevista no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do TRT6, biênio 2015/2016. Tem-se, ainda, a adoção do *software* Risk Manager, desde dezembro de 2016, como ferramenta para a elaboração de PCN voltados a serviços essenciais de Tecnologia de Informação.

Verifica-se que a STI procedeu à elaboração da primeira versão do Plano de Continuidade do Negócio em Tecnologia da Informação – PCNTI, tendo como escopo "Parada Total do PJe" por estar no rol dos principais processos finalísticos do Tribunal. Tem-se, ainda, a inclusão no PDTIC do TRT6, triênio 2017/2019, de revisão (análise e aprimoramento) do PCN, cuja iniciativa encontra-se alinhada com o Planejamento Estratégico Institucional.

Constata-se, por fim, consoante manifestação da Coordenadoria de Gestão Estratégica, que a construção do PCN institucional encontra-se em fase incipiente, o que pode comprometer o planejamento e a execução do PCN de TI, face ausência de diretrizes gerais.

Tem-se, portanto, que o Plano de Continuidade do Negócio aplicado à TI (PCN) está em processo de elaboração, evoluindo de forma satisfatória, e encontra-se alinhado aos objetivos estratégicos do TRT6, apesar do PCN institucional ainda não se encontrar formalmente estabelecido.

Diante das considerações acima, **conclui-se** que a implantação da gestão da segurança da informação transcorre gradualmente e a contento. Os achados identificados são passíveis de correção e não comprometem, de forma significativa, o andamento dos trabalhos desenvolvidos. Verifica-se que as crescentes ações que vêm sendo adotadas demonstram o envolvimento da instituição com o tema segurança da informação e sinalizam à implementação de uma cultura organizacional comprometida em assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações de TI.

Em vista das constatações relatadas, esta equipe de auditoria propõe as seguintes recomendações cujos prazos serão contados a partir da apresentação do respectivo plano de ação:

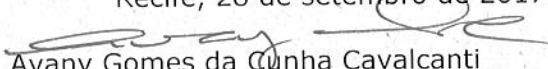


PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO - PE
SECRETARIA DE AUDITORIA E CONTROLE INTERNO

Recomendações

1. Submeter ao Comitê de Governança de TI projeto de controle de acesso contemplando procedimentos formais para o credenciamento/descredenciamento de perfis de usuário, previsão de realização periódica de análise crítica pelos gestores de ativos, regramento acerca do uso de senhas e mapeamento do processo do trabalho, no prazo de 90 dias (Achado nº 1);
2. Promover ações de capacitação e de comunicação para possibilitar o uso efetivo do canal de segurança da informação, no prazo de 180 dias (Achado nº 2);
3. Dotar o Plano de Comunicação da STI de ações permanentes de comunicação e conscientização em segurança da informação, contemplando, no mínimo, as cinco ações previstas no PDTIC 2017-2019, no prazo de 30 dias (Achado nº 2);
4. Aprimorar os procedimentos de controle referentes à quantificação e monitoração dos incidentes de segurança da informação, no prazo de 90 dias (Achado nº 3);
5. Formalizar, junto à Administração, recomendação para promoção do inventário dos ativos de informação, a nível institucional, compreendendo a identificação, classificação e designação de responsável de cada ativo, bem como o mapeamento do respectivo processo de trabalho, no prazo de 90 dias (Achados nº 4 e nº 5);
6. Apresentar cronograma para realização de testes de restauração de cópias de segurança, no prazo de 60 dias (Achado nº 5).

Recife, 28 de setembro de 2017.


Avany Gomes da Cunha Cavalcanti
Chefe da Seção de Monitoramento, Acompanhamento e
Avaliação de Atos de Gestão
Matrícula 30860000827

Silvio Ramos da Silva
Técnico Judiciário
Matrícula 30860002107
(Em gozo de férias)

De acordo com a proposta de recomendações.

Recife, de setembro de 2017.


MYRTHES CASTRO DE MELO E SILVA
Diretora da Secretaria de Auditoria e Controle Interno – em Exercício