AVANY GOMES DA CUNHA CAVALCANTI
SILVIO RAMOS DA SILVA
MARCIA FERNANDA DE MENEZES ALVES DE ARAUJO

RELATÓRIO DE ACOMPANHAMENTO DE AUDITORIA DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO	**RAA – SACI - SMAAAG – 002/2019**
Unidade Auditada:	Secretaria de Tecnologia da Informação
Referência/Assunto:	Auditoria da Gestão de Segurança da Informação
Processo nº	1291/2018
Equipe de Acompanhamento:	Avany Gomes da Cunha Cavalcanti Silvio Ramos da Silva

A atividade de acompanhamento de auditoria está prevista no artigo 6º, IV, do Ato- TRT - GP nº 193/2014, em consonância com a Resolução nº 171/2013 do Conselho Nacional de Justiça, e tem por objetivo verificar as ações efetivamente realizadas pela unidade auditada e o grau de atendimento das recomendações, com possíveis esclarecimentos e justificativas do gestor responsável quanto a obstáculos e dificuldades para a implementação do Plano de Ação, a fim de possibilitar a correção das inconsistências identificadas no relatório de auditoria.

Este relatório apresenta o resultado dos exames realizados no acompanhamento das providências adotadas pela Secretaria de Tecnologia da Informação, acerca das recomendações constantes do Relatório de Auditoria RA-SACI-SMAAAAG-004/2017, abaixo discriminadas, referente à Auditoria da Gestão da Segurança da Informação, e que resultou na elaboração do Plano de Ação (PA) remetido pela unidade auditada em 30/10/2017:

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).

O Plano de Ação residiu na proposição de doze atividades, distribuídas entre as seis recomendações supracitadas.

Os trabalhos de execução do acompanhamento da auditoria ocorreram no período de 08 a 31/01/2019, e as técnicas utilizadas consistiram na indagação escrita e no exame documental.

Cumpre informar que todos os documentos recebidos eletronicamente encontram-se disponíveis na pasta I:\2aInstancia\Pres\SACI\trib.saci\ AUDITORIAS_CNJ 171\ MONITORAMENTO_ACOMPANHAMENTO\FINALIZADAS\GESTAO SEGURANÇA DA INFORMAÇÃO.

Com a finalidade de verificar o atendimento das recomendações, encaminhou-se à unidade auditada a Requisição de Documentos e Informações RDI-SACI-SMAAAG- Nº 035/2018. Em resposta, a Secretaria de Tecnologia e Informação teceu pronunciamento, compartilhando as evidências correspondentes, remetendo, ainda, informações complementares em 21/11/2018, por meio do serviço de colaboração e comunicação coorporativa deste Tribunal, inclusive disponibilizando a documentação comprobatória referente aos links indicados em sua manifestação.

Apresenta-se, a seguir, a consolidação das informações prestadas pela Secretaria de Tecnologia da Informação e a análise final do grau de atendimento das recomendações:

Recomendação 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;

A Unidade auditada sinalizou positivamente e informou o que se segue:

> A organização do controle de acesso à rede e sistemas do TRT6 foi realizada com formalização e publicação do Processo de Concessão e Remoção de Acessos (http://novaintranet.trt6.jus.br/fluxos/Processos-de-ConcessaoeRemocaoDeAcesso) – Portaria TRT DG Nº 091/2018 de 15/06/2018.
>
> Em relação à troca periódica de senha, estamos aguardando posicionamento do comitê gestor de TI quanto a eficácia da estratégia, visto que com a atualização e unificação dos Sistemas de autenticação de Rede (Active Directories) uma nova política de senha será implementada com base em critérios mais rígidos e obrigatórios (Caracteres especiais, tamanho mínimo, números, letras maiúsculas e minúsculas entre outros). Dessa forma, há uma preocupação a respeito da exigência de uma troca periódica, que pode induzir os usuários a utilizar senhas menos fortes para facilitar a memorização, além de um possível aumento significativo de solicitações a Central de Serviços nos períodos de troca. Ainda, cabe ressaltar que foi desenvolvido um sistema que permite a recuperação e a troca de senhas para Aposentados e Pensionistas via formulário na internet. Há estudo sendo realizado para verificar se é possível a extensão do uso deste sistema para todos os usuários.

Ainda acerca do tema, a Seção de Gestão de Segurança da Informação (SGSI) da STI, esclareceu que o Projeto de Acesso ao Ambiente Virtual consistiu, fundamentalmente, no mapeamento e implantação de um processo de gestão de acessos ao ambiente virtual do TRT6, o qual foi submetido e aprovado pelo Comitê de Governança de TI, consoante Ata da 2ª Reunião realizada em 02/05/2018, tendo sido formalizado por meio da Portaria TRT DG Nº 91/2018.

A unidade destacou, ainda, que o escopo inicial do projeto previa a implementação de rotinas automatizadas para a concessão e remoção de acessos, porém durante a sua execução, revelou-se inoportuna a sua implantação, razão de não constar na versão final do Plano de Projeto (abril/2018). A SGSI disponibilizou link de acesso ao Projeto, com Termo de Encerramento homologado em 05/09/2018 (PROAD nº 19333/2018). Destacou, porém, que o processo formalizado contempla a análise do acesso, o qual estabelece a responsabilidade ao chefe do usuário pela emissão de alerta para solicitar a concessão ou remoção de acesso.

No tocante a procedimentos formais de credenciamento/descredenciamento de acesso, a Seção reportou ao Ato–TRT-GP nº 296/2017, que atualiza a Política de Segurança da Informação no âmbito do TRT6.

Convém destacar que, após exames, constatou-se que o normativo supracitado não resultou em modificação, nem acréscimo na normatização acerca do controle de acesso lógico, mantendo-se o teor do Anexo do Ato-TRT-GP 408/2013, anteriormente vigente.

Diante do exposto, verifica-se que o projeto de controle de acesso foi submetido e aprovado pelo Comitê de Governança de TI - e posteriormente instituído, e o regramento acerca do uso de senhas encontra-se em curso. Recomendação implementada.

Recomendação 2: Promover ações de capacitação e de comunicação para possibilitar o uso efetivo do canal de segurança da informação;

A STI sinalizou positivamente ao atendimento da recomendação. Em seu pronunciamento à RDI, apresentou as seguintes informações:

> Conforme observações apontadas no plano de ação, as seguintes tratativas foram realizadas:
>
> Página da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Tribunal: (http://novaintranet.trt6.jus.br/sti/segurancadainformacao/etir);
>
> Formulário para notificação de incidentes de segurança da informação: http://www.trt6.jus.br/portal/formulario/notificar-incidente-de-seguranca-da-informacao);
>
> Divulgação do Canal: http://novaintranet.jus.br/noticias/2017/11/28.etir-trt6-disponibiliza-formulario-para-notificacao-de-incidentes-de-seguranca
>
> Os alertas de segurança da informação emitidos fazem referência ao canal de notificação como forma de divulga-lo, exemplo: http://novaintranet.trt6.jus.br/noticias/2018/11/06/alerta-de-seguranca-da-informacao.

Quanto a ações de capacitação, a unidade informou que ocorreu capacitação apenas para a equipe da SGSI. Em que pese à ausência de ações voltadas para os usuários,

constatou-se, na intranet, a inclusão de informações e link direcionando para a página da ETIR (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Tribunal), com instruções de preenchimento, orientação sobre o que notificar, qual a importância da notificação e como comunicar um incidente, bem como, acesso ao formulário para envio da notificação de incidentes. Destaque-se que tais ações, embora não tenham integrado o Plano de Ação, foram apontadas pela STI como oportunidade de melhoria, por meio do Ofício TRT6-STI-nº 046/2017, consoante Relatório de Auditoria RA-SACI-SMAAAG-004/2017.

Em consulta à página da intranet, acesso em 31/01/2019, identificou-se registro de publicação em 28/11/2017 acerca da disponibilização de formulário para notificação de incidentes de segurança pela ETIR-TRT6 e, em 19/07/2018, da Dica de TI nº 17 – *Você sabe o que é Phishing e como notificar sua ocorrência?* com divulgação do link de acesso ao canal de notificação de Incidente de Segurança da Informação. Tais publicações também foram divulgadas por meio do endereço eletrônico institucional.

Foram identificadas, ainda, mensagens de Alerta de segurança da informação, emitidas em 22/03/2018, 06/04/2018, 08/06/2018 e 15/06/2018, decorrentes de notificações feitas à STI, por servidores, acerca de recebimento de e-mail suspeito. Registre-se que nas mensagens, além da advertência da unidade de Tecnologia da Informação, constaram orientações e informação do link para registro de conteúdo suspeito. Tais registros sinalizam o uso do canal de notificação pelos usuários.

Dessa forma, verifica-se que ocorreram ações de comunicação e de capacitação em 2018 e que contribuíram para o uso efetivo do canal. Recomendação implementada.

Recomendação 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.

A STI apresentou resposta afirmativa ao atendimento da recomendação. Em seu pronunciamento, informou o seguinte:

> Foram realizadas ações de comunicação relativas à segurança da informação por meio da publicação de Boletins, Dicas e Alertas de Segurança da Informação.
> (http://novaintranet.trt6.jus.br/sti/plano-de-comunicacao-da-sti)
> **Boletins**
> http://novaintranet.trt6.jus.br/sti/boletim-fake-news
> http://novaintranet.trt6.jus.br/sti/boletim-conceitos-basicos-de-ransomware
> http://novaintranet.trt6.jus.br/sti/senhas-dicas
> **Dicas**
> http://novaintranet.trt6.jus.br/sti/dica-de-ti-no-01-28-de-janeiro-dia-internacional-deprotecao-de-dados-pessoais
> http://novaintranet.trt6.jus.br/sti/dica-de-ti-no-05-como-denunciar-spam-no-correioeletronico
> http://novaintranet.trt6.jus.br/sti/dica-de-ti-no-11-politica-de-mesa-limpa-e-tela-limpa
> http://novaintranet.trt6.jus.br/sti/dica-de-ti-no-17-sgsi
> http://novaintranet.trt6.jus.br/sti/dica-de-ti-no-28-como-proteger-suas-senhas
> **Alertas**
> http://novaintranet.trt6.jus.br/noticias/2018/06/08/alerta-de-seguranca-da-informacao

http://novaintranet.trt6.jus.br/noticias/2018/04/06/alerta-de-seguranca-da-informacao
http://novaintranet.trt6.jus.br/noticias/2018/03/22/alerta-de-seguranca-da-informacao

Em consulta ao portal institucional, verificou-se que ocorreu a revisão do Plano de Comunicação da STI, em 29/01/2018 (2ª. versão), com a inclusão de duas ações relativas à segurança da informação: Emissão de Alerta de Segurança da Informação e Ações de Comunicação em Segurança da Informação. No tocante a Ações de Comunicação, o Plano estabelece a realização de, no mínimo, cinco ações de divulgação e conscientização em segurança da informação por ano, visando reduzir os incidentes relacionados à segurança da informação de TI, utilizando-se diversos canais de comunicação (Portal do TRT6, Intranet, Correio eletrônico, Informativo semanal impresso no "Mural da Sexta", curso e palestra). Quanto à Emissão de Alertas, a versão atual do Plano determina a divulgação de alertas ou advertências sempre que ocorrerem situações que caracterizem um incidente de segurança da informação, com as devidas orientações aos usuários sobre como agir diante de tais situações.

Constatou-se, por fim, a realização das seguintes ações de comunicação em 2018: "Dicas de TI" acerca de Proteção de Dados Pessoais (nº 01), Como denunciar Spam no correio eletrônico (nº 05), Política de mesa limpa e tela limpa (nº11), Você sabe o que é *Phishing* e como notificar sua ocorrência (nº 17) e Como proteger suas senhas (nº 28); e "Boletins de Segurança da Informação" acerca de Conceitos básicos de *Ransomware*, *Fake News*, Boas Práticas para senhas e Teletrabalho.

Tem-se, portanto, que o Plano de Comunicação da STI, atualmente vigente, contempla as cinco ações previstas no PDTIC 2017-2019, que foram efetivamente realizadas em 2018, com registro na 2ª Ata de Reunião de 2018, do Comitê Gestor de Segurança da Informação (CGSI), de 13/12/2018. Recomendação implementada.

Recomendação 4: Aprimorar os procedimentos de controle referentes à quantificação e monitoração dos incidentes de segurança da informação.

Em seu pronunciamento, a STI informou a realização das ações, previstas no Plano de Ação para o atendimento da recomendação, por meio do PROAD nº 17598/2017:

- Elaborar modelo para relatório de incidentes de segurança da informação: 17598/2017 (PROAD)
- Elaborar tabela de categorização de incidentes de segurança da informação:17598/2017(PROAD)
- Aprimorar modelo de formulário para notificação de incidentes de segurança da informação:17598/2017 (PROAD) http://www.trt6.jus.br/portal/formulario/notificar-incidentede-seguranca-da-informacao

Após exames, constatou-se a elaboração do Modelo de Relatório de Incidentes de Segurança da Informação (SI), com definição da tabela de categorização que classifica os incidentes em oito categorias: "conteúdo abusivo", "código malicioso", "prospecção por informações", "tentativa de intrusão", "intrusão", "indisponibilidade de serviço ou informação", "fraude", "outros".

Observou-se, ainda, a elaboração de Modelo de formulário para Notificação de Incidentes de SI e definição dos canais para disponibilização do formulário, consoante Ata da Reunião de Gestão de Incidentes de 25/10/2017 (PROAD nº 17598/2017).

Ressalte-se que as referidas ações integraram o Projeto Estratégico "Estabelecimento da Gestão de Incidentes de Segurança da Informação", que se encontra com status finalizado, conforme Termo de Encerramento e 2ª Ata da Reunião de 2018 do CGSI. Recomendação implementada.

Recomendação 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.

Inicialmente, convém registrar a Resolução Administrativa TRT6 nº 21/2017, publicada no Diário Eletrônico da Justiça do Trabalho de 21/08/2017 e com vigência a partir de 17/02/2018, que regulamenta a Lei nº 12.527/2011 (Lei de Acesso à Informação) no âmbito deste Regional, inclusive quanto à classificação e tratamento das informações. Destaque-se que o normativo estabelece, no seu art. 28, que "compete à unidade detentora ou produtora da informação adotar providências para a formalização e tramitação do processo para classificação do documento", cabendo ao Núcleo de Gestão Documental do Tribunal "disponibilizar orientações, formulários, instrumentos, entre outros para a uniformização dos procedimentos a serem adotados pelas unidades deste Regional para obtenção da classificação da informação" (Parágrafo único).

No tocante ao atendimento da recomendação, a STI sinalizou positivamente. A título de documentação comprobatória, a unidade acostou cópia da Ata de reunião referente à Discussão sobre a Gestão de Inventário de Ativos de Informação, ocorrida no dia 14/11/2018, na Secretaria Geral da Presidência (PROAD nº 25168/2018).

De acordo com a Ata, a reunião contou com a participação do Secretário Geral da Presidência, do Diretor-Geral, das Chefias do Núcleo de Gestão Documental e Memória e da Divisão de Gestão e Governança de TI, e de membros da Seção de Gestão da Segurança da Informação. Na ocasião, foram discutidos os principais pontos da Resolução Administrativa TRT6 nº 21/2017, apresentado o mapeamento preliminar do Macroprocesso de classificação/desclassificação de informações, bem como, dos procedimentos pertinentes à TI. Informou-se, ainda, "que já se encontra em andamento uma série de atividades no sentido de implementar o inventário e classificação dos ativos de informação no âmbito da Justiça do Trabalho, existindo ainda a iniciativa de adoção de uma solução nacional para informatização dos controles e procedimentos", objeto de evento ocorrido recentemente e que contou com a participação do TST, Núcleos de Gestão Documental e algumas Secretarias de Tecnologia da Informação da Justiça do Trabalho.

Registre-se, por fim, que a reunião gerou quatro encaminhamentos, cabendo à STI obter mais informações sobre as diretivas do TST quanto ao uso do software ICA-Atom, e ao Núcleo de Gestão Documental e Memória às demais inciativas, com vistas à efetiva implementação da Resolução Administrativa nº 21/2017.

Dessa forma, constata-se que ocorreu a formalização, junto à Administração, da necessidade de se promover o inventário de ativos de informação, e que se encontra na fase preliminar de implantação. Recomendação implementada.

Recomendação 6: Apresentar cronograma para realização de testes de restauração de cópias de segurança.

A STI informou que ocorreu a definição de cronograma, apresentando como documentação comprobatória links de acesso abaixo, e ainda, a Política de Restauração.

> Cronograma de testes de restauração está no seguinte endereço do WIKI: http://wiki.trt6.gov.br/wiki/index.php/Se%C3%A7%C3%A3o_de_Gest%C3%A3o_de_Backup_e_Restore:_Pol%C3%ADtica_para_testes_de_restaura %C3%A7%C3%A3o
>
> Agenda de testes de Restauração: http://wiki.trt6.gov.br/wiki/index.php/Se%C3%A7%C3%A3o_de_Gest%C3%A3o_de_Backup_e_Restore:_Calend%C3%A1rio_de_teste_de_restaura%C3%A7%C3%A3o_2018

Ressalte-se que a Política de Restauração aplica-se aos seguintes grupos de *backup*: Servidores de arquivos Sede, Servidores de arquivos Imbiribeira, Servidores de arquivos Interior, Arquivos servidores Linux, Arquivos de Máquinas Oracle, e Arquivos do PJe, com estabelecimento da periodicidade, data de execução, definição de arquivos para restauração, equipe responsável e procedimento de validação.

Verificou-se que ocorreu a elaboração do Calendário de teste de restauração de 2018, pela Seção de Gestão de Backup e Restauração, unidade responsável.

Importa frisar que a presente recomendação visa à implantação anual do procedimento de controle, a fim de contribuir efetivamente para a realização tempestiva de testes de restauração de cópias de segurança. Recomendação implementada.

CONCLUSÃO

Diante dos apontamentos e esclarecimentos adicionais prestados pela Secretaria de Tecnologia da Informação, apresenta-se o grau de atendimento das recomendações:

RECOMENDAÇÃO	GRAU DE ATENDIMENTO DA RECOMENDAÇÃO					
	Implementada	Em implementação (no prazo)	Em implementação (com prazo expirado)	Parcialmente implementada	Não implementada	Não mais aplicável
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);	x					
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);	x					
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	x					

RECOMENDAÇÃO	GRAU DE ATENDIMENTO DA RECOMENDAÇÃO					
	Implementada	Em implementação (no prazo)	Em implementação (com prazo expirado)	Parcialmente implementada	Não implementada	Não mais aplicável
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);	x					
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); e	x					
6. Apresentar cronograma para realização de testes de restauração de cópias de segurança, no prazo de 60 dias (Achado nº 5).	x					

Em vista das constatações e observações, **conclui-se** que as ações foram efetivamente implementadas pela Secretaria de Tecnologia da Informação e proporcionaram o atendimento de 100% das recomendações constantes no RA-SACI-SMAAAG nº 004/2017, de forma satisfatória.

Recife, 12 de fevereiro de 2019.

SILVIO RAMOS DA SILVA
Técnico Judiciário
Matrícula 30860002107

AVANY GOMES DA CUNHA CAVALCANTI
Chefe da Seção de Monitoramento, Acompanhamento e Avaliação dos Atos de Gestão
Matrícula 30860000827

De acordo.

Atendidas as recomendações constantes do RA-SACI-SMAAAG-nº 004/2017.

Recife, 12 de fevereiro de 2019.

MÁRCIA FERNANDA DE MENEZES ALVES DE ARAÚJO
Diretora da Secretaria de Auditoria e Controle Interno