Ata Reunião do Comitê Gestor de Segurança da Informação

Ata nº 002/2021 **Tipo:** Ordinária **Data:** 21.05.2021 **Duração:** 02 horas

RODRIGO MAFRA
RODRIGO CARTAXO MARQUES DUARTE
ANTONIO FRAGOSO CAVALCANTE NETO
ARYOSWALDO JOSE BRITO ESPINOLA
LINDINALDO SILVA MARINHO
HYDERLANDSON COELHO DA COSTA
EWERTON LEANDRO DA COSTA ARAUJO

Pauta:	1. Nova Política de Segurança da Informação e Comunicações - POSIC; 2. Alteração norma de utilização do correio eletrônico; 3. Status do Plano de Ação Prevenção Ransomware; 4. Alteração de senhas de pensionistas e aposentados; 5. Atualização do escopo do Sistema de Gestão de Segurança da Informação - SGSI; 6. Calendário próximas reuniões.	
Relator:	Rodrigo Mafra	**Local:** Videoconferência

1 Participantes

Lindinaldo Silva Marinho	lsmarinho@trt13.jus.br
Antônio Fragoso Cavalcante Neto	afneto@trt13.jus.br
Aryoswaldo José Brito Espínola	aespinola@trt13.jus.br
Hyderlandson Coelho da Costa	hccosta@trt13.jus.br
Rodrigo Cartaxo Marques Duarte	rcduarte@trt13.jus.br
Rodrigo Mafra	rmafra@trt13.jus.br
Ewerton Leandro da Costa Araujo	elaraujo@trt13.jus.br

2 Tópicos/decisões/ações

Itens	Tópicos tratados	Ações/Decisão
1	*Nova Política de Segurança da Informação e Comunicações - POSIC*	• *Presidente do Comitê irá encaminhar minuta da RA para aprovação do Tribunal Pleno.*
2	*Alteração norma de utilização do correio eletrônico*	• *Presidente do Comitê irá encaminhar minuta do Ato para aprovação da Presidência do Tribunal.*

Itens	Tópicos tratados	Ações/Decisão

3	*Status do Plano de Ação Prevenção Ransomware*	• *Seção de Segurança da Informação (SSI) apresentou ao Comitê o status do Plano de Ação elaborado pela SETIC sobre as recomendações da SSI relacionadas aos ataques ocorridos no CNJ e STJ em novembro/2020 (chamado OTRS 068468);*
		• *Comitê deliberou sobre as ações do plano com status de "Não implantado", conforme segue:*
		  ○ *O risco de algumas ações não implantadas foi aceito pelo Comitê, mediante as observações técnicas apresentadas pelo Núcleo de Infraestrutura de TIC (NITIC);*
		  ○ *O plano de ação de outras ações não implantadas foi atualizado com as observações do Comitê;*
		• *O documento atualizado encontra-se no Anexo I.*

4	*Alteração de senhas de pensionistas e aposentados*	• *Seção de Segurança da Informação (SSI) apresentou ao Comitê as dificuldades relatadas pelo NITIC para a alteração de senhas de pensionistas e aposentados;* • *Diretoria da SETIC irá alinhar com a SEGEPE procedimentos para a alteração de senhas de pensionistas e aposentados no processo de recadastramento destes ("prova de vida"), sugerindo as alterações necessárias nos regulamentos pertinentes.*
5	*Atualização do escopo do Sistema de Gestão de Segurança da Informação - SGSI*	• *Comitê deliberou pela inclusão do PROAD no escopo do SGSI;* • *Presidente do Comitê irá encaminhar minuta do Ato para aprovação da Presidência do Tribunal.*
6	*Calendário próximas reuniões*	• *Próxima reunião em 90 dias.*

3 Observações gerais

Itens	
1	*Próxima reunião ordinária: a definir*
2	*Protocolo da reunião: PROAD 21981/2021*

4 Lista de arquivos relacionados

Itens	https://www.trt13.jus.br/intranet/informatica/seguranca-da-informacao

Obs.: Qualquer alteração desta ata deverá ser comunicada ao relator dentro de 24 horas após seu recebimento.

LINDINALDO SILVA MARINHO
Magistrado - Presidente CGSI

ARYOSWALDO JOSÉ BRITO ESPÍNOLA
Diretor da Secretaria Administrativa
TRT 13

FRANCISCO H. DE OLIVEIRA MENDONÇA
Secretária-Geral da Presidência
TRT 13

HYDERLANDSON COELHO DA COSTA
Representante do GVP
TRT 13

RODRIGO CARTAXO MARQUES DUARTE
Diretor SETIC
TRT 13

RODRIGO MAFRA
Chefe Seção de Segurança da Informação
TRT 13

EWERTON LEANDRO DA COSTA ARAUJO
Chefe Núcleo de Infraestrutura de TIC
TRT 13

ANEXO I
PLANO DE AÇÃO RANSOMWARE
(ATUALIZAÇÃO 21/05/2021)

RECOMENDAÇÕES SSI	REFERÊNCIAS	NÚCLEO	SERVIDOR	PLANO DE AÇÃO	STATUS	OBSERVAÇÕES TÉCNICAS
Ativar no IPS a detecção e bloqueio ao JexBoss	https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0710.html	NITIC	Ricardo	---	Implantado	Proteção já implantada pelo nosso firewall.
Monitorar nos logs de acesso web as strings "jexws" e "jexinv"	https://us-cert.cisa.gov/ncas/analysis-reports/AR18-312A	NITIC	---	Item não se aplica mais.	Não implantado	Nosso ambiente não é vulnerável ao JexBoss, conforme testes realizados pela SSI (Chamado#069154). Então, acreditamos que não traz benefícios ao ambiente gastar recursos computacionasis para realizar o monitoramento recomendável.
Utilizar o JexBoss para testes de vulnerabilidade	https://blog.corujadeti.com.br/jexboss-testando-a-seguranca-do-jboss https://github.com/joaomatosf/jexboss	SSI	Manuel	Executado em novembro/2020	Implantado	Não foram detectadas vulnerabilidades (Chamado#069154)
Atualizar SO e JBossAS/WildFly nos servidores de aplicação		NITIC/NDMS	Wilberto/Danillo	NDMS irá elaborar plano para atualização das aplicações pertinentes. Prazo a definir.	Não implantado	**Em relação ao PJe, as imagens (containers) são padronizadas para todos os TRTs.** Não temos como atualizá-las ou modificar a versão do servidor de aplicação. **Em relação às aplicações internas, a versão do SO e do servidor de aplicação não podem ser atualizadas sem que o desenvolvimento atualizem as aplicações.** Convém destacar que consideramos o **risco envolvido é relativamente baixo**, uma vez que os servidores de aplicação não são exposto para a Internet.
Ativar no IPS a detecção e bloqueio das vulnerabilidades CVE-2019-5544, CVE-2020-3992 e CVE-2020-1472	https://www.checkpoint.com/defense/advisories/public/2020/cpai-2019-1794.html ; https://www.checkpoint.com/defense/advisories/public/2020/cpai-2020-0872.html	NITIC	Ricardo	---	Implantado	Estava pendente da imaplantação da CVE-2020-3992 no IPS pela CheckPoint. Porém, a própria VMware lançou release para correção desta vulnerabilidade.
Configurar os antivírus nos servidores para bloquear os seguintes executáveis (MD5 hashes): 4bb2f87100fca40bfbb102e48ef43e65; 80cfb7904e934182d512daa4fe0abbfb; aa1ddf0c8312349be614ff43e80a262f ; fcd21c6fca3b9378961aa1865bee7ecb;	https://community.mcafee.com/t5/Endpoint-Security-ENS/How-to-block-the-Hashes-in-epo-server/td-p/637532	NAU	Alessandra	---	Implantado	Chamado Aberto na Netsafe. Recebemos da NetSafe as orientações técnicas deste link, as quais foram implantadas quando aplicável. Não foi necessário criar regra de controle de acesso, como diz o link da referência, pois as vacinas estão atualizadas, conforme explica o item 6 do referido material da Netsafe.
Verificar na gerência do antivírus (ePO) detecções recentes, especialmente por: Artemis, Ransomexx ou RDN/Generic.dx		NAU	Alessandra	---	Implantado	Resposta neste link.
Monitorar tentativas de acesso à porta 427 nos servidores de administração do VMware		NITIC	Ruber	---	Implantado	O VMware não disponibiliza uma ferramenta para monitorar requisições às portas. Porém, **os patches mais recentes para corrigir a vulnerabilidade no serviço CIM foram instalados em todos os hosts, e ainda assim o serviço foi desabilitado** em todos os hosts, por não ser necessário na nossa estrutura.

RECOMENDAÇÕES SSI	REFERÊNCIAS	NÚCLEO	SERVIDOR	PLANO DE AÇÃO	STATUS	OBSERVAÇÕES TÉCNICAS
Trocar todas as senhas administrativas (SOs, VMware, SGBDs, etc)		NITIC	Ewerton	Trocar padrão de senhas no segundo semestre de 2021. NITIC irá definir procedimentos para alteração das referidas senhas anualmente. Prazo a definir.	Não implantado	Utilizamos um padrão de senhas e planejamos fazer a troca deste padrão no segundo semestre de 2021. Convém resaltar alguns pontos: - **A troca de senha administrativas tem que ser planejada e orquestrada**, para evitar vulnerabilidades no próprio procedimento de troca de senhas; - **São muitos ativos e itens de configuração** e isto requer um tempo dispendioso da equipe de infraestrutura; - **Estamos restrigindo o acesso aos equipamentos apenas a rede do núcleo de infraestrutura. Isto traz um granho muito maior ao ambiente em termos de segurança da informação**. - A mudança periódica de senha está se tornando uma prática não-recomendável, que gera mais vulnerabilidades do que manter uma senha complexa por mais tempo. **Gigantes da tecnologia estão desaconhelhando esta prática. A própria microsoft classificou com "É uma prática velha e obsoleta"** (https://g1.globo.com/economia/tecnologia/noticia/2021/04/21/quando-mudar-periodicamente-suas-senhas-pode-te-deixar-mais-vulneravel-a-hackers.ghtml)
Desabilitar o CIM Server no VMware ESXi	https://www.vmware.com/security/advisories/VMSA-2020-0023.html https://kb.vmware.com/s/article/76372	NITIC	Ruber	---	Implantado	Funcionalidade está desabilitada em todos os servidores ESXi.
Verificar se a base de assinaturas do IPS está atualizada e em modo de bloqueio	https://ntsec.com.br/academy/ips-check-point	NITIC	Ricardo	---	Implantado	A base é atualizada automaticamene de maneira regular.
Bloquear no firewall qualquer acesso de ou para IPs envolvidos em ataques (listas atualizadas em tempo real)	http://reputation.serpro.gov.br https://www.abuseipdb.com https://www.dshield.org/block.txt	NITIC	Ewerton	---	Implantado	As listas recomendadas abuseipdb e da dshield não permitem de forma simples a automatização no nosso firewall. Utilizamos, porém, outras listas: https://s3.i02.estaleiro.serpro.gov.br/blocklist/blocklist.txt http://reputation.alienvault.com/reputation.data https://secureupdates.checkpoint.com/IP-list/IP-blacklist.txt https://www.talosintelligence.com/documents/ip-blacklist https://secureupdates.checkpoint.com/IP-list/TOR.txt
Verificar se o antivírus do filtro web está ativo e atualizado	http://www.eicar.org/download/eicar.com.txt	NITIC	Ricardo	---	Implantado	O antivírus do firewall é atualizado automaticamene de maneira regular.
Ativar filtro web com inspeção HTTPS e autenticação	https://secure.eicar.org/eicar.com	NITIC	Ricardo	Para o HTTPS Inspection: Maio/2021	Pacialmente implantado	A versão anterior de firewall apresentava muitos problemas no HTTPS Inspection, fazendo com que a feature fosse desabilitada. Na nova versão atualizada no último mês, podemos notar que houve melhorias consideráveis nesta feature. Estamos testando o HTTPS Inspection em um ambiente controlado, funcionando sem problemas iremos replicar para toda rede interna. Sobre autenticação,não achamos necessário. Há outros meios de correlacionar o tráfego aos usuários. Achamos que só vale a pena configurar autenticação se ficar transparente aos usuários.
Verificar se os antivírus nas estações estão atualizados		NAU	Alessandra		Pacialmente implantado	Resposta neste link.

RECOMENDAÇÕES SSI	REFERÊNCIAS	NÚCLEO	SERVIDOR	PLANO DE AÇÃO	STATUS	OBSERVAÇÕES TÉCNICAS
Bloquear acesso Internet a partir dos servidores, permitindo somente os acessos necessários		NITIC	Ricardo	Risco aceito pelo CGSI, considerando que os acessos Internet oriundos de servidores passam pelo filtro web.	Risco aceito	Se implementarmos esta recomendação, teríamos que deslocar boa parte da mão de obra do núcleo de infraestrutura de TI para ficar fazendo apenas isto de plantão. Enquanto isto demais controles bem mais importantes seriam relegados. **Resumindo: a recomendação é viavel técnicamente, mas o custo de administração é extremamente alto. Temos convição que devemos priorizar esforços no tráfego que entra na nossa rede e não no que sai.** Convém ressaltar também que desconhecemos qualquer TRT, até mesmo de grande porte, que implemente uma restrição deste tipo.
Configurar autenticação 2FA no OpenVPN, GV 2, e GSuite;	https://openvpn.net/vpn-server-resources/google-authenticator-multi-factor-authentication ; http://gsuite.ufla.br/habilitando-a-autenticacao-de-2-fatores-na-conta-gsuite	NITIC	Ewerton	NITIC irá realizar estudos sobre a implantação de 2FA nas VPNs utilizadas. Prazo a definir.	Não implantado	A ideia é interessante. Porém, no momento não é possível ser realizado esta configuração, uma vez que até a autenticação do google irá passar a ser feita internamente.
Configurar autenticação 2FA no SSH, RDP, administração VMWare e outros acessos administrativos	https://www.100security.com.br/ssh-google-authenticator	NITIC	Ewerton	Risco aceito pelo CGSI, mediante as observações técnicas apresentadas pelo NITIC.	Risco aceito	**A relação custo-benefício não justifica a adoção desta recomendação.** A autenticação por dois fatores para ferramentas de administração dificultará a execução de scripts e tarefas automáticas. Achamos que segmentar a rede para ter um controle melhor dos acessos seja uma solução mais efetiva.
Restringir acessos administrativos SSH, RDP, VMWare, Oracle e outros para determinados IPs	https://qastack.com.br/unix/406245/limit-ssh-access-to-specific-clients-by-ip-address ; https://support.managed.com/kb/a2499/restrict-rdp-access-by-ip-address.aspx ; https://blogs.vmware.com/vsphere/2014/03/restricting-access-to-the-esxi-host-console-revisiting-lockdown-mode.html	NITIC	Ricardo/Ruber	Previsto para o segundo semestre de 2021.	Pacialmente implantado	Antes de efetivar qualquer restrição das ferramentas de acesso administrativo, deveremos segmentar as redes. Já foi realizado a segmentação da rede da SETIC. Falta fazer com que a rede dos equipamentos e a rede dos servidores passem obrigatoriamente pelo Firewall.
Alterar porta SSH nos servidores e configurar quarentena por erros	https://blog.remontti.com.br/97	NITIC	Ewerton	---	Pacialmente implantado	**Achamos aque a sugestão não traz qualquer aumento no nível de segurança do ambiente. Qualquer port scan, por mais simples que seja, consegue identificar a porta que o SSH está rodando.** **Não é alterando a altura da fechadura de uma porta que a torna mais segura.** Em nosso ambiente já monitoramos os erros de acesso de usuários privilegiados.
Criação de filtros de acesso no OpenVPN, permitindo somente os acessos necessários	---	NITIC	Ewerton	---	Implantado	Já há um filtro para acesso à VPN.
Utilização da solução VPN da Checkpoint em substituição à atual		NITIC	Ewerton	Verificar se nas próximas versões do firewall se o cliente da VPN teve melhorias que justifiquem a mudança da solução. Prazo a definir.	Não implantado	A solução da checkpoint tem uma série de problemas que fizeram com que fosse preterida, tais como: - Necessidade de padronizar a versão do java e do navegador. (Só roda em navegadores de 32bit) - Cliente Mobile muito ruim; Nas próximas versão do firewall iremos verificar se tais problema tiveram melhoras.
Restringir acesso VPN somente à SETIC		NITIC	Ewerton	---	Implantado	Restringido o acesso a VPN para somente usuários com necessidades reais.
Não utilização do GV 2 para acessos administrativos e remoção de possíveis ferramentas administrativas do mesmo		NITIC	Ruber	---	Implantado	Foi bloqueado o acesso administrativos por meio de GPO.

RECOMENDAÇÕES SSI	REFERÊNCIAS	NÚCLEO	SERVIDOR	PLANO DE AÇÃO	STATUS	OBSERVAÇÕES TÉCNICAS
Implantar todas as recomendações do TCU referente à gestão de backups	Protocolo: 10051/2020	NITIC	Paulo	Deverá ser implantado no segundo semestre de 2021.	Pacialmente implantado	Falta a implantação de um site backup para que não fique no mesmo local em que os sistemas são hospedados. **Pendente de mudanças elétricas que estão sendo realizadas na sala de TI do 2º andar do Fórum JPA.**
Conformidade com a norma de utilização de senhas	ATO TRT SGP Nº 253/2019	NITIC	Ewerton	Primeiro semestre de 2021	Pacialmente implantado	O openldap, que é a grande restrição desta implantação, deverá ser desativado no fim de 05/2021.
Implantar antivírus em todos servidores, incluindo o ambiente virtualizado		NITIC	Ewerton	NITIC irá avaliar os recursos da nova solução antivirus, a ser adquirida em 2021, em relação a servidores. Prazo a definir.	Não implantado	**Achamos que a recomendação de implantar o antivírus em todos os servidores seja inefetiva, uma vez que nem todos sevidores possuem arquivos de usuários.** Adotar antivírus em todos os servidores geraria um aumento do gasto em recursos computacionais sem grande benefícios ao ambiente. **O próprio PJe, sistema mais crítico e mais acessado da Justiça do Trabalho, que possuem imagens padronizadas e distribuídas a todos os regionais não contém sistema de antivírus.**
Implantar monitoramento de "Arquivos Canário" nos servidores críticos utilizando o Zabbix	https://www.researchgate.net/publication/240496151_CANARY_FILES_GENERATING_FAKE_FILES_TO_DETECT_CRITICAL_DATA_LOSS_FROM_COMPLEX_COMPUTER_NETWORKS ; https://www.zabbix.com/documentation/current/manual/config/items/itemtypes/zabbix_agent	NITIC	Wilberto	Risco aceito pelo CGSI, mediante as observações técnicas apresentadas pelo NITIC.	Risco aceito	**A ideia é boa, mas propícia a muito falso positivo. Ou mesmo pode passar uma falsa sensação de segurança.** Um backup funcional continua sendo uma melhor solução.
Segmentar a rede de servidores da rede de usuários	https://blog.athenasecurity.com.br/segmentacao-de-rede	NITIC	Ricardo	Previsto para o segundo semestre de 2021.	Não implantado	Sugestão que seja tratado como um projeto, visto que envolve a participação de outros núcleos da SETIC.
Implantar solução NAC (Controle de Acesso à Rede)	---	NITIC	Ricardo	Incluído no plano de contratação 2021	Não implantado	Depende de contratação de solução específica.
Implantar solução ou serviço SIEM (Gerenciamento e Correlação de Eventos de Segurança)	https://solutionsreview.com/security-information-event-management/the-10-best-open-source-siem-tools-for-businesses	NITIC	Wilberto	Segundo trimestre de 2021	Pacialmente implantado	Temos já uma solução de correlacionamento de logs que atende bem a demanda, só que está desatualizada. A atualização da soluão está prevista para acontecer no segundo trimestre de 2021.
Implantar solução ou serviço de gestão de vulnerabilidades/pentest	---	SSI	Rodrigo Mafra	Incluído no plano de contratação 2021	Não implantado	Depende de contratação de solução específica. PROAD 19778/2021.
Implantar solução PAM (Gerenciamento de Acessos Privilegiados)	https://zillion.com.br/boas-praticas-gerenciamento-de-acessos-privilegiados	SSI	Rodrigo Mafra	Incluído no plano de contratação 2022	Não implantado	Depende de contratação de solução específica.
Implantar solução WAF (Web Application Firewall)	https://geekflare.com/open-source-web-application-firewall	SSI	Rodrigo Mafra	Incluído no plano de contratação 2022	Não implantado	Depende de contratação de solução específica.

Outras ações realizadas:

- Desativação do protocolo SMBv1 no nosso parque;
- Desativação de alguns sistemas externos vulneráveis;
- Bloqueio total do tráfego originado de alguns países;
- Atualização do sofwate de VPN e Firewall;

RECOMENDAÇÕES SSI	REFERÊNCIAS	NÚCLEO	SERVIDOR	PLANO DE AÇÃO	STATUS	OBSERVAÇÕES TÉCNICAS
- Aumento do nível de inspeção do IPS; - Segmentação da rede da SETIC e NITIC;						