TRIBUNAL REGIONAL ELEITORAL DA BAHIA

ATA - PRE/COMISS2165

ATA DE REUNIÃO nº 02/2023
(CGSI)

1. Identificação da Reunião

Data	Horário		Local	Coordenador da reunião
16/06/2023	11:30	12:00	Virtual	André Luiz C. e Cavalcante

2. Pauta

- Informes Gerais
- NSI 14 – SEI nº 0010636-34.2023.6.05.8000
- Minuta de Portaria de Controle de Acesso às dependências do Tribunal Regional Eleitoral da Bahia – SEI nº 0007125-28.2023.6.05.8000
- Política de gestão de provedores de serviços de TIC – SEI nº 0007118-36.2023.6.05.8000

3. Participantes

Nome	Lotação	Ramal	E-mail
Mª Thaís Pinheiro Habib	SGPRE	7003	mthabib@tre-ba.jus.br
André Luiz Cavalcanti e Cavalcante	STI	7117	andre.cavalcante@tre-ba.jus.br
Josênoel Bastos Pinto	SJU (Substituto)	7157	jbpinto@tre-ba.jus.br
Victor Araujo Mesquita Junior	SPL	7099	vaxavier@tre-ba.jus.br
Arnaldo Torres da Silva	SJR (Substituto)	9150	atsilva@tre-ba.jus.br
Andréa O. Almeida Queiroz	ASSGSI	9287	aoalmeida@tre-ba.jus.br

4. Informes

Não houve

5. Discussão da pauta

	DESCRIÇÃO/DECISÃO	RESPONSÁVEL
1	Informações Gerais **CONSIDERAÇÕES:** • - SEI nº 0002758-92.2022.6.05.8000 - prorrogação do prazo final da *a10 - Segurança da Informação no TRE-BA: Planejamento, Capacitação, Implantação e Certificação* para 2024.2 foi aprovada pelo Conselho de Governança na Reunião de Análise da Estratégia - RAE, realizada em 30/05/2023;	CGSI

	• SEI nº 0004866-60.2023.6.05.8000 - questionário eletrônico do Ranking da Transparência 2023 – manifestar ciência da necessidade de manter os dados atualizados no portal da transparência; • NSI 012 – USO DE REDES SOCIAIS - 0138630-50.2020.6.05.8000 – manifestar ciência; • relatório de incidentes cibernéticos referente ao 1º trimestre/2023 - SEI nº 0005800-18.2023.6.05.8000 – Em 04/03/23, foram registrados ataques via Internet aos Firewall SonicWALL dos SAC da Capital, causando lentidão nos acessos. A providência adota foi o bloqueio dos acessos via SSH (protocolo usado para fazer alterações de configurações) dos firewall. • ciência do mapa estratégico – SEI nº 0003984-35.2022.6.05.8000 **DECISÃO:** Foi dado conhecimento ao CGSI	
2	NSI-14 - SEI nº 0010636-34.2023.6.05.8000 **CONSIDERAÇÕES:** • Pontos principais: – 4.2.1. É estritamente proibido o uso de contas pessoais para armazenar dados institucionais ou dados pessoais de servidores, juízes, colaboradores terceirizados e estagiários. – 4.3.1. Todos os dados armazenados em serviços de computação em nuvem devem ser adequadamente classificados de acordo com a política de classificação de informações da organização. – 4.3.2. Os dados pessoais de servidores, juízes, colaboradores terceirizados e estagiários devem ser tratados como informações sensíveis e devem receber proteção especial. Pelo Secretário da STI foi dito que algumas unidades estavam colocando arquivos de trabalho em contas pessoais e este procedimento não é o adequado. O TRE vai contratar o serviço em nuvem e daí será solicitado que todos os arquivos de trabalho sejam movidos para a conta institucional. André Cavalcante (STI) encaminhou proposta de aprovação da norma, com a ressalva de que esta NSI só será publicada após a realização da contratação do serviço em nuvem. Adicionalmente, propôs a inclusão da observância a IN nº 05/2021 do GSI da Presidência da República sobre segurança da informação. **DECISÃO:** Aprovado por unanimidade	CGSI
3	Minuta de Portaria de Controle de Acesso às dependências do Tribunal Regional Eleitoral da Bahia - SEI nº 0007125-28.2023.6.05.8000 **CONSIDERAÇÕES:** • A Minuta foi elaborada pela ASSEGIN;	CGSI

• Propostas de alteração da ASSGSI:

1. No Art. 6º, alterar a expressão “(II, II I e Centro de Apoio Técnico - CAT)” para “(I, II, III e Centro de Apoio Técnico - CAT)”;

2. No Art. 14 sugiro que os crachás dos estagiários sejam classificados como categoria “permanente”;

3. No intuito de estabelecer diretrizes para implantação de controles de acesso físico relativos à Segurança da Informação e Comunicação, sugiro acrescentar na referida minuta de Portaria o seguinte Capítulo:

DO PERÍMETRO DE SEGURANÇA

Art. 27. O Comitê de Governança de Segurança da Informação (CGSI) deve definir, juntamente com a Assessoria de Inteligência e Segurança Institucional (ASSEGIN), o perímetro de segurança física para proteção das instalações de processamento e armazenamento da informação (datacenter) e das demais áreas que contenham informações críticas ou sensíveis.

Art. 28. As instalações do datacenter devem atender às seguintes diretrizes:

I - paredes fisicamente sólidas, sem brechas nem pontos por onde possa ocorrer uma invasão, portas externas adequadamente protegidas por mecanismos de controle contra acesso não autorizado, sem janelas ou, na impossibilidade, com janelas com proteção externa;

II- videomonitoramento de sua área interna e de seu perímetro;

III - controle de acesso físico às áreas e instalações, sob a responsabilidade da Secretaria de Tecnologia da Informação e Comunicação (STI), utilizando-se dos mecanismos necessários para o controle e registro de data e hora de todas as entradas e saídas, sejam de servidores, visitantes ou prestadores de serviço, permitindo-lhes o acesso, desde que previamente autorizados;

IV- mecanismos de autenticação de multifatores, para as instalações de processamento, armazenamento e comutação de dados, restritas ao pessoal autorizado;

V - portas corta-fogo com sistema de alarme, monitoradas, que funcionem de acordo com os códigos locais, para minimizar os riscos de ameaças físicas potenciais;

VI - sistemas para detecção de intrusos em todas as portas externas e janelas acessíveis;

VII - instalações de processamento e armazenamento das informações que sejam projetadas para minimizar os riscos de ameaças físicas potenciais, tais como fogo, inundação, terremoto, explosão, manifestações civis, contra-ataques maliciosos, fumaça, furtos;

VIII - edifícios que sejam dotados de proteção contra raios e que, em todas as linhas de entrada de força e de comunicações, tenham filtros de proteção contra raios;

IX - alimentações alternativas de energia elétrica e telecomunicações, com rotas físicas diferentes;

X - iluminação e comunicação de emergência;

XI - sistema de controle de temperatura e umidade com recurso de emissão de alertas.

Art. 29. A segurança do conjunto datacenter/gerador e da sala de redundância será realizada por vigilantes contratados sob supervisão da ASEGU.

Art. 30. As diretrizes para proteção das demais áreas que contenham informações críticas ou sensíveis que não estejam armazenadas no datacenter devem ser estabelecidas pela CGSI, observadas as legislações vigentes.

	O Secretário da STI esclareceu que essas normas já se aplicam ao Datacenter, mas precisam ser implantadas para a sala de redundância, uma vez que esta precisou ser transferida para o Ed. Anexo III, em razão da reforma do prédio principal. Em seguida, leu diversos dispositivos da Minuta apresentada pela ASEGIN/ASEGU. Pela Secretária da SGPRE foi proposto que em relação aos estagiários seja acrescido o texto para constar "o estagiário pelo prazo que durar o estágio", nos mesmos moldes do dispositivo relacionado a contratados. Arnaldo Torres (SJR) sugeriu corrigir o art. 20, III, da Minuta para retirar o sigla "CJF". A Assessora da ASSGSI alertou o dispositivo que prevê o pagamento de crachá em caso de perda precisa determinar o valor a ser ressarcido. O Secretário da STI disse que essa análise será feita pela Assessoria Jurídica, pois foge ao escopo deste Comitê. **DECISÃO:** Aprovado por unanimidade.	
4	Política de gestão de provedores de serviços de TIC - SEI nº 0007118-36.2023.6.05.8000 **CONSIDERAÇÕES:** • Propósito e objetivos O propósito desta política é garantir que os provedores de serviço de TIC são gerenciados efetiva e eficientemente, de acordo com e da ISO20000, para habilitar a organização a entregar serviços de alta qualidade a seus clientes. • São quatro as classificações possíveis: • Estratégico – fornecedores que são críticos para o sucesso da organização. São tipicamente fornecedores de longo termo que proveem serviços ou produtos únicos ou de alto valor que são difíceis de substituir; • Tático – fornecedores que proveem produtos ou serviços importantes, mas que não são críticos para o sucesso da organização. São tipicamente mais transacionais em natureza e requerem menos gerenciamento que os fornecedores estratégicos. Devem ser monitorados para garantir que atendem aos padrões de qualidade e geram valor para a organização; • Operacional – fornecedores que proveem produtos ou serviços padronizados que são facilmente substituídos. Requerem gerenciamento e supervisão mínima. Serão regularmente revistos para garantir que continuam atendendo às necessidades e geram valor para a organização. • Comodity – fornecedores de insumos de fácil obtenção, acesso, contínuo e/ou com baixo impacto operacional as atividades finalisticas. • Inventário - Será mantido, pela Secretaria de Tecnologia da InformaçãoeComunicação(STI), um registro de todos os provedores de serviço de TIC • Avaliação e monitoramento • Qualidade • Custo • Entrega • Risco • Descomissionamento e desmobilização	CGSI

	• No que tange ao uso de recursos em nuvem, o repasse de conteúdo armazenado, deverá ocorrer, no mínimo, 30 (trinta) dias antes do término do contrato, sendo que o pagamento da última fatura ficará condicionado ao repasse conteúdo do conteúdo gerado e que poderá ser exigido e cobrado ao prestador. • No que tange aos contratos que envolvem pessoal terceirizado com acesso à rede de dados do Tribunal, os acessos dos profissionais deverão ser removidos em conformidade com a Norma de Segurança da Informação nº 13 (NSI-013). Pelo Secretário da SPL foi alertado que o penúltimo parágrafo do documento trouxe a palavra 'conteúdo' em duplicidade e sugeriu a correção ortográfica do trecho citado. Também destacou que o item 5 fala em 'monitoramento' e posteriormente no tópico 'qualidade, custo e entrega' o termo utilizado é 'monitoração'. Quanto ao 'operacional" sugeriu mudar a expressão 'supervisão mínima' por 'supervisão menos rigorosa'. O Secretário da STI agradeceu as sugestões e disse que as correções serão feitas. **DECISÃO:** Aprovado por unanimidade.	

6. Fechamento da ata:

Esta ata será validada após análise e aceite do conteúdo disposto, que se dará através da assinatura eletrônica dos participantes citados no item 3, no documento correspondente, anexado ao SEI 3375-52.2022.6.05.8000.

Documento assinado eletronicamente por **Arnaldo Torres da Silva**, **Secretário Substituto**, em 26/06/2023, às 12:22, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Andréa Oliveira Almeida Queiroz**, **Assessor**, em 26/06/2023, às 13:21, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **André Luiz Cavalcanti e Cavalcante**, **Secretário**, em 26/06/2023, às 15:17, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Maria Thaís Pinheiro Habib**, **Secretária-Geral da Presidência**, em 27/06/2023, às 11:30, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Victor Araujo Mesquita Xavier**, **Secretário**, em 03/07/2023, às 18:28, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marta Maria Barreiros Gavazza de Brandão Lima**, **Secretário**, em 20/07/2023, às 17:19, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ba.jus.br/autenticar informando o código verificador **2396227** e o código CRC **7A52D49B**.