Plano para Implementação do Manual de Proteção de Infraestruturas Críticas de TIC				
Portaria nº 162/2021 - Anexo IV				
O Manual de Proteção de Infraestruturas Críticas de TIC baseia-se em um conjunto de controles mínimos exigidos compreendidos como pertinentes e condizentes com				
ID	**Item**	**Responsáve**	**Implementação**	**Situação**
1.3	Manter inventário atualizado e preciso de todos os ativos de tecnologia que detenham o potencial de armazenamento ou processamento de informações. Esse inventário deve incluir ativos de hardware, conectados ou não à rede da organização.	STI	Aquisição de ferramenta de gestão de ativos de TIC, adquirida a ferramenta Ivanti. Processo SEI nº 0003288-15.2022.6.08.8000	Concluído
1.5	Garantir que ativos não autorizados sejam removidos da rede ou colocados em quarentena, ou que o inventário seja atualizado em tempo hábil.	STI	Aquisição de ferramenta para verificação de ativos na rede, adquirida a ferramenta Trend Vision One. Processo SEI nº. 0000589-51.2022.6.08.8000	Concluído
2.1	Manter uma lista atualizada de todos os softwares autorizados que sejam necessários à organização para qualquer propósito ou sistema de negócios	STI	Aquisição da ferramenta Ivanti que gerencia os softwares instalados nos ativos. Criação da lista de softwares homologados. Documentação dos softwares desenvolvidos pela CSGIT no confluence. Processo SEI nº 0003288-15.2022.6.08.8000 e 0000582-59.2022.6.08.8000	Concluído
2.2	Garantir que apenas aplicações ou sistemas operacionais atualmente suportados pelo fabricante sejam adicionados ao inventário de softwares autorizados. Softwares sem suporte devem ser indicados no sistema de inventário.	STI	Aquisição de ferramenta para controle de atualizações de software. Adquirida a ferramenta Ivanti. Processo SEI nº 0003288-15.2022.6.08.8000	Concluído
2.6	Garantir que qualquer software não autorizado seja removido, ou que o inventário seja atualizado em tempo hábil.	STI	Aquisição de ferramenta para softwares instalados nos ativos de TIC. Adquirida a ferramenta Ivanti. Processo SEI nº 0003288-15.2022.6.08.8000	Concluído
3.4	Implantar ferramentas de atualização automatizada de software, de forma a garantir que os sistemas operacionais sejam executados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	STI	Aquisição de ferramenta para controle de atualizações de software. Adquirida a ferramenta Ivanti. Processo SEI nº 0003288-15.2022.6.08.8000	Concluído

3.5	Implantar ferramentas de atualização automatizada de software de forma a garantir que os softwares de terceiros em todos os equipamentos sejam utilizados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	STI	Aquisição de ferramenta para controle de atualizações de software. Adquirida a ferramenta Ivanti. Processo SEI nº 0003288-15.2022.6.08.8000	Concluído
4.2	Antes de ativar qualquer novo ativo, modificar todas as senhas padrão de forma consistente com contas de nível administrativo.	STI	As contas administrativas são adiciondas ao cofre de senhas adquirido pelo tribunal. Processo SEI nº. 0000662-23.2022.6.08.8000	Concluído
4.3	Garantir que todos os usuários com contas administrativas utilizem uma conta secundária para atividades de privilégio elevado. Essa conta deve ser utilizada somente para atividades administrativas e não para navegação na internet, correio eletrônico ou atividades similares.	STI	Foram criadas contas secundárias para a relização de atividades administrativas. NSI 009	Concluído
5.1	Manter padrões documentados de configuração segura para todos os sistemas operacionais e softwares autorizados.	STI	Está em andamento contratação de serviços nacionais de cibersegurança em que poderão ser solicitados modelos de configuraçõe seguras para implementação nos equipamentos. Processo SEI nº 0001459-62.2023.6.08.8000	Em desenvolvimento, previsão de conclusão em julho 2024
6.2	Garantir que o log local tenha sido habilitado em todos os sistemas e dispositivos de rede.	STI	Configurada ferramenta centralizadora de logs para a qual os servidores enviam os logs. Ferramenta gratuita Graylog. NSI 007	Concluído
7.1	Garantir que apenas navegadores web e clientes de e-mail suportados possam ser executados na organização, idealmente utilizando apenas a versão mais recente disponibilizada pelo fabricante.	STI	Os usuários não possuem permissão de instalação de aplicativos nas máquinas, apenas a equipe técnica pode realizar instalações e apenas para softwares homologados. Conforme NSI 009 - Uso aceitável de recursos de TI	Concluído
7.6	Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos	STI	Aquisição de firewall de rede e configuração de políticas de liberação de acesso. Processo SEI nº 0002068-50.2020.6.08.8000	Concluído

8.2	Garantir que o software antimalware atualize seu motor de varredura e base de assinaturas de malware de forma regular.	STI	As atualizações do software antimalware são realizadas por meio de políticas de segurança de forma automática. Processo SEI nº. 0000589-51.2022.6.08.8000	Concluído
8.4	Configurar os dispositivos de forma que automaticamente conduzem uma varredura antimalware em mídias removíveis assim que sejam inseridas ou conectadas.	STI	Configurada a desabilitação de execução automática de mídias removíveis e a varredura automática pela ferramenta antimalware. É vetado o uso de mídias removíveis nos computadores do TRE-ES, conforme NSI 009 - uso aceitável de recursos de TI	Concluído
8.5	Configurar os dispositivos para que não autoexecutem conteúdo em mídia removível	STI	Configurada a desabilitação de execução automática de mídias removíveis e a varredura automática pela ferramenta antimalware. É vetado o uso de mídias removíveis nos computadores do TRE-ES, conforme NSI 009 - uso aceitável de recursos de TI	Concluído
9.1	Garantir que todos os dados dos sistemas tenham cópias de segurança (backups) realizados automaticamente de forma regular.	STI	Foi atualizada a política de backup do TRE-ES e o procedimento de backups e restores. O procedimento contém a frequência em que os backups são executados. NSI 008	Concluído
9.2	Garantir que todos os sistemas chave da organização tenham suas cópias de segurança (backups) realizadas como um sistema completo, por meio de processos como a geração de imagem, de forma a permitir uma rápida recuperação de todo o sistema.	STI	São realizados backups completos de sistemas, conforme estabelecido no procedimento de backups do TRE-ES. NSI 008	Concluído
9.4	Garantir que as cópias de segurança (backups) sejam apropriadamente protegidas por meio de segurança física ou criptografia quando forem armazenadas, assim como quando são movimentadas através da rede. Isso inclui cópias de segurança (backups) remotas e em serviços de nuvem.	STI	Os backups são guardados em rede separada para evitar que sejam afetados por ameaças à rede do TRE-ES. NSI 008	Concluído
9.5	Garantir que todas as cópias de segurança contenham ao menos uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.	STI	Os backups são guardados em rede separada não acessível pela rede principal do TRE-ES. NSI 008	Concluído

10.1	Manter um inventário de todas as informações sensíveis armazenadas, processadas ou transmitidas pelos sistemas de tecnologia da organização, incluindo aquelas localizado nas próprias dependências da organização ou em um provedor de serviços remoto.	STI	Mapeamento realizado pela equipe da LGPD	Concluído
10.2	Remover da rede dados sensíveis ou sistemas não acessados regularmente pela organização. Tais sistemas devem ser utilizados somente como sistemas isolados (desconectados da rede) pela unidade de negócios que necessite de acesso ocasional, ou devem ser completamente virtualizados e desligados até que sejam necessários.	STI	É realizado o desligamento dos sistemas não utilizados regularmente, realizando seu religamento apenas por solicitação do usuário. Sistemas que não são mais utilizados são desligados definitivamente. Ex. 0003947-24.2022.6.08.8000, 0001194-60.2023.6.08.8000	Concluído
10.4	Utilizar ferramentas aprovadas para criptografia total dos discos rígidos de todos os dispositivos móveis	STI	Utilização da ferramenta Trend. Processo SEI nº 0000589-51.2022.6.08.8000	Concluído

Plano para Implementação da Gestão de Identidade e Controle de Acesso.				
Portaria nº 162/2021 - Anexo VI				
Este Manual estabelece as diretrizes principais para a gestão de identidades e credenciais eletrônicas bem como para o controle de acessos aos sistemas, serviços e				
ID	**Item**	**Responsáve**	**Implementação**	**Situação**
2.1	Formalizar Política de Gestão de Identidade e Controle de Acesso	CSI	Ata CSI 27 -06/12/2023, processo SEI nº 0006783-33.2023.6.08.8000	Concluído
2.2	Aplicar critérios de padronização de nome de usuário e conta de email	SGIR	Revisão e Atualiação do AD do Órgão	Concluído
2.3	Efetuar processo de revisão para identificar privilégios excessivos de usuários, administradores de TI e de contas de serviço	SGIR	Processo de aquisição do Varonis: 0001607-73.2023.6.08.8000	Concluído
2.4	Definir e utilizar um processo para a revogação de direitos de acesso, desabilitando imediatamente as contas no momento do término do vínculo ou da alteração das responsabilidades de um servidor ou prestador de serviços.	STI	Estagiários: 0001275-72.2024.6.08.8000 Inativos: 0001299-03.2024.6.08.8000 Terceirizados: 0003153-32.2024.6.08.8000 Magistrados e requisitados: 0001238-45.2024.6.08.8000 Servidores: 0001241-97.2024.6.08.8000	Concluído

2.5	Manter um inventário de cada um dos sistemas de autenticação da organização, incluindo aqueles internos ou em provedores de serviços internos.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 8.3. A área técnica de segurança cibernética deverá manter o inventário dos sistemas de autenticação do TRE-ES, abrangendo os internos e aqueles hospedados em provedores remotos".	Concluído
2.6	Adotar modelo de controle de acesso baseado em funções (RBAC).	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 7.3 O modelo de controle de acesso será, preferencialmente, fundamentado no controle de acesso baseado em papéis (RBAC) que, basicamente, consiste em atribuir-se uma ou mais "funções" a cada usuário, concedendo permissões diferentes a cada função.	Concluído
2.7	Registrar em logs acessos, operações e período para fins de auditoria.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 13.6. Manter, para fins de auditoria, registro dos acessos, das operações e dos respectivos períodos;	Concluído
2.8	Garantir que todas as contas tenham uma data de expiração de senha e que isso seja configurado e monitorado.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 13.2. Forçar as mudanças de senha a intervalos regulares de, no máximo, 6 (seis) meses, conforme necessidade;	Concluído

2.9	Gerenciar acessos e ações executadas com credenciais privilegiados, não utilizando credenciais genéricas e de uso compartilhado.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 11.2. O acesso privilegiado deve ser concedido ao usuário por meio de credenciais de acesso exclusivas para este fim, distintas das credenciais de acesso concedidas a tal usuário para a realização de suas atividades normais de negócio. Processo que adiquiriu a ferramenta de gestão de acesso privilegiado: 0000662-23.2022.6.08.8000	Concluído
2.10	Criptografar ou embaralhar (*hash*) com a utilização de *salt* as credenciais de autenticação armazenadas.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 13.4. Criptografar ou embaralhar (hash) com salt as credenciais de autenticação armazenadas.	Concluído
2.11	Utilizar criptografia no canal de comunicação ao trafegar credenciais de acesso.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 8.1.3. Mecanismo de tráfego criptografado de senhas e dados pessoais	Concluído
2.14	Configurar o acesso a todas as contas por meio da menor quantidade de pontos de autenticação centralizados possível, incluindo sistemas de rede, segurança e sistemas em nuvem	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 9. Da concessão do acesso às redes, aos sistemas internos e aos serviços informatizados: 9.1. A gestão de contas e do controle de acesso dar-se-á de forma centralizada, por meio de serviço de diretório, ou provedor SSO, onde houver suporte.	Concluído

2.15	Garantir que todas as contas (*usernames*) e senhas sejam transmitidas em rede utilizando canais criptografados.	STI	Norma de Implantação Segura de Sistemas (NSI-005): 8.1.3. Mecanismo de tráfego criptografado de senhas e dados pessoais. Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 8.1.3. Mecanismo de tráfego criptografado de senhas e dados pessoais	Concluído

2.16	Manter um inventário de todas as contas organizadas por sistema de autenticação.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 8. Do inventário de contas de acesso 8.1. Deverá ser estabelecido e mantido atualizado um inventário de todas as contas gerenciadas, contendo data de início e término, incluindo: 8.1.1. contas de usuário 8.1.2. contas de administrador; e 8.1.3. contas de serviço. 8.2. O inventário das contas de usuário e de administrador deverá conter, no mínimo, o nome completo da pessoa, o nome de usuário de rede, data de início de acesso, data de término de acesso (quando disponível) e a sua unidade de lotação, enquanto o das contas de serviço indicará ao menos a unidade gestora, as datas de revisão e o propósito. 8.3. A área técnica de segurança cibernética deverá manter o inventário dos sistemas de autenticação do TRE-ES, abrangendo os internos e aqueles hospedados em provedores remotos."	Concluído
2.17	Desabilitar contas, em vez de excluí-las, visando à preservação de trilhas de auditoria.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 7.5.3. As contas deverão ser desabilitadas, em vez de excluídas, para preservação de trilhas de auditoria".	Concluído

2.18	Desabilitar qualquer conta que não possa ser associada a um processo de negócio ou a um usuário.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 10.3. As contas de usuários deverão ser revisadas trimestralmente para avaliar se todas as contas ativas permanecem autorizadas".	Concluído
2.19	Desabilitar automaticamente contas não utilizadas após um período de inatividade pré-definido.	STI	Norma de Gestão de Identidade e Controle de Acesso Lógico (NSI-011): 10.4. Usuários que não realizarem o acesso à rede de dados por mais de 60 (sessenta) dias, terão o seu acesso bloqueado temporariamente até que solicitem o reestabelecimento do acesso por meio de ferramenta de abertura de chamados".	Concluído
2.20	Bloquear automaticamente as estações de trabalho após um período de inatividade pré-definido	STI	Norma de Uso Aceitável de Recursos de TI (NSI-009): 8.2.6. Bloqueio automático de tela por inatividade, com restauração da sessão somente por meio do uso de credencial de acesso válida."	Concluído
2.21	Monitorar tentativas de acesso a contas desativadas, por meio de logs de auditoria.	STI	Processo de aquisição do Varonis: 0001607-73.2023.6.08.8000	Concluído
2.22	Segregar as redes de comunicação a depender do grupo dos serviços, sistemas ou usuários.	STI	Não foi identificada necessidade de segregação devido ao porte até o momento.	Concluído
2.23	Implementar controles de acesso físico aos ativos de TIC.	STI	NSI- 003 - TRE-ES - Gestão de Acesso Físico	Concluído