PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DO MANUAL DE GESTÃO DE IDENTIDADES E CONTROLE DE ACESSO

	5W2H								GUT			OBSERVAÇÕES
Controle	Ação/Atividade	What (O que fazer?)	Why (Por que fazer?)	Who (Quem fará?)	When (Quando?)	Where (Onde?)	How (Como fazer?)	How much (Quanto custará?)	Gravidade	Urgência	Tendência	
1	Estabelecimento de padrão de identidade do Tribunal	Definir critérios para padronização de nome de usuário e conta de e-mail	Para garantir consistência e segurança na identificação dos usuários	Equipe de TI	Já implementado	Na infraestrutura local de TIC	Realizar reuniões para identificar os critérios e documentar o padrão de identidade	Baixo	2	2	1	1) Solução já implementada
2	Implementação do princípio de privilégio mínimo e segregação de funções	Avaliar e revisar as políticas de acesso para garantir que apenas as autorizações necessárias sejam concedidas	Para reduzir os riscos de vazamento de informações e evitar acessos indevidos	Equipe de TI	Em até 45 dias	Na infraestrutura local de TIC	Revisar as políticas de acesso existentes, identificar áreas de melhoria e implementar mudanças conforme necessário	Médio	4	3	4	1) Não haverá custo orçamentário/financeiro, somente esforço das equipes envolvidas;
3	Estabelecimento de processo de solicitação, gerenciamento e revogação de contas de acesso	Definir procedimentos claros e responsáveis pelo ciclo de vida das contas de usuário	Para garantir que o acesso seja concedido e revogado de forma apropriada, reduzindo o risco de acesso não autorizado	Equipe de Segurança da Informação	Em fase final de aprovação	Na infraestrutura local de TIC	Documentar procedimentos de solicitação, gerenciamento e revogação de contas e treinar os usuários sobre esses processos	Médio	4	3	3	1) Nova PARTIC atende. 2) Precisa ser aprovada e publicada.
4	Utilização de login único para acesso a serviços de diretório corporativo e sistemas	Implementar um sistema de login único para garantir uma experiência de usuário consistente e segura	Para simplificar o acesso do usuário e garantir a integridade das credenciais	Equipe de TI	Dependerá da solução que será adotada	Na infraestrutura local de TIC	Pesquisar e implementar soluções de login único compatíveis com os sistemas existentes	Alto	3	3	2	1) Será necessária análise de mercado sobre às soluções; 2) Poderá necessitar investimento em contratação; 3) Outro projeto deverá ser aberto e outros prazos estabelecidos.
5	Adoção de modelo de controle de acesso baseado em funções (RBAC)	Implementar um modelo de controle de acesso que conceda privilégios de acordo com as funções do usuário	Para garantir que os usuários tenham acesso apenas ao que é necessário para realizar suas funções	Equipe de TI	Em até 60 dias	Na infraestrutura local de TIC	Mapear as funções dos usuários e definir os privilégios de acesso de acordo com suas responsabilidades	Médio	3	3	2	1) Não haverá custo orçamentário/financeiro, somente esforço das equipes envolvidas; 2) Nova PARTIC prevê ações necessárias.
6	Criação de processos de verificação de identidade nas interações entre sistemas	Estabelecer procedimentos para garantir a identidade dos usuários durante as interações entre sistemas	Para garantir que apenas usuários autorizados tenham acesso aos sistemas	Equipe de TI	Em até 60 dias	Na infraestrutura local de TIC	Implementar métodos de verificação de identidade, como autenticação multifator e certificados digitais	Médio	3	2	2	1) Implementar a solução Cisco DUO nos sistemas de acesso que forem possíveis.
7	Registro de trilhas de auditoria	Implementar um sistema de registro de auditoria para rastrear acessos a sistemas de informação e operações realizadas	Para fins de conformidade regulatória, investigações de segurança e monitoramento de atividades suspeitas	Equipe de Segurança da Informação	Dependerá da solução que será adotada	Na infraestrutura local de TIC	Configurar sistemas de registro de auditoria para capturar e armazenar informações sobre acessos e operações realizadas	Alto	3	3	3	1) Será necessária análise de mercado sobre às soluções; 2) Poderá necessitar investimento em contratação; 3) Outro projeto deverá ser aberto e outros prazos estabelecidos.
8	Definição de requisitos de senhas	Estabelecer critérios para tamanho, complexidade e expiração de senhas	Para garantir que as senhas sejam robustas e seguras contra ataques de força bruta e acesso não autorizado	Equipe de TI	Já implementado	Na infraestrutura local de TIC	Definir políticas de senha que incluam requisitos mínimos de comprimento, caracteres especiais e períodos de expiração	Baixo	2	2	1	1) Solução já implementada.
9	Adoção de autenticação multifator (MFA)	Implementar autenticação multifator para fortalecer a segurança das contas	Para mitigar o risco de acesso não autorizado mesmo em caso de comprometimento das credenciais de usuário	Equipe de TI + SI	Em até 60 dias	Na infraestrutura local de TIC	Avaliar e implementar soluções de autenticação multifator compatíveis com os sistemas existentes	Médio	5	4	5	1) Implementar a solução Cisco DUO nos sistemas de acesso que forem possíveis.
10	Unificação de plataformas de autenticação, autorização e auditoria	Consolidar as plataformas de autenticação, autorização e auditoria para simplificar a gestão e garantir a consistência	Para reduzir a complexidade, melhorar a eficiência e garantir a uniformidade nas políticas de segurança	Equipe de TI	Dependerá da solução que será adotada	Na infraestrutura local de TIC	Avaliar as plataformas existentes, identificar oportunidades de consolidação e migrar para soluções unificadas, se aplicável	Alto	2	2	2	1) Será necessária análise de mercado sobre às soluções; 2) Poderá necessitar investimento em contratação; 3) Outro projeto deverá ser aberto e outros prazos estabelecidos.
11	Estabelecimento de regras para acesso remoto	Definir diretrizes e procedimentos para acesso remoto seguro aos sistemas e serviços	Para proteger os sistemas e dados contra ameaças externas e garantir a continuidade dos negócios em situações de emergência	Equipe de Segurança da Informação	Dependerá da solução que será adotada	Na infraestrutura local de TIC	Desenvolver políticas e procedimentos para acesso remoto, incluindo autenticação, criptografia e monitoramento de atividades	Alto	5	5	5	1) Será necessária análise de mercado sobre às soluções; 2) Poderá necessitar investimento em contratação; 3) Outro projeto deverá ser aberto e outros prazos estabelecidos.
12	Rastreabilidade de acessos e ações executadas por administradores de TI	Implementar sistemas de registro de trilhas de auditoria para monitorar as ações dos administradores de TI	Para garantir a prestação de contas e facilitar a investigação de incidentes de segurança	Equipe de Segurança da Informação	Já implementado	Na infraestrutura local de TIC	Configurar sistemas de registro de trilhas de auditoria para capturar e armazenar ações realizadas por administradores de TI	Médio	4	4	2	1) Solução já implementada (VARONIS).
13	Utilização de mecanismos seguros de criptografia	Implementar protocolos de criptografia para proteger o armazenamento e transmissão de credenciais de acesso	Para proteger as credenciais contra acesso não autorizado e garantir a integridade dos dados	Equipe de Segurança da Informação	Dependerá da solução que será adotada	Na infraestrutura local de TIC	Avaliar e implementar protocolos de criptografia adequados para armazenamento e transmissão de credenciais de acesso	Alto	5	5	4	1) Será necessária análise de mercado sobre às soluções; 2) Poderá necessitar investimento em contratação; 3) Outro projeto deverá ser aberto e outros prazos estabelecidos.
14	Segregação de redes conforme grupo de serviços, sistemas ou usuários	Dividir as redes de acordo com a função e sensibilidade dos dados para minimizar o risco de comprometimento	Para isolar e proteger os sistemas e dados sensíveis contra ataques externos e internos.	Equipe de TI	Já implementado	Na infraestrutura local de TIC	Avaliar a arquitetura de rede existente, identificar segmentos relevantes e implementar medidas de segregação de acordo com as diretrizes	Baixo	3	1	1	1) Solução já implementada.
15	Controle do acesso físico aos ativos de TIC	Implementar medidas de controle de acesso físico para proteger os ativos de TIC contra acesso não autorizado.	Para prevenir o acesso físico não autorizado aos equipamentos e infraestrutura crítica de TI.	Equipe de TI	Já implementado	Na infraestrutura local de TIC	Instalar sistemas de controle de acesso físico, como fechaduras eletrônicas e sistemas de monitoramento, nos locais relevantes	Alto	3	1	1	1) Solução já implementada.
16	Implementação de controles de acesso proporcionais à classificação da informação	Implementar controles de acesso diferenciados com base na classificação de dados para garantir a proteção adequada	Para garantir que apenas usuários autorizados tenham acesso a informações sensíveis e confidenciais	Equipe de TI + SI	Dependerá da solução que será adotada	Na infraestrutura local de TIC	Classificar os dados conforme sua sensibilidade e implementar controles de acesso de acordo com as diretrizes de classificação	Alto	4	3	4	1) Será necessária análise de mercado sobre às soluções; 2) Poderá necessitar investimento em contratação; 3) Outro projeto deverá ser aberto e outros prazos estabelecidos.
17	Monitoração dos acessos e tentativas de acesso	Implementar sistemas de monitoramento para registrar e alertar sobre acessos e tentativas de acesso não autorizados	Para identificar e responder rapidamente a tentativas de acesso não autorizado e atividades suspeitas	Equipe de TI + SI	Já implementado	Na infraestrutura local de TIC	Configurar sistemas de monitoramento de segurança para registrar e alertar sobre acessos e tentativas de acesso não autorizados	Alto	4	4	3	1) Solução já implementada (VARONIS + DARKTRACE + TRENDMICRO).

*** Os prazos estimados poderão variar para mais ou para menos, conforme a disponibilidade operacional das equipes diretamente responsáveis pela ação/atividade**

**** A previsão para início das atividades e ações é em Março/2025**

***** Somente as atividade e ações que tem o custo estimado como ALTO, que poderão precisar de orçamento financeiro que possam ser executadas**