PLANO DE AÇÃO Nº 0610062 / 2023 - PRESI/DG/STI/ASPGOVTI

Plano de Ação

Implementação do Manual de Referência – Gestão de Identidade e de Controle de Acessos

IMPLEMENTAÇÃO DO MANUAL DE REFERÊNCIA – GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS

1. APRESENTAÇÃO

Os órgãos do Poder Judiciário devem efetuar a gestão de identidade e o controle de acessos de seus usuários, sejam magistrados ou magistradas, servidores ou servidoras, prestadores ou prestadoras de serviços, usuários ou usuárias dos serviços e equipe de TIC.

2. PADRÕES MÍNIMOS DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A gestão de riscos em âmbito corporativo é essencial para a boa governança, uma vez que fornece garantia razoável para que os objetivos organizacionais sejam alcançados. A integração da gestão de riscos à governança corporativa é apontada em diversos modelos de melhores práticas.

3. OBJETIVO GERAL

Implementação dos itens do Manual de Referência - Gestão de Identidade e de Controle de Acessos, constantes do anexo VI, da Portaria CNJ n. 162/2021.

4. REFERÊNCIA NORMATIVA

- Resolução CNJ no 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Portaria CNJ n. 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário;
- Portaria CNJ n. 249/2020, que designa os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);
- Portaria TRE/AC n. 165/2023, que institui o Protocolo Protocolo de Prevenção de

Incidentes Cibernéticos;

- Portaria TRE/AC n. 163/2023, que institui o Protocolo de Investigação para Ilícitos Cibernéticos;
- Portaria TRE/AC n. 156/2023, que institui o Protocolo Protocolo de Gerenciamento de Crises Cibernéticas;
- CIS Controls v7.1 - Center for Internet Security Critical Security Controls for Effective Cyber Defense20 - publicação de diretrizes de práticas recomendadas para segurança cibernética.
- MITRE ATT&CK , modelos e metodologia de ameaças;
- Norma ABNT NBR ISO/IEC 27001:2013 - Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Essa norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.
- NIST SP 800-53 - catálogo de controles de segurança e privacidade para os sistemas de informações e organizações para proteger operações e ativos organizacionais, indivíduos e outras organizações de um conjunto diversificado de ameaças.

5. CAMPO DE APLICAÇÃO

Tribunal Regional Eleitoral e Zonas Eleitorais do Estado do Acre.

6. FINALIDADE E METAS

Estabelecer as diretrizes estratégicas para aplicação dos controles de Gestão de Identidade e de Controle de Acessos.

A aplicação dos checklist implementado pelo TRE/AC, devem ser realizado anualmente, como o estabelecimento do nível de maturidade a cada nova avaliação. O objetivo é possibilitar a melhoria contínua de normativos, processos e iniciativas em segurança cibernética do Tribunal.

7. PADRÕES MÍNIMOS DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Os padrões mínimos de Gestão de Riscos de Segurança são um conjunto de diretrizes que fornecem uma estrutura para a implementação de um programa de gestão de riscos eficaz. Esses padrões são geralmente baseados nas melhores práticas internacionais, conforme normas acima citadas.

8. ORÇAMENTO

As despesas relacionadas a esse plano que por ventura venham a ter gastos, serão providas com recursos provenientes do orçamento corrente do TRE-AC.

9. PLANO DE AÇÃO PARA UTILIZAÇÃO DOS CONTROLES PARA PREVENÇÃO E MITIGAÇÃO

DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL

Plano de Ação 2023-2024

Gestão de identidade e controle acesso (Referência - CIS Controls v7.1)					
Ação		**Setor Responsável**	**Previsão de conclusão**	**Situação**	Maturidade
01	Formalizar Política de Gestão de Identidade e Controle de Acesso em conformidade com as diretrizes previstas neste Manual e boas práticas de segurança.	SCSEG	dez/2023	Pendente de revisão	3
02	Aplicação dos critérios de padronização de nome de usuário e de conta de e-mail.	SCSEG	dez/2023	Pendente de revisão	3
03	Realizar processo de revisão para identificar privilégios excessivos de usuários, administradores de TI e de contas de serviço.	SCSEG	dez/2023	Implementado	4
04	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.	SCSEG	dez/2023	Implementado	4
05	Manter um inventário de cada um dos sistemas de autenticação da organização, incluindo aqueles internos ou em provedores de serviços remotos.	SCSEG	dez/2023	Em andamento	2
06	Adotar modelo de controle de acesso baseado em funções (RBAC).	SCSEG	dez/2023	Não iniciado	1
07	Registrar em logs acessos, operações e período para fins de auditoria	SCSEG	dez/2023	Implementado	4

08	Garantir que todas as contas tenham uma data de expiração de senha e que isso seja configurado e monitorado.	SCSEG	dez/2023	Finalizado	5
09	Gerenciar acessos e ações executadas com credenciais privilegiados, não utilizando credenciais genéricas e de uso compartilhado.	SCSEG	dez/2023	Implementado	3
10	Criptografar ou embaralhar (hash) com a utilização de salt as credenciais de autenticação armazenadas.	SCSEG	dez/2023	Não iniciado	1
11	Utilizar criptografia no canal de comunicação ao trafegar credenciais de acesso.	SCSEG	dez/2023	Pendente de revisão	3
12	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.	SCSEG	dez/2023	Em andamento	2
13	Garantir que todas as contas (usernames) e senhas sejam transmitidas em rede utilizando canais criptografados	SCSEG	dez/2023	Pendente de revisão	3
14	Manter um inventário de todas as contas organizadas por sistema de autenticação.	SCSEG	dez/2023	Pendente de revisão	3
15	Desabilitar contas, em vez de excluí-las, visando à preservação de trilhas de auditoria.	SCSEG	dez/2023	Finalizado	5
16	Desabilitar qualquer conta que não possa ser associada a um processo de negócio ou a um usuário.	SCSEG	dez/2023	Finalizado	5

17	Desabilitar automaticamente contas não utilizadas após um período de inatividade pré-definido.	SCSEG	dez/2023	Não iniciado	1
18	Bloquear automaticamente as estações de trabalho após um período de inatividade pré-definido.	SCSEG	dez/2023	Finalizado	5
19	Monitorar tentativas de acesso a contas desativadas, por meio de logs de auditoria.	SCSEG	dez/2023	Implementado	4
20	Segregar as redes de comunicação a depender do grupo dos serviços, sistemas ou usuários.	SCSEG	dez/2023	Implementado	4
21	Implementar controles de acesso físico aos ativos de TIC.	SCSEG	dez/2023	Finalizado	5

9. Tabela de Referência para definição de Maturidade do Tribunal

Definição	Descrição
1 – Não observado ou inicial	Fator não foi demonstrado claramente.
2 – Maturidade baixa ou em desenvolvimento	Fator demonstrado claramente, mas não integrado.
3 – Maturidade média ou definida	Fator suficientemente demonstrado, integrado, mas não está medido.
4 – Maturidade alta ou gerenciada	Fator constantemente demonstrado, integrado, gerenciado, mas não possui melhoria contínua.
5 – Melhoria contínua ou otimizada	Fator complemente demonstrado, integrado, gerenciado e continuamente melhorado.

10. PREMISSAS E RESTRIÇÕES DO OBJETO

- Apoio da Administração, Diretoria Geral e Secretarias do Tribunal

- Disponibilidade orçamentária;

- Cumprimento dos prazos previamente fixados para realização das tarefas pelas unidades envolvidas;

- Comprometimento de todas as áreas impactadas;

Controle de versões:

Plano de Ação 2023-2025

versão preliminar 1.1

Responsável: STI/ASPGOVTI/ACSEG