



SENADO FEDERAL
Auditoria



Sumário Executivo

Foram objetos de análise nesta auditoria operacional, os processos de trabalho e ferramentas implementados pela Tecnologia da Informação - TI do Senado Federal relacionados à Segurança da Informação-SegInfo e Segurança Cibernética-SegCiber.

Baseado no Plano Anual de Auditoria Interna - PAInt, bem como nas recomendações do Tribunal de Contas da União - TCU constantes no Acórdão 1.768/2022-TCU-Plenário quanto à implementação urgente de controles críticos e medidas de segurança cibernética observando-se boas práticas como as preconizadas pelo *Center for Internet Security-CIS* e pela norma técnica ABNT NBR ISO/IEC 27002:2013, o presente trabalho buscou avaliar os controles que as unidades de TI Secretaria de Tecnologia da Informação - Prodasen, Secretaria de Engenharia de Comunicação - SEC/SECOM e Coordenação de Tecnologia da Informação do Instituto Legislativo Brasileiro - COTIN/ILB adotam em relação à gestão de contas (credenciais), controle de acesso e proteções de *endpoints* (e-mail, navegador web e defesas contra *malware*).

Após avaliar em que medida essas áreas do Senado Federal buscam garantir a proteção das informações e dos ativos de TI por meio de gestão de contas, controles de acesso e proteções de *endpoints*, a auditoria identificou dois achados, listados a seguir com as respectivas recomendações:

Achado	Recomendação
1 - Necessidade de melhoria nos processos e ferramentas para gestão das "Contas Privilegiadas" (administrador, contas de serviço e contas de aplicativos).	Recomenda-se ao Prodasen, à SEC/SECOM e à COTIN/ILB aprimorar a gestão sobre contas de acesso privilegiado , considerando, na medida do possível, os itens "a"; "b"; "c"; e "d" constantes deste respectivo achado no capítulo 7 deste relatório.
2 - Necessidade de melhoria nos processos de revogação de acessos após mudanças de lotação e/ou função.	Recomenda-se ao Prodasen aprimorar os processos relativos à revogação de acessos após mudanças de lotação e/ou função , considerando, na medida do possível, os itens "a" e "b", constantes deste respectivo achado no capítulo 7 deste relatório.

