SIG-PPSI

CONTROLES Cibersegurança

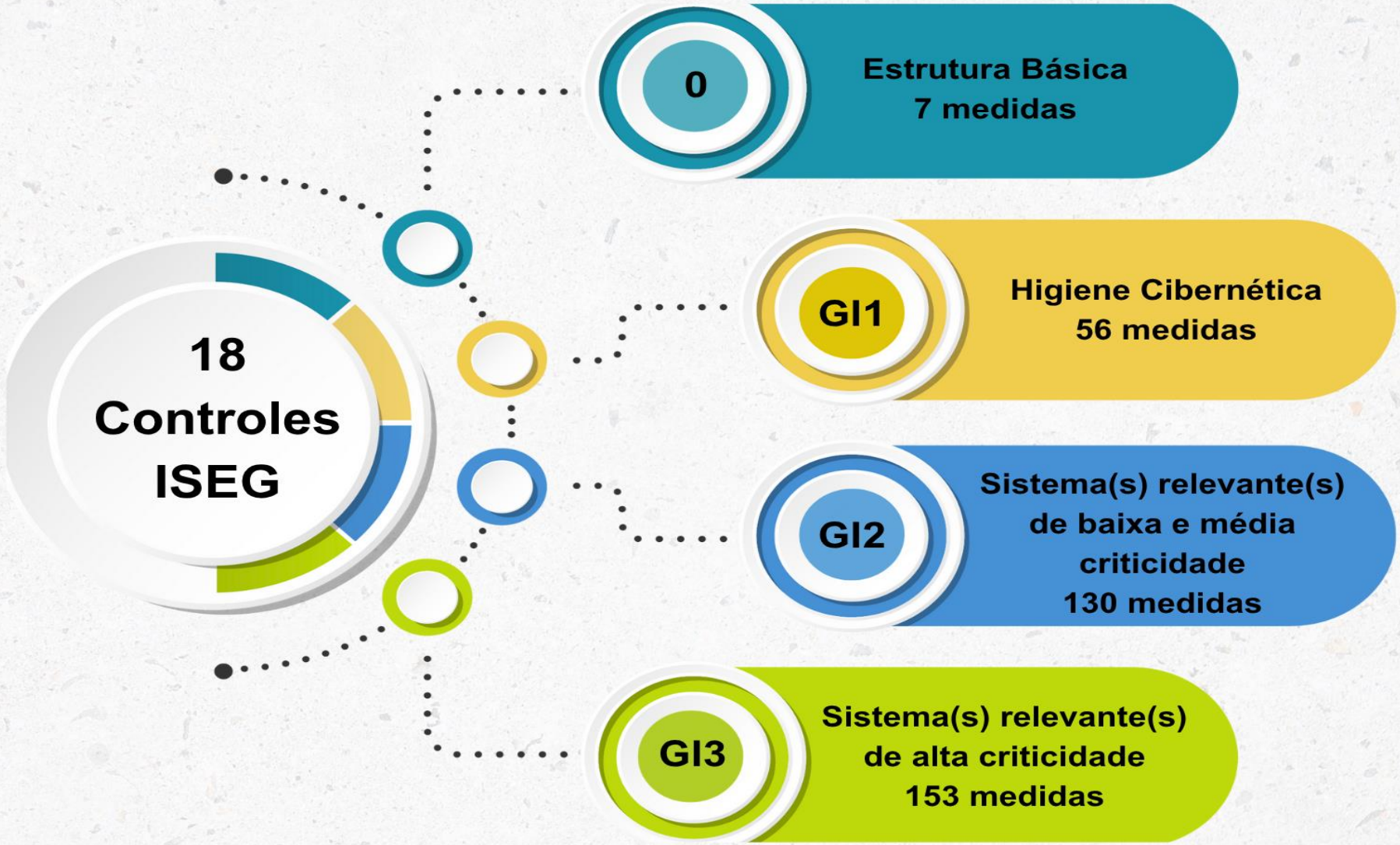
Carla Pires | Fabiana Cardoso | Flávio Testa
ppsi.sgd@gestao.gov.br

gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

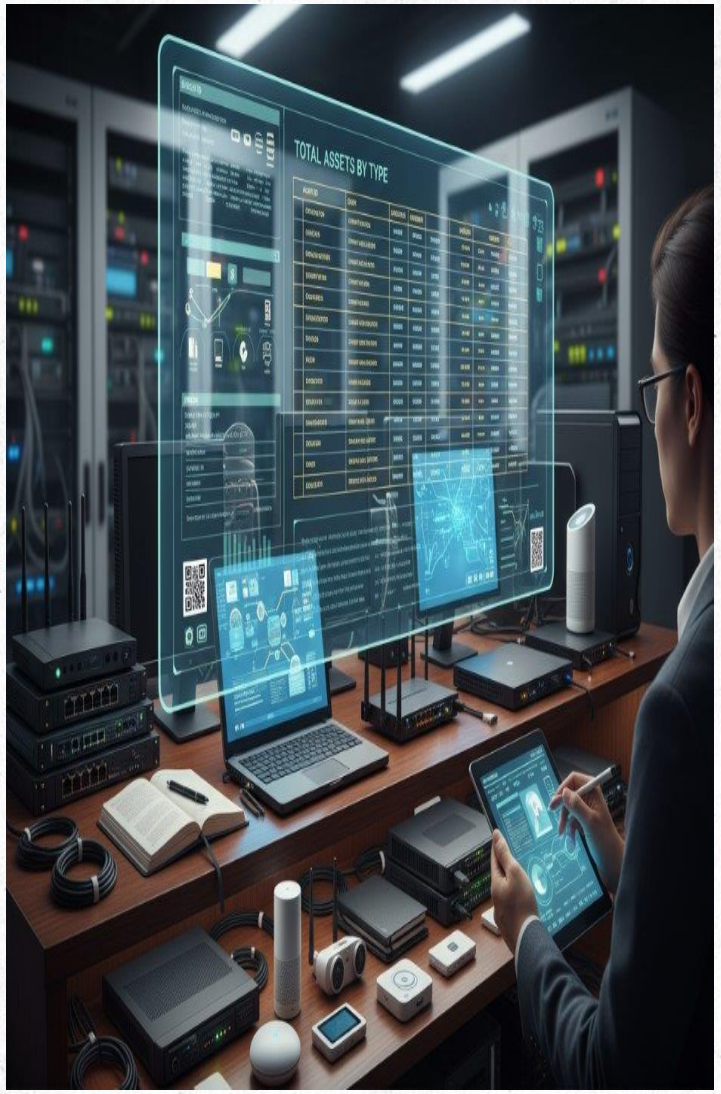
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Como nossos dados devem ser protegidos?



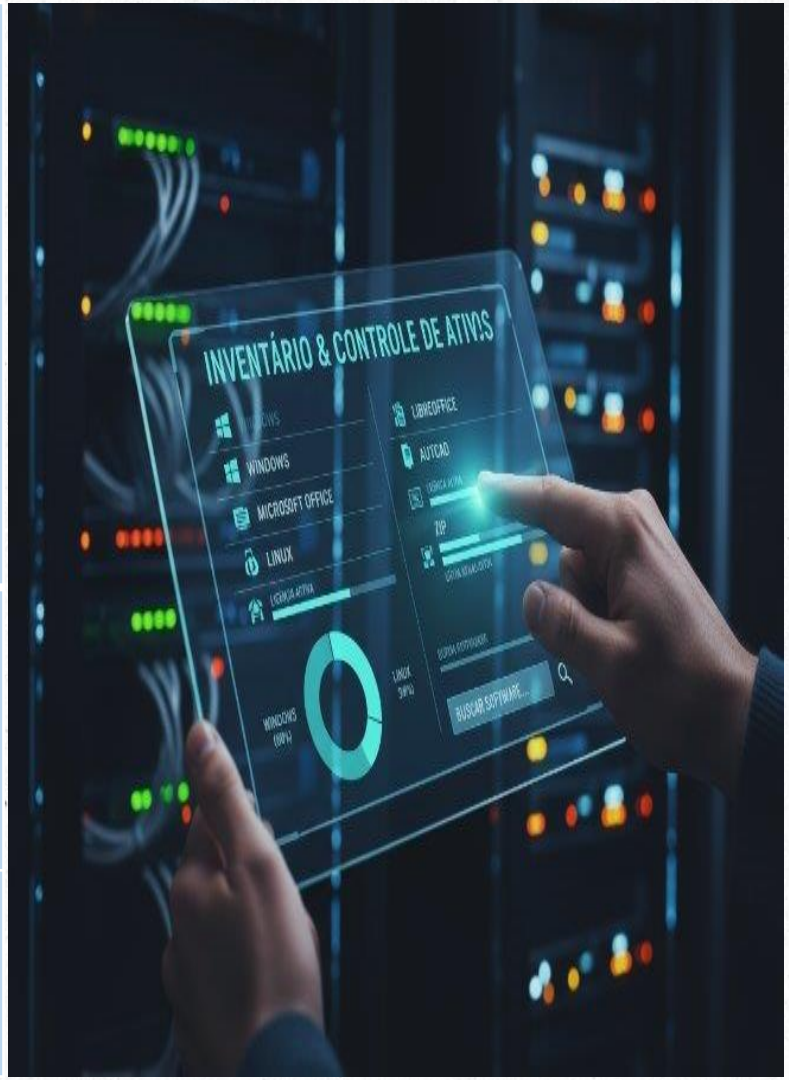
1 Inventário e controle de ativos institucionais: 5 medidas

Objetivo	Gerenciar ativamente todos os ativos institucionais conectados à rede, com o objetivo de identificar precisamente quais necessitam ser monitorados e/ou protegidos dentro da organização, mapeando todos os ativos não autorizados para uma possível remoção ou remediação futura.
Práticas identificadas	Política de gestão de ativos Ferramentas e softwares: planilhas eletrônicas, GLPI, OCS Inventory, DHCP, Nmap, Open-AudIT, SolarWinds NVM, Qualys CSAM, iTop.
Participantes	Gestor de Segurança da Informação Equipe de Tecnologia da Informação



2 Inventário e controle de ativos de software: 7 medidas

Objetivo	Gerenciar ativamente (inventariar, rastrear e corrigir) todo o *software* na rede para que apenas o *software* autorizado seja instalado e possa ser executado, e que todo o *software* não autorizado e não gerenciado seja encontrado e impedido de instalação ou execução.
Práticas identificadas	<u>Política de gestão de ativos</u> Ferramentas e softwares: planilhas eletrônicas, GLPI, OCS Inventory.
Participantes	Equipe de Tecnologia da Informação



3 Proteção de Dados: 14 medidas

Objetivo	Utilizar processos e ferramentas para identificar, classificar, manusear, reter e descartar dados. Abordagem integral que fortalece a governança de dados, reduz riscos e promove a confiança dos cidadãos.
Práticas identificadas	Processo de Gestão de Dados. Guia de Elaboração do Processo de Gestão de Dados (classificação, proteção e descarte). Ferramentas: BitLocker, LUKS, FileVault, SSH, TLS e IPsec.
Participantes	Equipe de Tecnologia da Informação

4 Configuração segura de ativos institucionais e software: 12 medidas

Objetivo	Estabelecer e manter a configuração segura de ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos de rede; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicações).
Práticas identificadas	Processo de Gestão de Configuração Ferramentas e softwares: CIS-CAT Pro / Lite, Lynis, (conformidade), Ansible, Puppet, Chef, GPO, scripts bash powershell, iptables. (hardening). NetBox, Cisco Prime / DNA, SolarWinds.
Participantes	Equipe de Tecnologia da Informação Equipe de Segurança da Informação

5 Gestão de Contas: 6 medidas

Objetivo	Usar processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, administrador e serviços para ativos e softwares institucionais.
Práticas identificadas	Política de controle de acesso. Inventário de Contas + Contas de Serviço. Ferramentas e softwares: • Serviço de diretório: Active Directory / Samba AD, LDAP / FreeIPA. • IAM/IDM: Keycloak, Okta.
Participantes	Administrador de Redes Equipe de Tecnologia da Informação Equipe de Gestão de Pessoas

6 Gestão de Controle de Acesso: 7 medidas

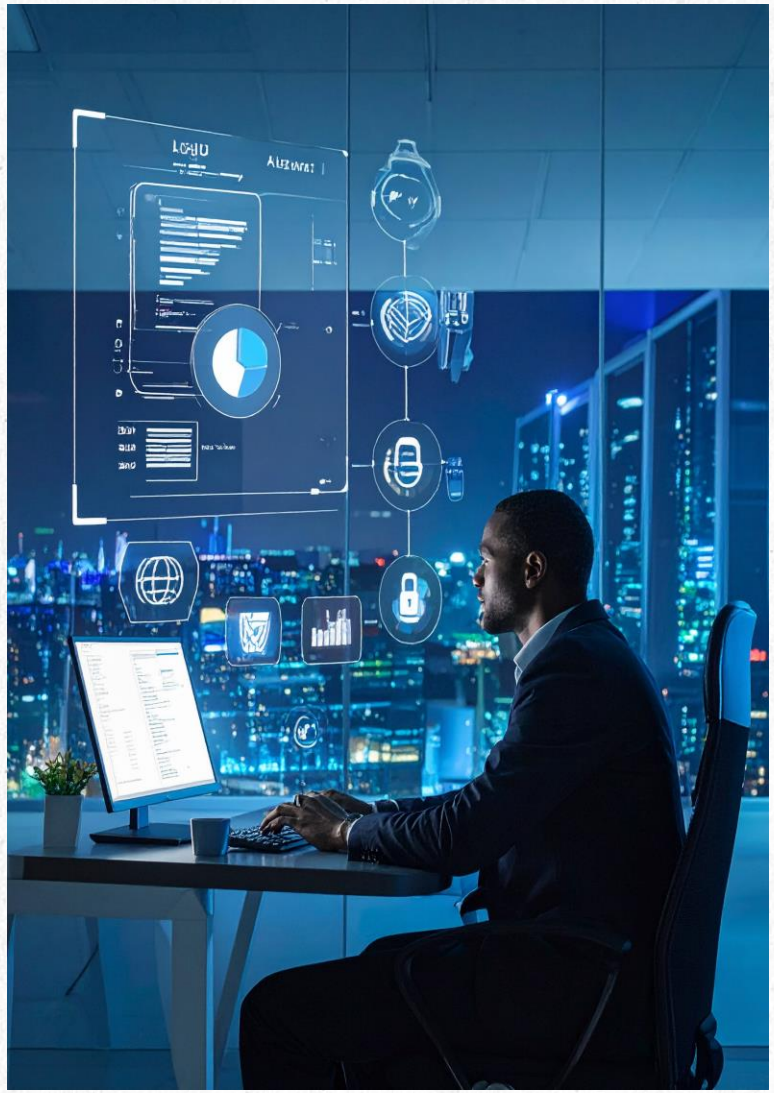
Objetivo	Usar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e *softwares* institucionais.
Práticas identificadas	Política de Controle de Acesso. Inventário Sistemas de Autorização. • Ferramentas e softwares: Diretório: FreeIPA, Samba AD, AD. • IdP / SSO: Keycloak, Shibboleth, OpenAM, ADFS / Entra ID. • MFA: privacyIDEA, LinOTP, Authelia • Acesso administrativo / PAM: Apache Guacamole, Teleport OSS, Segura.
Participantes	Administrador de Redes Equipe de Tecnologia da Informação

7 Gestão contínua de vulnerabilidades: 7 medidas

Objetivo	Desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura da organização, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar as fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.
Práticas identificadas	Guia de gerenciamento de vulnerabilidades Política de gerenciamento de vulnerabilidades Ferramentas e Softwares: Tenable Nessus, Qualys VMDR, Greenbone OpenVAS, TheHive + Cortex, Ansible, Rundeck, OpenSCAP + scripts, Tanium Chocolatey + scripts, Nmap + scripts, OWASP ZAP.
Participantes	Administrador de Redes, Sistemas e Segurança da Informação.

8 Gestão de Registro de Auditoria: 6 medidas

Objetivo	Coletar, alertar, analisar e reter logs de eventos com a finalidade de ajudar a detectar, compreender ou se recuperar de ataques cibernéticos.
Práticas identificadas	Política de Gestão de Registros (logs) de Auditoria Ferramentas e softwares: Wazuh, Elastic Stack, Graylog, Splunk, LogPoint, CrowdStrike Falcon LogScale, Blockbit SIEM, ManageEngine Log360, ManageEngine EventLog Analyzer.
Participantes	Administrador de Redes, Sistemas, ETIR e Equipe de Segurança da Informação.



9 Proteções de e-mail e navegador web: 7 medidas

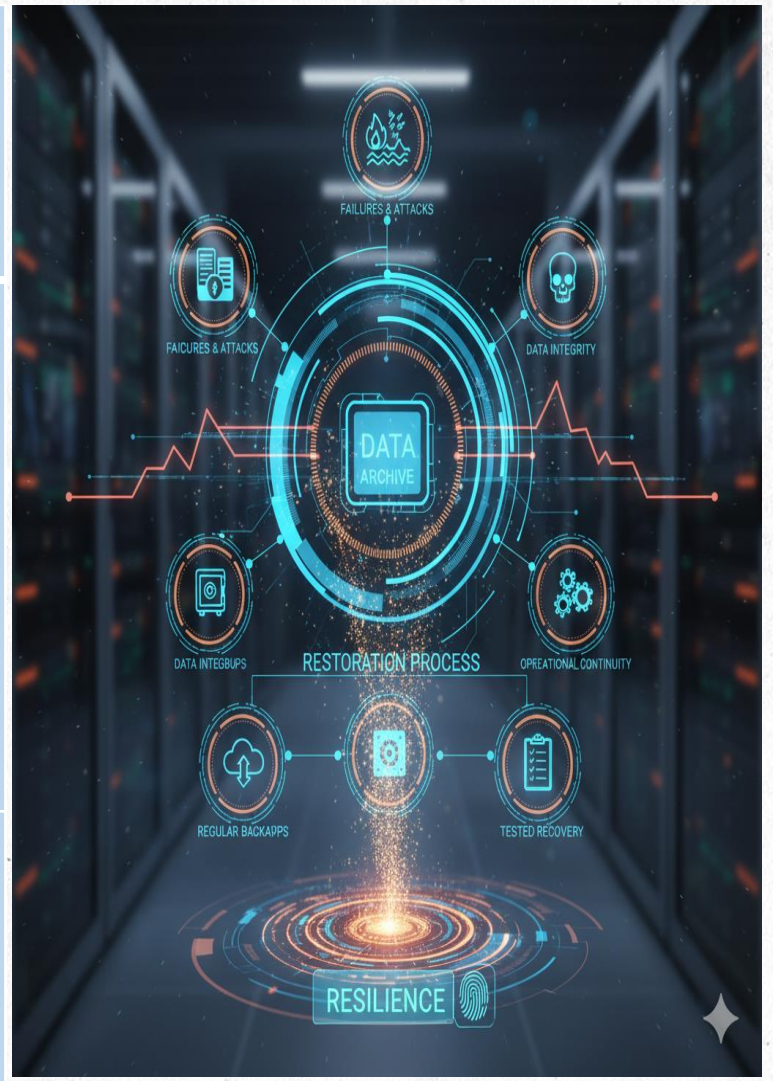
Objetivo	Melhorar as proteções e detecções de vetores de ameaças de e-mail e web, pois são oportunidades para atacantes manipularem o comportamento humano por meio de engajamento direto.
Práticas identificadas	Implementação de DMARC / SPF / DKIM para domínios de e-mail. Ferramentas e softwares: • Implementação de DMARC / SPF / DKIM. • Gateways de e-mail seguro: Google Workspace, Kaspersky Secure Mail. • Filtragem DNS / URL: DNSFilter, FlashStart, firewalls com DNS Security e URL Filtering. • Endpoint: Chrome Enterprise, políticas de Edge/Chrome via Intune/GPO.
Participantes	Administrador de Redes / Sistemas / Email. Equipe de Tecnologia da Informação

10 Defesas contra malware: 7 medidas

Objetivo	Impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou *scripts* maliciosos em ativos da organização.
Práticas identificadas	Aplicação de múltiplas camadas de proteção, incluindo soluções para detecção, monitoramento de comportamento e bloqueio de aplicações. Política de defesa contra malware Ferramentas e softwares: CrowdStrike Falcon, Microsoft Defender for Endpoint, Kaspersky Endpoint Security, Bitdefender Endpoint Security, ESET Endpoint Security; opções open source como Wazuh (detecção comportamental) integrado ao ClamAV.
Participantes	Administrador de Redes Equipe de Tecnologia da Informação

11 Recuperação de dados: 5 medidas

Objetivo	Criar e manter práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível.
Práticas identificadas	Política de Backup Manter cópias de segurança regulares, testadas e armazenadas em ambientes seguros, garantindo a disponibilidade, integridade e confidencialidade dos dados em caso de incidentes, falhas ou perdas. Ferramentas e *softwares*: veeam, bacula, Bareos, Commvault, Rsync para storage offline, Scripts de restore automático com cron, Bareos + restore jobs.
Participantes	Administrador de Backup. Equipe de Tecnologia da Informação. Equipe de Segurança da Informação.



12 Gestão de infraestrutura de rede: 8 medidas

Objetivo	Estabelecer, implementar e gerenciar ativamente (rastrear, reportar e corrigir) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos vulneráveis.
Práticas identificadas	• Documentação: Draw.io, Lucidchart. • Gerência: SolarWinds NCM, Cisco DNA Center / Prime, Ansible Networking. • AAA / Acesso seguro: FreeRADIUS, TACACS+, Cisco ISE. • Coleta/telemetria: NetFlows, Elastiflow, Wazuh (logs de dispositivos), syslog-ng. • Protocolos seguros: SSH, TLS, SNMPv3.
Participantes	Equipe de Redes

13 Monitoramento e defesa da rede: 11 medidas

Objetivo	Implementar processos e ferramentas para que a organização estabeleça o monitoramento e a defesa de rede contra ameaças de segurança em toda a sua infraestrutura de rede e base de usuários.
Práticas identificadas	Ferramentas e softwares: pfSense, Suricata, Snort, iptables/nftables, FortiGate, Palo Alto, OpenVPN + certs, SSH + Fail2Ban, CrowdStrike Falcon, Symantec EDR, Squid Proxy, ModSecurity (com Nginx/Apache), Cisco, Aruba, Wazuh, ntopng, PRTG ...
Participantes	Equipe de Redes Equipe de Segurança da Informação

14 Conscientização e treinamento de competências sobre segurança: 9 medidas

Objetivo	Implantar e manter um programa de conscientização de segurança que possa influenciar e conscientizar o comportamento dos colaboradores, tornando-os devidamente qualificados e assim atingir o objetivo de reduzir riscos de segurança cibernética.
Práticas identificadas	Política de desenvolvimento de pessoas em privacidade e segurança da informação Ferramentas e softwares: portal institucional, e-mail, cartazes, moodle, GoPhish, vídeos, jogos educativos, treinamentos regulares, TV, rádio, redes sociais.
Participantes	Equipes de Segurança da Informação, Pessoas, Capacitações, Comunicação e Tecnologia da Informação e Encarregado.

15 Gestão de provedor de serviços: 7 medidas

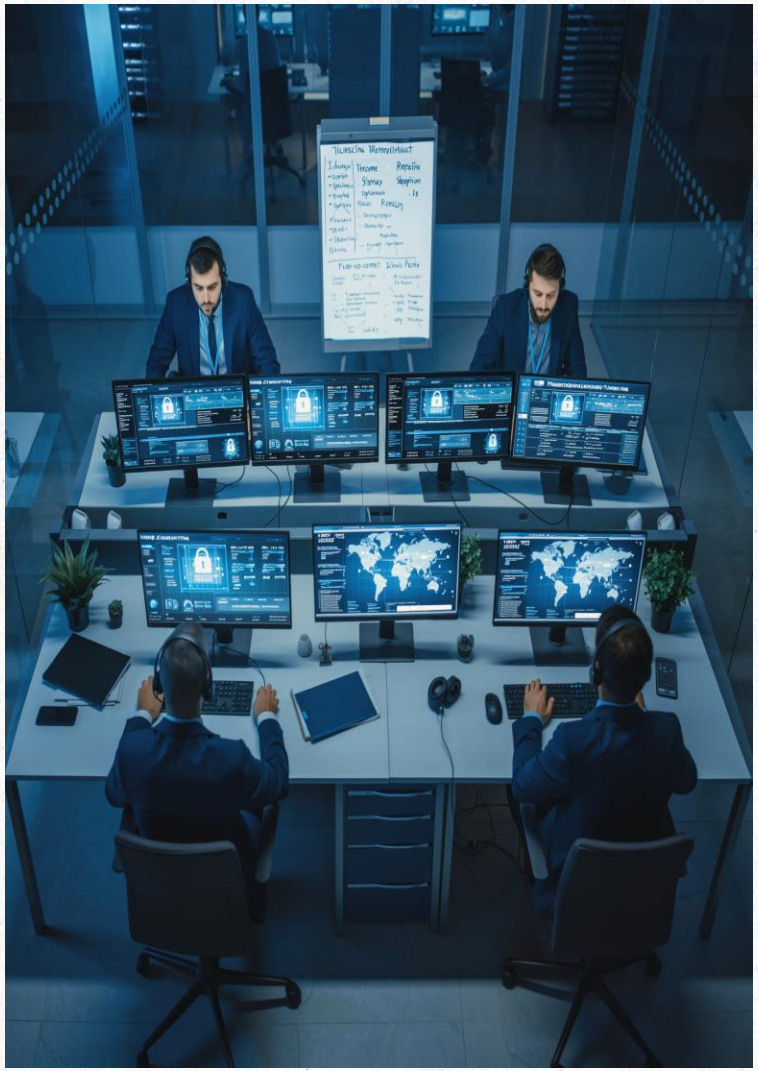
Objetivo	Garantir a proteção das informações, sistemas e processos críticos da organização, estabelecer um processo para avaliar os provedores de serviços que operem e matenham estes ativos da organização.
Práticas identificadas	Avaliação, monitoramento e revisão contínua dos provedores contratados de forma a reduzir riscos associados à tercerização de serviços. Política de gestão de provedor de serviços Guia de requisitos e obrigações quanto a privacidade e à segurança da informação Ferramentas e softwares: Zabbix, Grafana + Prometheus (para monitoramento técnico); GLPI (para SLAs); documentos e planilhas eletrônicas.
Participantes	Gestor(a) de Contratos Fiscal de Contratos

16 Segurança de aplicações: 14 medidas

Objetivo	Gerenciar o ciclo de vida de segurança de todos os *softwares* desenvolvidos e adquiridos internamente, a fim de prevenir, detectar e corrigir falhas de segurança.
Práticas identificadas	Segurança incorporada desde a concepção, desenvolvimento, testes e implantação aplicada de forma contínua e sistematizada. Guias de requisitos mínimos para privacidade e segurança da informação parA aplicações web, APIs, e aplicativos móveis Ferramentas e softwares: OWASP, DevSecOps pipelines com GitLab, GitHub, Docker Compose, Kubernetes Namespaces.
Participantes	Equipe de desenvolvimento de *softwares* Equipe de segurança da informação

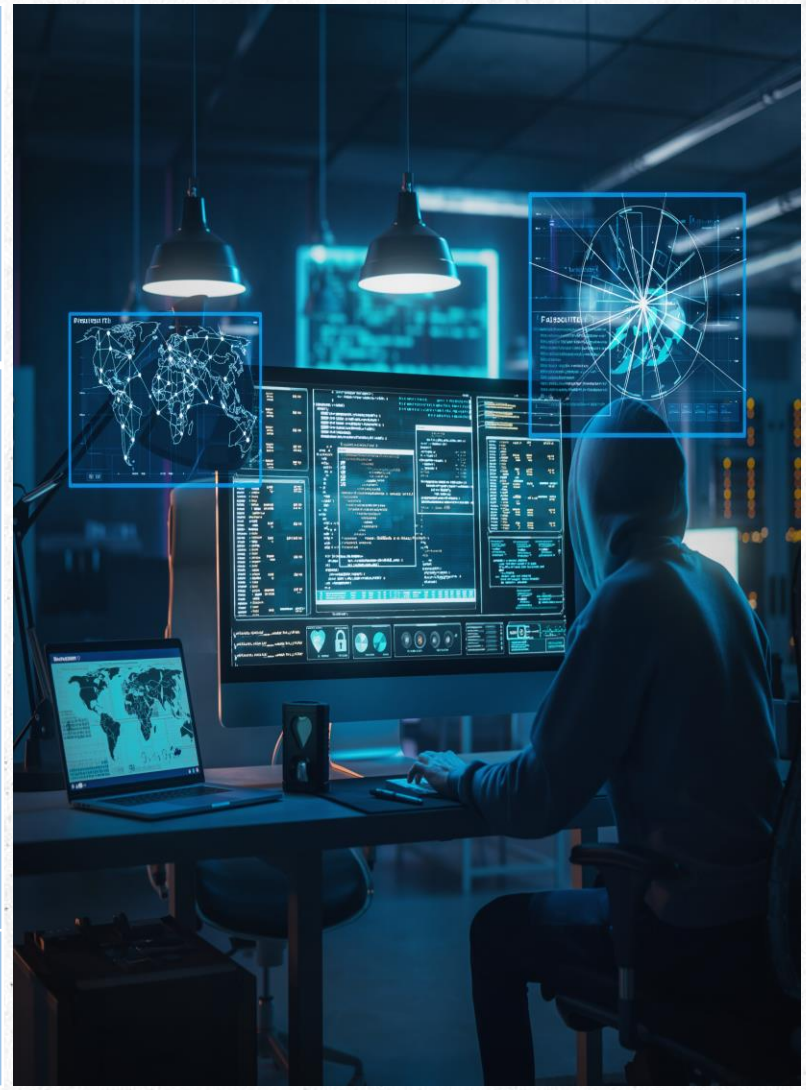
17 Gestão de resposta a incidentes: 9 medidas

Objetivo	Proteger as informações e a reputação da organização, desenvolvendo e implementando uma infraestrutura de resposta a incidentes para descobrir um ataque de forma ágil, e depois, conter efetivamente o impacto, eliminar a presença do atacante, e restaurar a integridade da rede e dos sistemas da organização.
Práticas identificadas	Guia de resposta a incidentes de segurança Ferramentas e softwares: Planilhas colaborativas, Jira Service Management, Wikis institucionais, painéis em Nextcloud, Microsoft Teams, GLPI, TheHive, sistemas locais...
Participantes	Equipe de Tecnologia da Informação Gestor de Segurança da Informação ETIR



18 Testes de Invasão: 5 medidas

Objetivo	Testar a eficácia e a resiliência dos ativos institucionais por meio da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.
Práticas identificadas	Realização de testes planejados e controlados por especialistas qualificados que simulam ataques reais para identificar, explorar e avaliar vulnerabilidades, assegurando a eficácia dos controles de segurança. Ferramentas e Softwares: PTES (diretrizes), Kali Linux, Metasploit, Wireshark, Nmap, OWASP ZAP, Nessus Professional, MITRE.
Participantes	Equipes de Tecnologia da Informação e Segurança da Informação



Resumo de Interdependência dos Controles de Segurança da Informação

Controle	Relacionamentos
1. Inventário e controle de ativos institucionais	Base para os demais controles
2. Inventário e controle de ativos de *software*	Inventário e controle de ativos institucionais (1)
3. Proteção de dados	Ativos institucionais e software (1 e 2), configuração segura de ativos (4), controle de acesso (6), gestão de vulnerabilidades (7), registro de auditoria (8), monitoramento e defesa de rede (13), e segurança de aplicações (16)
4. Configuração segura de ativos institucionais e *software*	Ativos institucionais e software (1 e 2), controle de acesso (6), gestão de vulnerabilidades (7), registro de auditoria (8), defesas contra malware (10) e recuperação de dados (11)
5. Gestão de contas (Identidade: usuários e senhas)	Ativos institucionais e software (1 e 2), controle de acesso (6), gestão de vulnerabilidades (7), registro de auditoria (8), segurança de aplicações (16)

Resumo de Interdependência dos Controles de Segurança da Informação

Controle	Relacionamentos
6. Gestão do controle de acesso	Proteção de dados (3), configuração segura de ativos (4), gestão de contas (5), registro de auditoria (8), segurança de aplicações (16).
7. Gestão contínua de vulnerabilidades	Ativos institucionais e software (1 e 2).
8. Gestão de registros de auditoria	Ativos institucionais e software (1 e 2), configuração segura de ativos (4), gestão de contas (5) e controle de acesso (6).
9. Proteção de e-mail e navegador web	configuração segura de ativos (4), gestão de vulnerabilidades (7), defesas contra malware (10), conscientização e treinamento (14) e segurança de aplicações (16).
10. Defesas contra *malware*	Ativos institucionais e software (1 e 2), configuração segura de ativos (4), gestão de vulnerabilidades (7), registro de auditoria (8) e proteções de e-mail e navegador web (9).

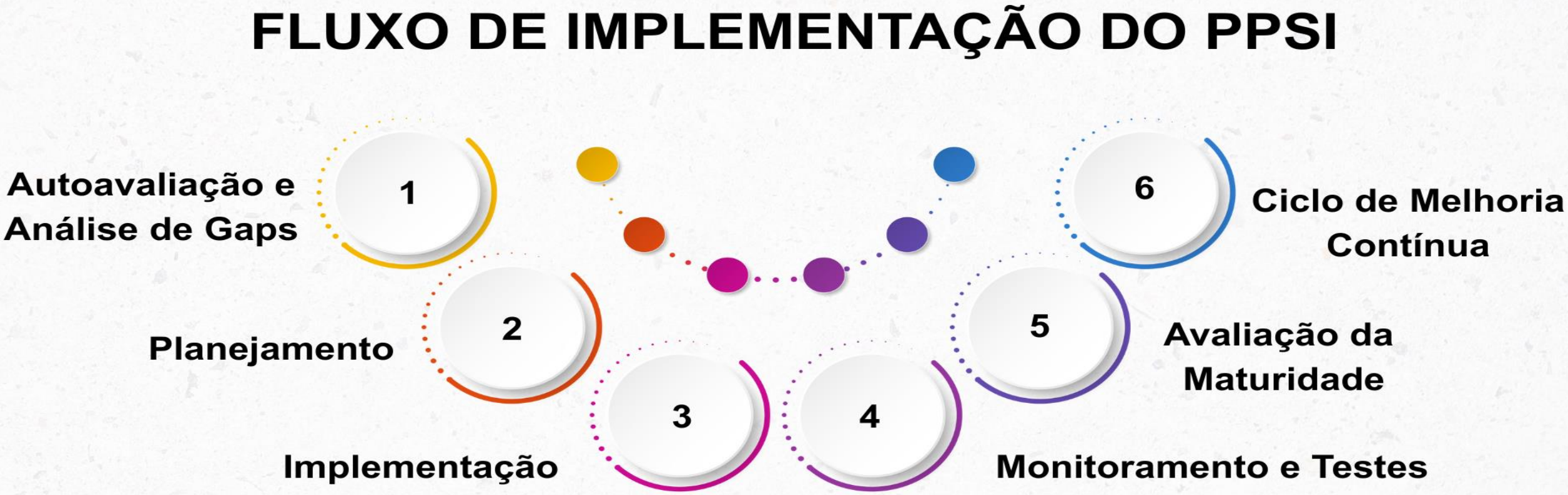
Resumo de Interdependência dos Controles de Segurança da Informação

Controle	Relacionamentos
11. Recuperação de dados	Proteção de dados (3), configuração segura de ativos (4), registro de auditoria (8), monitoramento e defesa de rede (13) e gestão de resposta a incidentes (17).
12. Gestão de infraestrutura de rede	Ativos institucionais e software (1), configuração segura de ativos (4), gestão de vulnerabilidades (7), registro de auditoria (8), defesa contra malware (10) e monitoramento e defesa de rede (13).
13. Monitoramento e defesa de rede	Ativos institucionais e software (1), configuração segura de ativos (4), gestão de vulnerabilidades (7), registro de auditoria (8), defesas contra malware (10), gestão de infraestrutura de rede (12) e gestão de resposta a incidentes (17).
14. Conscientização e treinamento de competências sobre segurança da informação	Proteções de e-mail e navegador web (9), defesas contra malware (10), recuperação de dados (11), segurança de aplicações (16), gestão de resposta a incidentes (17) e testes de invasão (18).

Resumo de Interdependência dos Controles de Segurança da Informação

Controle	Relacionamentos
15. Gestão de provedor de serviços	Ativos institucionais e software (1 e 2), proteção de dados (3), gestão de contas (5), controle de acesso (6), registro de auditoria (8), recuperação de dados e segurança de aplicações.
16. Segurança de aplicações	Ativos institucionais e software (1 e 2), proteção de dados (3), configuração segura de ativos (4), controle de acesso (6), gestão de vulnerabilidades (7), registro de auditoria (8) e proteções de e-mail e navegador web (9).
17. Gestão de resposta a incidentes	Ativos institucionais e software (1 e 2), proteção de dados (3), configuração segura de ativos institucionais e software, gestão de vulnerabilidades (7), registro de auditoria (8), recuperação de dados, monitoramento e defesa de rede (13), conscientização e treinamento (14) e testes de invasão (18).
18. Teste de invasão	Ativos institucionais e software (1 e 2), configuração segura de ativos institucionais e software, controle de acesso (6), gestão de vulnerabilidades (7), registro de auditoria (8), monitoramento e defesa de rede (13) e gestão de resposta a incidentes (17).

Como obter a segurança da informação na organização?



Principais desafios

- Ausência de diretrizes claras da alta administração em relação à segurança da informação
- Cultura organizacional e resistência à mudança
- Capacidade de atendimento em relação a escassez de profissionais qualificados e limitações orçamentárias
- Infraestrutura tecnológica e diversidade de dispositivos
- Monitoramento incompleto de riscos envolvendo a segurança da informação
- Ausência de conscientização e treinamento sobre segurança da informação
- Falta de coordenação entre os setores

Alicerces da Segurança da Informação

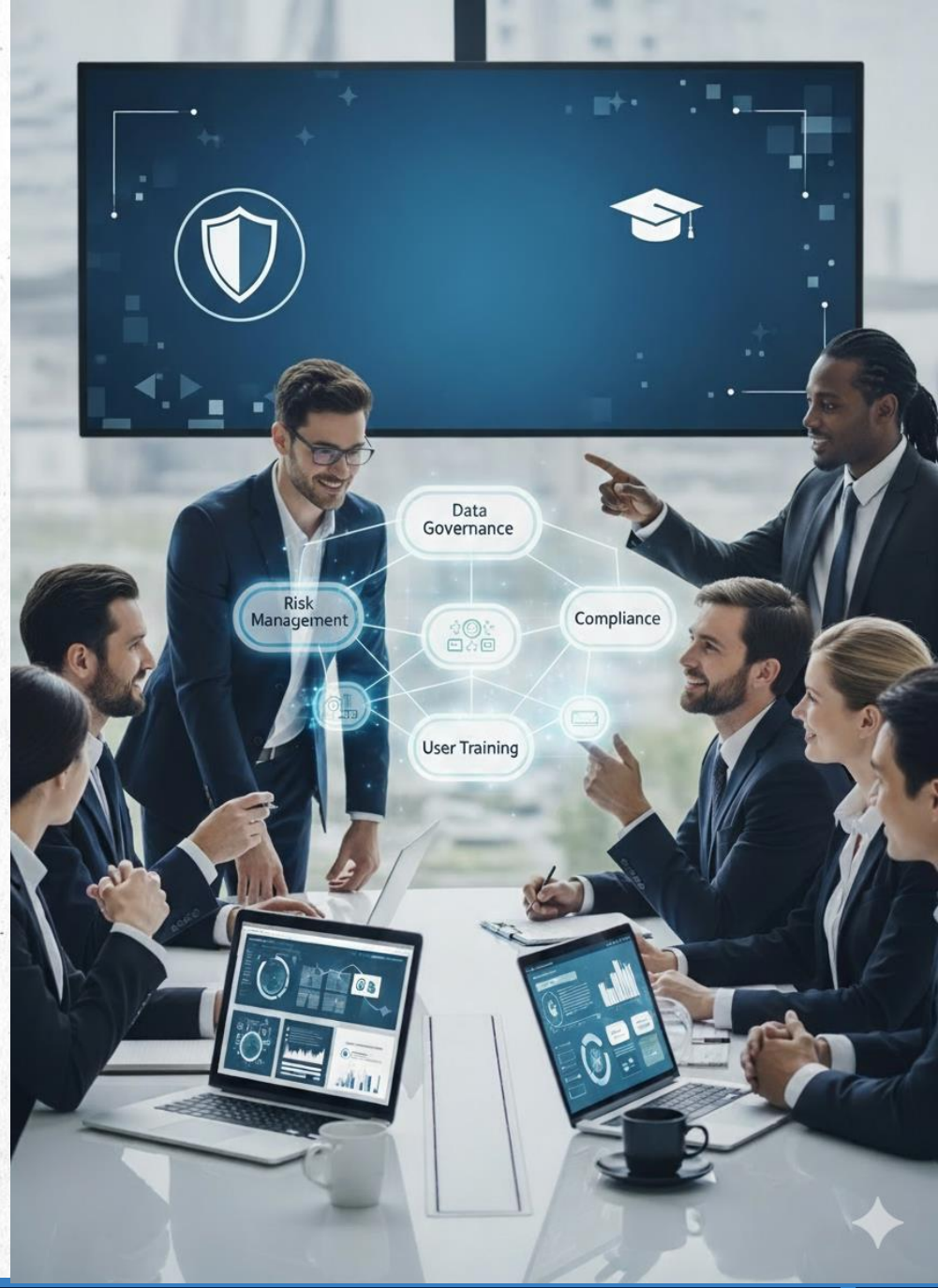
- Controle 0: Estrutura Básica de Governança
- Inventário e controle de ativos institucionais e software (1 e 2)
- Configuração segura de ativos e software (4)
- Proteção e recuperação de dados (3, 11)
- Gestão de contas e controle de acesso (5, 6)
- Gestão de Registros de Auditoria (8)
- Gestão contínua de vulnerabilidades (7)
- Gestão de respostas a incidentes (17)

Ações de apoio

gov.br

- Centro de Excelência em Privacidade e Segurança da Informação
- Centro Integrado de Segurança Cibernética
- Framework, Guias e Modelos
- Comunidades regionais - WhatsApp
- Formulário de dúvidas e solicitações do PPSI
- Pós Graduação em Privacidade e Segurança da Informação

Quem é o responsável pela Segurança da Informação?



Obrigado!

Carla Pires | **Fabiana Cardoso** | **Flávio Testa**
ppsi.sgd@gestao.gov.br

gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO