

Uma análise sobre a gestão de conformidade em ambientes críticos

Maurício Ariza,
Leonardo Lemes
Pâmela Carvalho
Sérgio Nunes

Autores



Maurício Ariza



Estudante da Graduação Tecnológica de Segurança da Informação da Universidade do Vale do Rio dos Sinos (UNISINOS/RS). Profissional com experiência nas áreas de análise de fraudes computacionais e de infraestrutura crítica, sendo certificado pela EMC. Atua como analista de segurança para Gestão de Incidentes e Gestão de Conformidades na equipe técnica do *Computer Emergency Response Team* da Defesa.

Leonardo Lemes



Mestre em Computação Aplicada e Bacharel em Análise de Sistemas, ambos pela Universidade do Vale do Rio dos Sinos (UNISINOS/RS). Professor e Coordenador da Graduação Tecnológica de Segurança da Informação na UNISINOS, Sócio-fundador e Diretor da área de Consultoria da Defesa. Instrutor da Escola Superior de Redes da RNP e profissional com as seguintes certificações: Auditor Líder ISO 27001, ABCP, CRISC.

Autores



Pâmela Carvalho



Estudante da Graduação Tecnológica de Segurança da Informação da Universidade do Vale do Rio dos Sinos (UNISINOS/RS) e Técnica em Sistemas de Informação pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - Campus Porto Alegre. Profissional com experiência nas áreas de análise de fraudes computacionais e de resposta à incidentes. Atua como analista de segurança para Gestão de Incidentes e Gestão de Conformidades na equipe técnica do *Computer Emergency Response Team* da Defesa.

Sergio Nunes



MBA em Gestão Estratégica de Negócios e Graduado em Segurança da Informação, ambos pela Universidade do Vale do Rio dos Sinos (UNISINOS/RS), certificado COBIT e ITIL v3. Profissional com experiência em projetos de infraestrutura, gestão de serviços de TI, gestão de riscos, conformidade e auditoria. Atua como consultor em Segurança da Informação & Compliance e coordenador do *Computer Emergency Response Team* da Defesa.

Agenda



Gestão de Conformidade

- ✓ O que é?
- ✓ Ciclo de Vida
- ✓ Como implementar?

CIS: Centro de Segurança para Internet

- ✓ Apresentação
- ✓ Security Benchmarks

Análise – Estudo de Caso

- ✓ Apresentação do Ambiente
- ✓ Resultados Gerais

Considerações Finais

Gestão de Conformidade

O que é?



- ✓ Conformidade é o ato de cumprir regras ou controles pré-estabelecidos;
- ✓ Gestão de Conformidade envolve o controle do cumprimento de boas práticas, leis ou padrões ou normas, sejam de mercado, de governo, fornecedores, etc.
- ✓ A conformidade em TI não é uma novidade, já são comuns padrões como o PCI-DSS, normas como a ISO 27002 e leis como a Sarbanes-Oxley.

Gestão de Conformidade

Ciclo de Vida



Gestão de Conformidade

Como implementar?



**“Mas se eu não sou obrigado
a seguir nenhuma política em específico,
como posso definir controles
de boas práticas para minha empresa?”**

Utilizando um framework!

CIS: Centro de Segurança para Internet



Apresentação

- ✓ Organização sem fins lucrativos voltada para melhorar a capacidade da segurança computacional, atua de forma colaborativa no desenvolvimento de conhecimento em segurança da informação.



<https://www.cisecurity.org>

CIS: Centro de Segurança para Internet

Security Benchmarks



- ✓ Divisão da CIS que elabora políticas com controles seguindo as melhores práticas para configuração e uso de equipamentos;

The screenshot shows the homepage of the CIS Security Benchmarks website. The header features the 'Security Benchmarks' logo, social media links for LinkedIn, Facebook, Twitter, and YouTube, and a search bar. The main navigation bar includes links for 'ABOUT US', 'MEMBERSHIP', 'COMMUNITY', 'SECURITY RESOURCES', and 'LOGIN'. The main content area has a 'Home' link and a 'Welcome to the CIS Security Benchmarks Division' section. This section includes a paragraph about the division's mission and a 'MORE' button. To the right, there is a carousel slide with a green background, a world map, a padlock, and a checkmark, with text about PCI Compliance Requirements. Below the main content, there are two columns: 'BECOME A MEMBER' and 'JOIN CONSENSUS TEAM', each with a brief description and a 'Learn more' link. At the bottom right, there is a 'Free CIS Security Resources' section with a link to leverage CIS resources.

<http://benchmarks.cisecurity.org/>

CIS: Centro de Segurança para Internet

Security Benchmarks



Atende diversas tecnologias:

- ✓ Apache;
- ✓ iOS;
- ✓ RedHat Linux;
- ✓ Android;
- ✓ HP-UX;
- ✓ Kerberos;
- ✓ Oracle;
- ✓ Etc.

Looking for XML or Oval Content? CIS has newly released Microsoft Windows Server 2012, Microsoft Windows 8 and Microsoft SQL Server Database R2 content NOW AVAILABLE. [Learn More](#)

BECOME A MEMBER	JOIN CONSENSUS TEAM
Take advantage of affordable, expert guidance and resources including automated security configuration assessment and remediation tools, along with industry-leading benchmarks.	Earn CPE credits and peer recognition by joining other IT security experts in establishing best practices through the collaborative development and maintenance of security Benchmarks and other resources.
More	More

Free CIS Security Resources

Leverage CIS resources to build a more secure and compliant environment.

Our benchmarks are referenced in the PCI Data Security Standard and included in the NIST National Checklist Program repository. They are also widely used for obtaining compliance with a number of recognized security standards.

- Apache HTTP & Tomcat Benchmarks
- Apache HTTP & Tomcat Benchmarks Archive
- Apache HTTP Server Assessment Tool
- Apple iOS Benchmarks
- Apple iOS Benchmarks Archive
- Apple OSX Benchmarks
- Apple OSX Benchmarks Archive
- Apple Safari Benchmarks
- Authentication Server Benchmarks
- Benchmark Assessment Tools
- CheckPoint Firewall Benchmarks
- Cisco Device Benchmarks
- Cisco Device Benchmarks Archive
- Collaboration Server Benchmarks
- Consensus Security Configuration Benchmarks
- Consensus Security Metrics
- Consensus Security Metrics Archive
- Database Server Benchmarks
- Debian Linux Benchmarks

CIS Security Benchmarks Member

Center for Internet Security | 31 Tech Valley Drive | East Greenbush, NY 12061
Trusted Purchasing Alliance | Multi-State ISAC | Integrated Intelligence Center | CIS Blog | Privacy Policy | Sitemap | Newsroom

CIS: Centro de Segurança para Internet



Security Benchmarks

1.1.23 Disable Mounting of squashfs Filesystems (Not Scored)

Profile Applicability:

- Level 2

Description:

The `squashfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to `cransfs`). A `squashfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

```
# /sbin/modprobe -n -v squashfs
install /bin/true
# /sbin/lsmod | grep squashfs
<No output>
```

Remediation:

Edit or create the file `/etc/modprobe.d/CIS` and add the following line:

```
install squashfs /bin/true
```

References:

1. CCE-14118-4

1.1.24 Disable Mounting of udf Filesystems (Not Scored)

Profile Applicability:

- Level 2

Description:

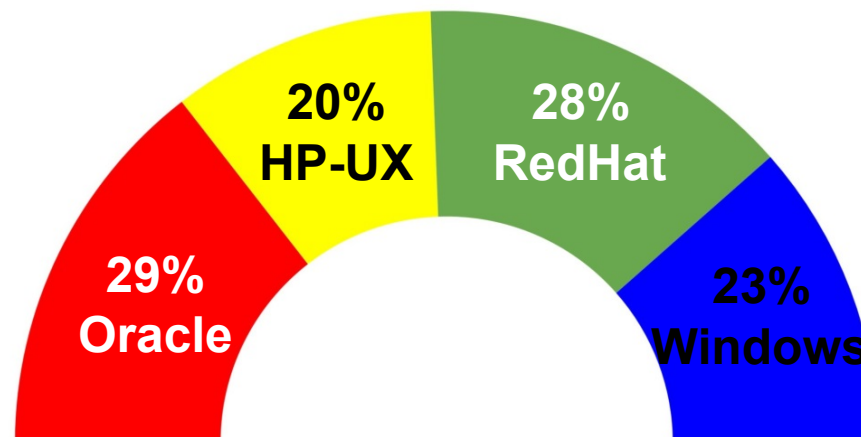
Trecho do CIS Benchmark para RedHat Enterprise Linux 5

Análise – Estudo de Caso

Apresentando o Ambiente



- ✓ Servidores distribuídos em 8 países;
- ✓ Total de 254 ativos monitorados;
- ✓ Um ano de coleta de dados.



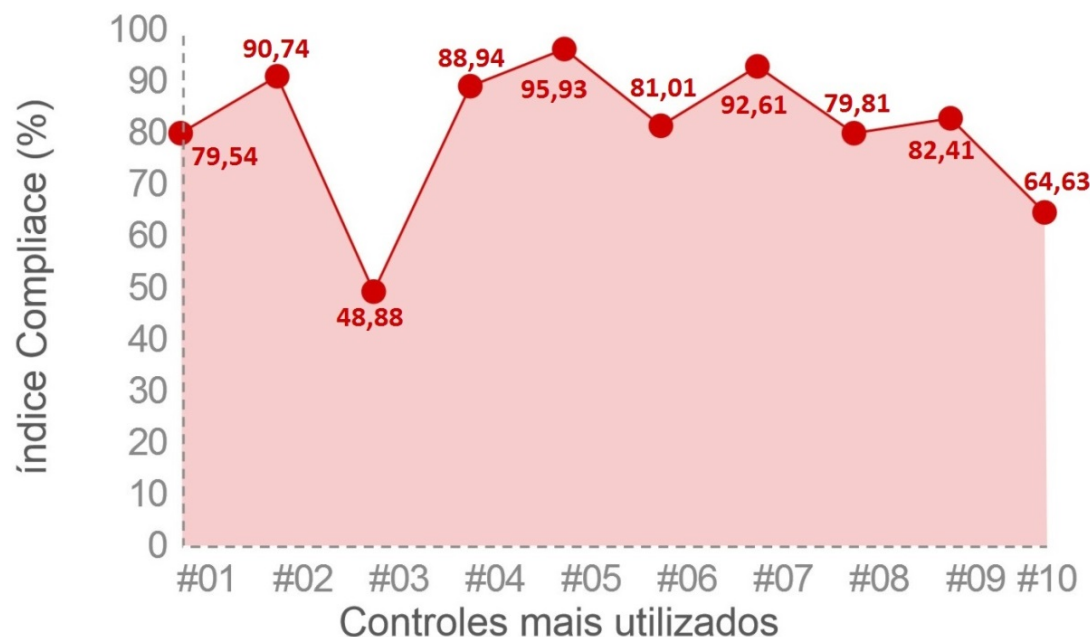
Análise – Estudo de Caso

Resultados



TOP 10 CONTROLES

Controles mais utilizados e nível de compliance



#01 Set Password Change
Minimum Number of Days

#02 Set Password Minimum Length

#03 Remove Oracle 'tkprof' utility

#04 Set Password Expiring Warning
Days

#05 Service Status – DHCP

#06 Set Password Expiration
Number of Days

#07 Set Password Minimum
History

#08 Service Status – DNS

#09 Unix Service Status - 'rwhod'

#10 Unix Service Status - 'rstatd'



DEFENDA
CERT

GTS 22ª - DEZ/2013
www.defenda.com.br

Análise – Estudo de Caso

Resultados



TOP 10 CONTROLES

Maior índice de compliance



Unix Service Status - 'RARPD'

Unix Service Status - 'RSTATD'

Unix Service Status – finger

Unix Service Status - 'RUSERSD'

User accounts who have root privileges (UID=0)

Accounts who have directly assigned privileges

Value set for Oracle 'user_dump_dest' parameter

Oracle accounts who have access to SYS.SOURCE\$ table

Value set for Oracle init.ora 'remote_os_rules' parameter

Value set for Oracle init.ora 'os_roles' parameter



TOP 10 CONTROLES

Menor índice de compliance



Permissions set to ORACLE_HOME/network/admin directory

Permissions set to ORACLE_HOME directory

Value set for 'password_lock_time' parameter

Oracle accounts who have access to V_\$ views

Oracle accounts who have access to SYS.LINK\$ table

Oracle accounts who have access to DBA_SYS_PRIVS views

Oracle accounts who have access to _CATALOG_ roles

Oracle accounts who have access to DBA_ROLES views

Value set for Oracle init.ora 'LOG_ARCHIVE_DUPLEX_DEST' parameter

Oracle accounts who have access to DBA_TAB_PRIVS views

Considerações Finais



Dos controles mais utilizados

- ✓ 50% estão relacionados com senhas
- ✓ 30% estão relacionados com status de serviços
- ✓ 20% estão relacionados com configuração

Dos controles com maior índice de compliance

- ✓ 40% estão relacionados com status de serviços
- ✓ 30% estão relacionados com permissionamento
- ✓ 30% estão relacionados com configuração

Dos controles com menor índice de compliance

- ✓ 70% estão relacionados com permissionamento
- ✓ 10% estão relacionados com configuração

Considerações Finais



- ✓ Auxilia as organizações a terem um maior controle sobre seu ambiente;
- ✓ Homogeneização da infraestrutura, tendo um melhor controle da configuração dos ativos;
- ✓ Tratamento de vulnerabilidades e riscos da rede;
- ✓ Melhora constante dos níveis de segurança da informação.

Considerações Finais



Os desafios da Gestão de Conformidade são:

- ✓ O abandono do ciclo de verificações;
- ✓ O engessamento dos processos de tratamento e correção dos itens não-conformes;
- ✓ O escaneamento de ativos sem a análise dos resultados;
- ✓ Vender a importância desse trabalho para as camadas superiores do negócio.

Considerações Finais



**Gestão de Conformidade
é para sua empresa também,
independente do tamanho!**



Perguntas?

Obrigado!

Maurício Ariza

mauricio.ariza@defenda.com.br

Pâmela Carvalho

pamela.carvalho@defenda.com.br

Leonardo Lemes

leonardo.lemes@defenda.com.br

Sérgio Nunes

sergio.nunes@defenda.com.br