Endereço do Site:	CONSELHO FEDERAL DE ODONTOLOGIA https://www.eleicoesodontologia.org.br
Código:	*CFO – 2017 – MG 2º TURNO*

Introdução:

Para fins de auditoria do processo eleitoral, foi realizada análise de segurança do sistema, cujo resultado foi expresso em relatório de adequação e as correções, aplicadas. O resultado do último teste é transcrito no corpo deste documento.

fgn

Observações:

Empresa de sistemas: favor preencher as seções abaixo: (**neste mesmo formulário, sem reformatações, mudanças de autoria ou qualquer outra característica do formulário):**

SEÇÃO I – SOFTWARE, no que for cabível,
SEÇÃO II – ESCLARECIMENTOS/JUSTIFICATIVAS, sobre as observações de auditoria. As justificativas podem incluir a determinação de correção das fragilidades apontadas nos testes e a data provável de implementação destas correções ou a explicação da não aplicabilidade da análise.

Recomendações:

1. - As recomendações decorrentes da análise técnica, para fins de clareza, são descritas no corpo do documento.

2. - As sugestões de regras de negócio, ou seja, incrementos técnico-administrativos, como facilidades de segurança e utilização, são resumidas a seguir:

   - Considerações sobre segurança na recuperação de senhas: recuperações de senhas ou mudanças de senhas serão feitas utilizando-se do CPF e DATA DE NASCIMENTO do inscrito, necessariamente. As senhas serão enviadas sempre para os endereços de e-mail e, na recuperação de senhas, para o telefone celular previamente cadastrados no sistema;
   - Considerações sobre votação: a votação, que poderá ser feita com a senha recebida por e-mail ou, pela senha cadastrada posteriormente, pelo inscrito, na troca de senha, deverá ser feita com a utilização de CPF e DATA DE NASCIMENTO, necessariamente;
   - Considerações sobre a separação lógica de bases de dados: deverá haver uma base de dados para os inscritos adimplentes (sendo considerados adimplentes aqueles que tiveram suas baixas computadas no arquivo fornecido no dia 06/01/17) e outra formada, exclusivamente, pelos inadimplentes. A base de inadimplentes poderá, com o uso de certificado digital, ser alterada, por profissional designado pelo Conselho Regional, habilitando-se aqueles inscritos que realizarem o pagamento na sede ou regionais autorizados do Conselho, sempre contra a apresentação do comprovante contábil de tal pagamento, permitindo o voto deste, exclusivamente, em computador disponível na sede ou regional.

Resumo da Avaliação:

As notações técnicas foram corrigidas, restando o sistema seguro para a perfeita execução do processo eleitoral em questão.

THE PERFECT LINK ASSESSORIA CONSULTORIA AUDITORIA:01912699000129

Digitally signed by THE PERFECT LINK ASSESSORIA CONSULTORIA AUDITORIA:01912699000129
Date: 2017.03.01 13:33:04 -03'00'

Site Survey/Audit Procedure

1. **IMPORTANTE**:
    a. **Não alterar as características do formulário, preenchendo este mesmo documento, sem conversões de formato, autoria e afins.**
    b. **As seções que devem ser preenchidas estarão disponíveis para edição, as demais, com edição vedada, são para visualização.**
2. Contatos - solicitamos atentar para o preenchimento dos contatos de plantão bem como das exatas características do hardware;
    a. **Testes** – serão realizados testes de capacidade do sistema de eleição, em data previamente agendada, na versão final do sistema (com as telas de votação adequadas e critérios de votação customizados para esta eleição), que deverão contar com o ambiente definitivo da realização da eleição;
    b. **Individualização do Software** - após os testes finais, obtida a aprovação da auditoria, o sistema será isolado em mídia criptografada e colocado à disposição da mesa/comissão eleitoral;
3. Lembre-se que as informações que necessitamos são referentes aos provedores, sites de hospedagem, hardware e softwares que têm relação direta ou indireta com o Processo de Eleição, não sendo necessário documentar software e hardware que não fazem parte deste escopo.
4. Complete todas as seções do formulário de Site Survey Documento de Auditoria (Necessário).
5. Copie e cole as fotografias/impressões de telas de votação nas seções próprias. Havendo dificuldade com esta seção, as imagens podem ser enviadas como anexo no e-mail de resposta.
6. Envie fotografias/impressões de tela dos formulários de inicialização (“zeração”) dos contadores, troca de senhas, votação, apuração, do Software de Votação.
7. Envie este formulário para auditoria@theperfectLink.com.br.
8. Forneça os telefones, e-mail e nome de contato da equipe técnica responsável pelas informações.
9. Forneça link de testes da eleição, bem como (acesso à) base de dados de teste com lista de usuários e senhas, incluindo-se usuários com impedimento.

SEÇÃO I – SOFTWARE – (SISTEMA DE VOTAÇÃO)

EMPRESA:	Scytl	
CNPJ:	05.494.350-0001-75	
Endereço da Empresa:	SCN Quadra 4 Bloco B Sala 502 Edifício Centro Empresarial Varig 70714-900 Brasília - DF - Brasil	
Código:	Scytl	
Identificação do Software:	Nome Comercial:	WEBVOTO
	Descrição completa:	Software para realização de eleições via WEB
	Fabricante:	SCYTL
	Versão/Ano de Fabricação:	2016
	Licenciamento-Contrato:	WEBVOTO

Características do Software:	Plataforma-Linguagem:	ASP.NET-C#
	Idioma:	Português
	Plataforma de Bando de Dados:	Microsoft SQL Server
	Monousuário / Multiusuário:	Multiusuário
	Comentários:	ASP.NET-C#

Requisitos para o Perfeito Funcionamento no **Servidor**:	Processador:	Aplicação: 4 cores
	Memória RAM:	Banco de dados: 50 DTUs
	Espaço livre em Disco Rígido:	Aplicação: 7 GB
	Capacidade Total Mínima do Disco Rígido:	Banco de dados: N/A
	Plataforma de Sistema Operacional Necessária:	Aplicação: 40 GB
	Comentários:	Banco de dados: 15 GB

Requisitos para o Perfeito Funcionamento no Acesso WEB (**Estação Votante**):	Processador:	Dual Core 1.5 GHz
	Memória RAM:	2 GB
	Espaço livre em Disco Rígido:	100 GB
	Capacidade Total Mínima do Disco Rígido:	500 GB
	Sistemas Operacionais que rodam a Aplicação:	Microsoft Windows 7 ou superior
	Incompatibilidades com Aplicações, Complementos, Plug-ins:	Apple Mac OS X 10.10 ou superior
	Comentários:	Linux com até 1 ano da última versão da distribuição ou superior

Características de Segurança:	Tecnologias de Segurança Utilizadas:	Encriptação e assinatura do voto no navegador e Decriptação e Verificação de integridade na apuração
	Série-Tipo de Criptografia (se houver):	
	Norma, Padrão, Protocolo de Segurança Adotado:	
	Características de Preservação dos Dados quando da Interrupção Não Programada do Sistema:	SQL Azure com replicação
	Prevenção de Não Duplicação de Protocolos de Votação:	SIM - Transação atomica
	Quantidade Máxima de Usuários Simultâneos já testada:	3.000
Segurança contra Ameaças Externas (Tecnologias Utilizadas/Recomendadas e sua compatibilidade com o software de votação):	Prevenção Contra Invasões:	Microsoft Azure Firewall
	Prevenção Contra Vírus:	Microsoft Azure Firewall
	Prevenção Contra Tentativa de Reincidência de Votação:	SIM-Transação atomica
	Certificados digitais:	Logins do BackOffice com certificados ICP Brasil
	Comentários:	Microsoft Azure Firewall

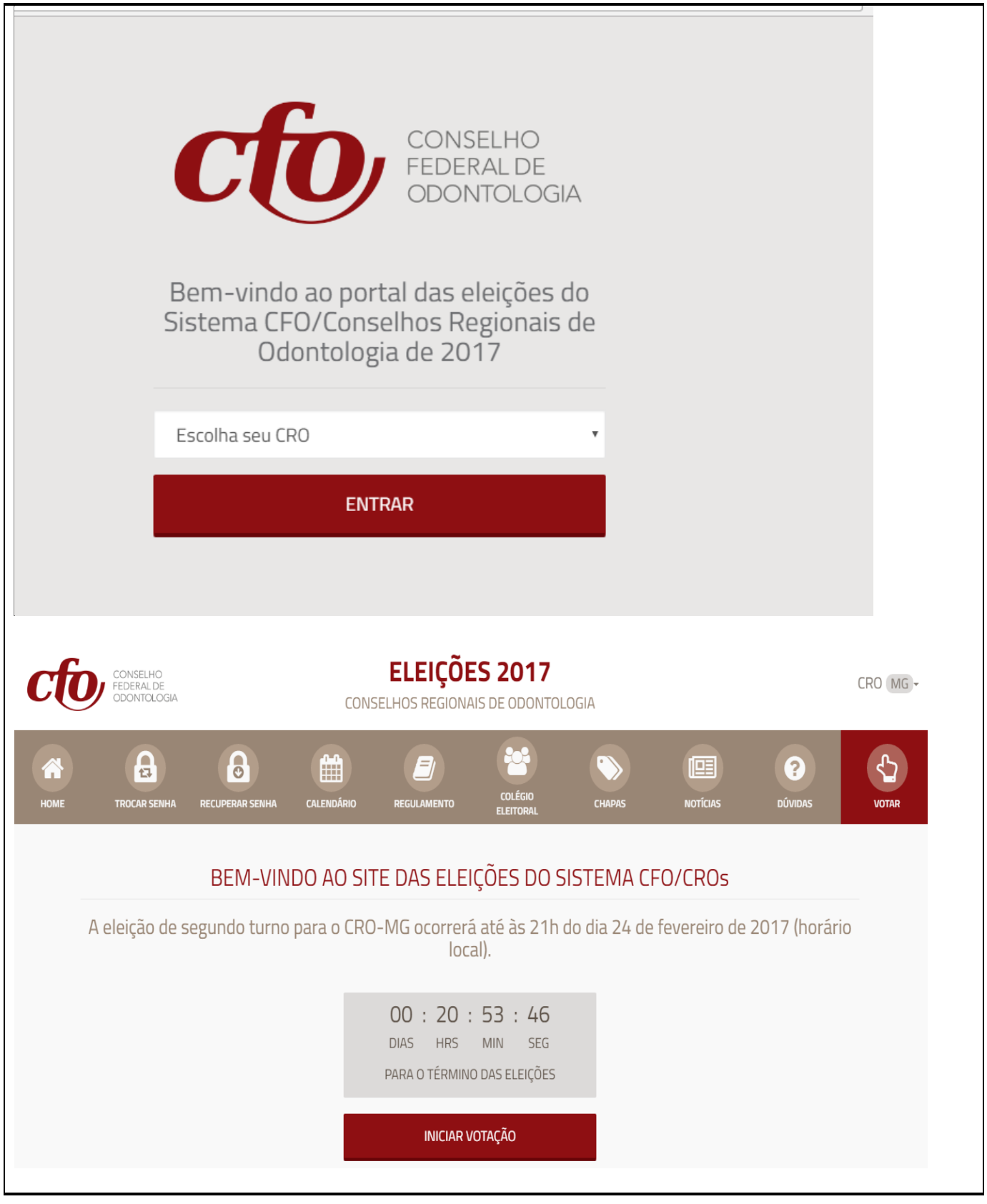
Segurança contra Ameaças Externas (Tecnologias Utilizadas/Recomendadas e sua compatibilidade com o software de votação):	Prevenção Contra Invasões:	Microsoft Antimalware para Azure
	Prevenção Contra Vírus:	Microsoft Antimalware para Azure
	Prevenção Contra-Ataques de DOS (Denial of Service):	Azure Firewall
	Prevenção Contra-Ataques de DNS:	Microsoft Azure DNS Zones

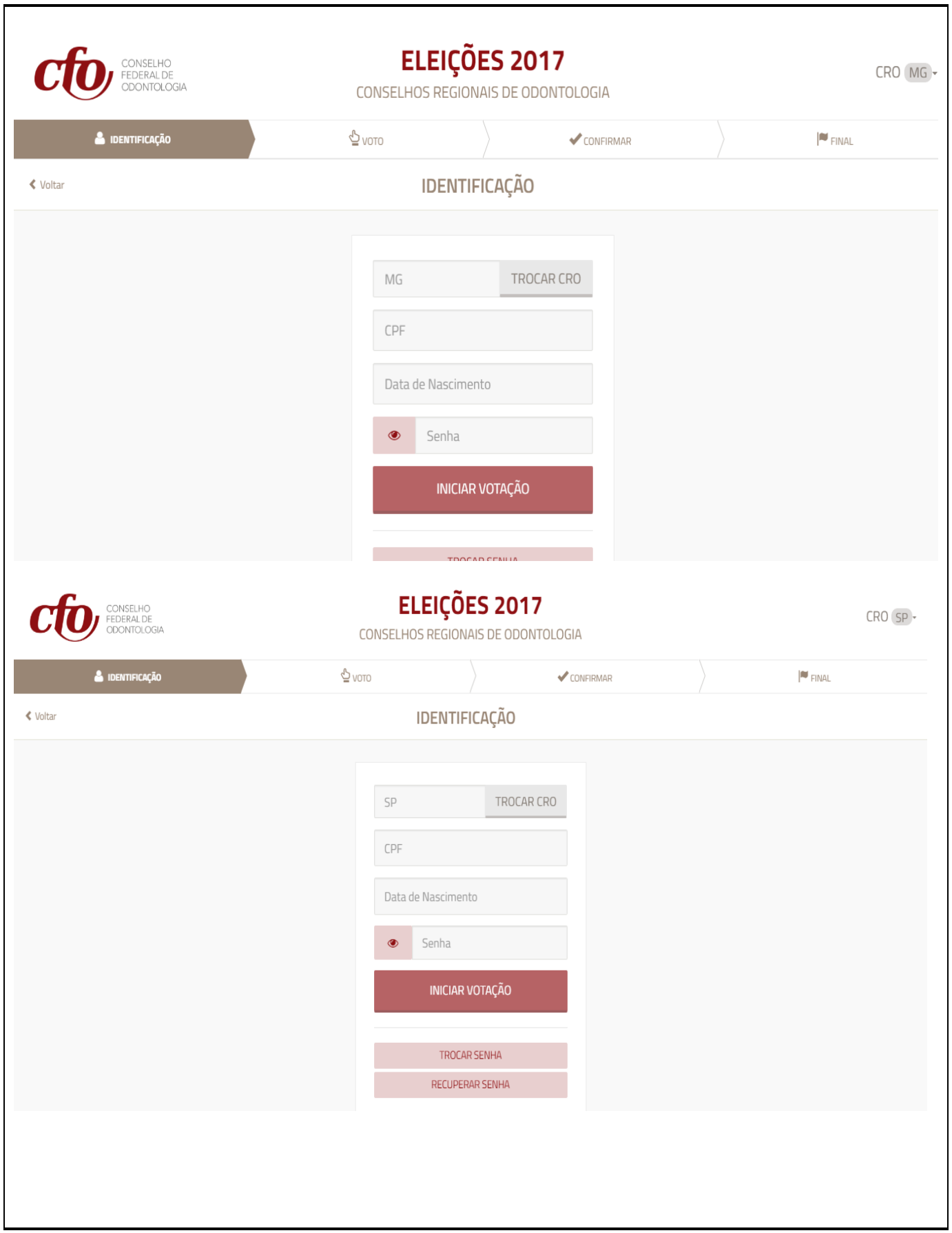
Equipe de Suporte Software:	Quantidade:	6
	Responsável:	Ubiratan Elias
	Contatos do Responsável:	61 3961 1800
	Técnico de Suporte:	Hermano Portella
	Contatos do Técnico de Suporte:	61 3961 1800
	Técnico de Suporte 2:	Denis Aguilar
	Contatos do Técnico de Suporte 2:	61 3961 1800

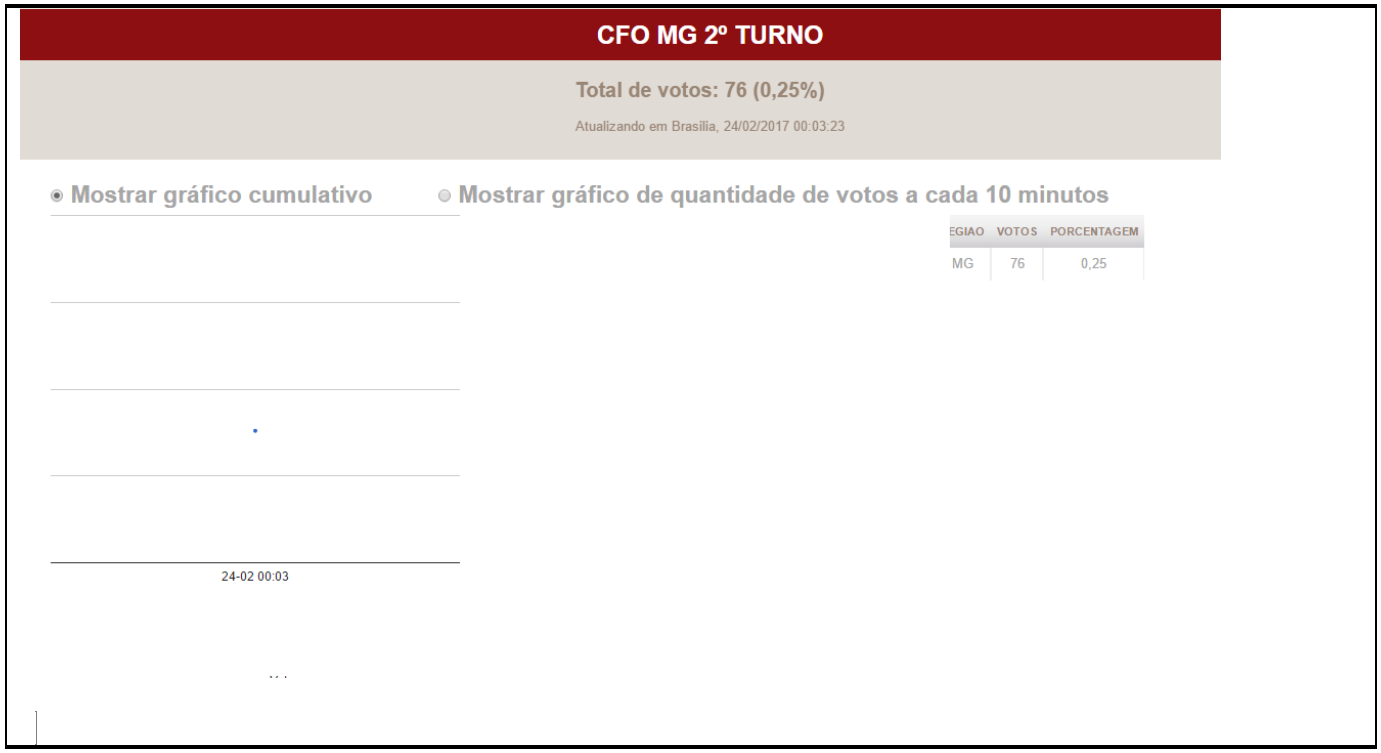
SEÇÃO II – ESCLARECIMENTOS E JUSTIFICATIVAS:

Justificativas/explicações sobre os testes de auditoria (as regras de negócio já estão fixadas):	Insecure Cookies e D - Non HTTP-Only Cookies- não coletam Informações do Sistema, sendo apenas cookies de controle de instâncias do sistema, para fins de operacionalização
Comentários	

SEÇÃO III – TELAS DE VOTAÇÃO:



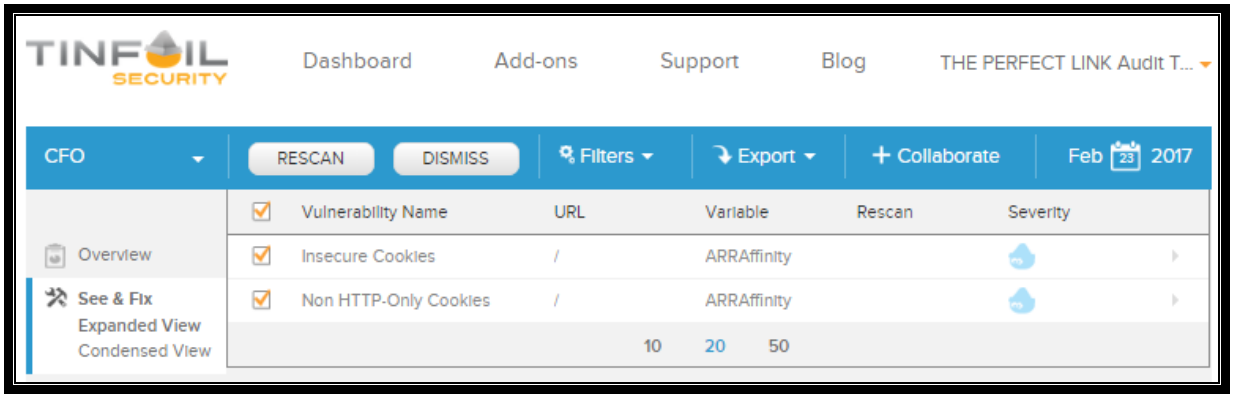

CONSELHO FEDERAL DE ODONTOLOGIA
ELEIÇÕES 2017
CONSELHOS REGIONAIS DE ODONTOLOGIA
CRO MG
IDENTIFICAÇÃO
VOTO
CONFIRMAR
FINAL
Voltar
IDENTIFICAÇÃO
MG
TROCAR CRO
CPF
Data de Nascimento
Senha
INICIAR VOTAÇÃO
CONSELHO FEDERAL DE ODONTOLOGIA
ELEIÇÕES 2017
CONSELHOS REGIONAIS DE ODONTOLOGIA
CRO SP
IDENTIFICAÇÃO
VOTO
CONFIRMAR
FINAL
Voltar
IDENTIFICAÇÃO
SP
TROCAR CRO
CPF
Data de Nascimento
Senha
INICIAR VOTAÇÃO
TROCAR SENHA
RECUPERAR SENHA


CFO MG 2º TURNO
Total de votos: 76 (0,25%)
Atualizando em Brasília, 24/02/2017 00:03:23
Mostrar gráfico cumulativo
Mostrar gráfico de quantidade de votos a cada 10 minutos
EGIAO VOTOS PORCENTAGEM
MG 76 0,25
24-02 00:03

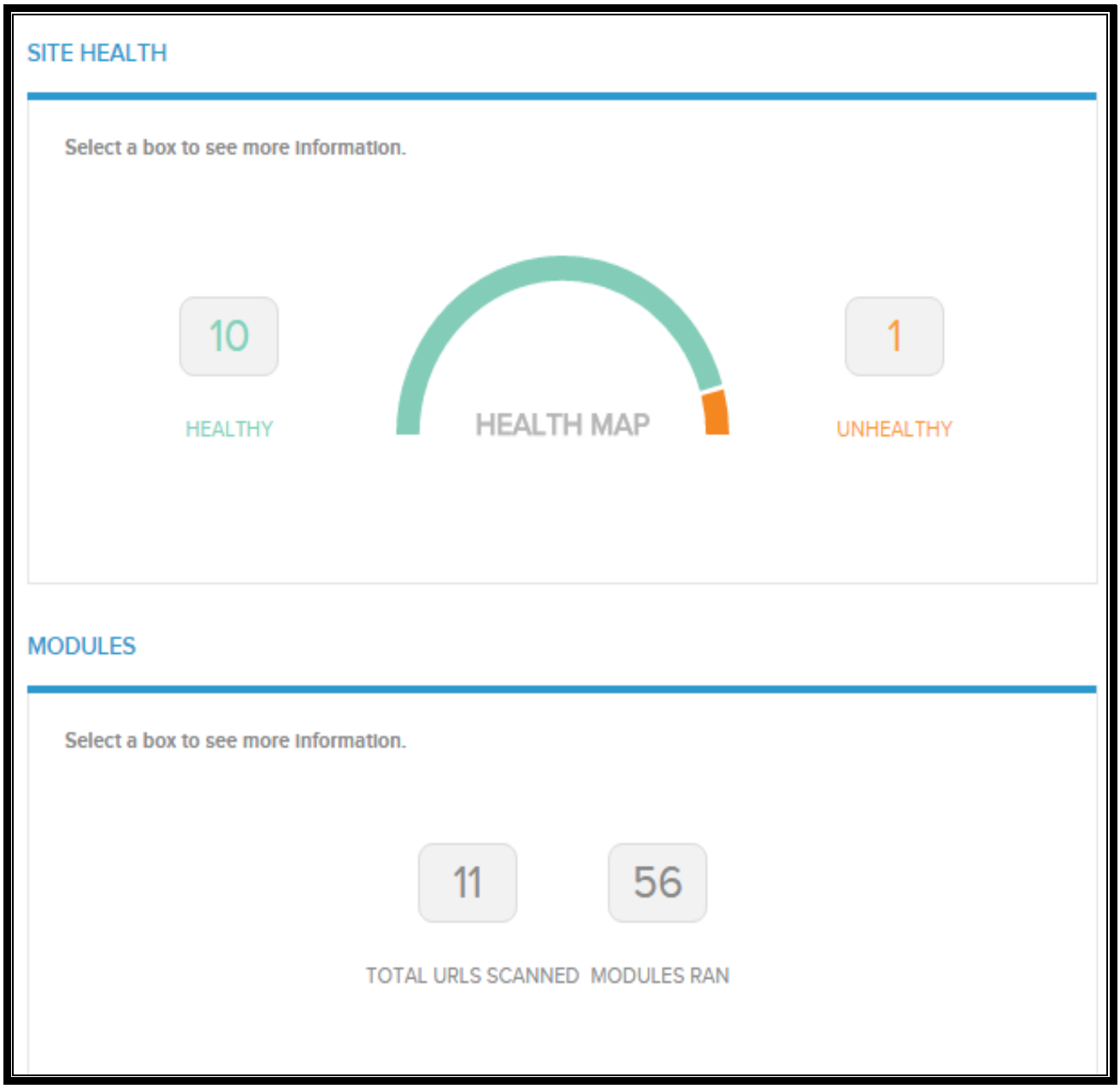
SEÇÃO IV – TESTES DE SITE E SISTEMAS:

1 – Testes:

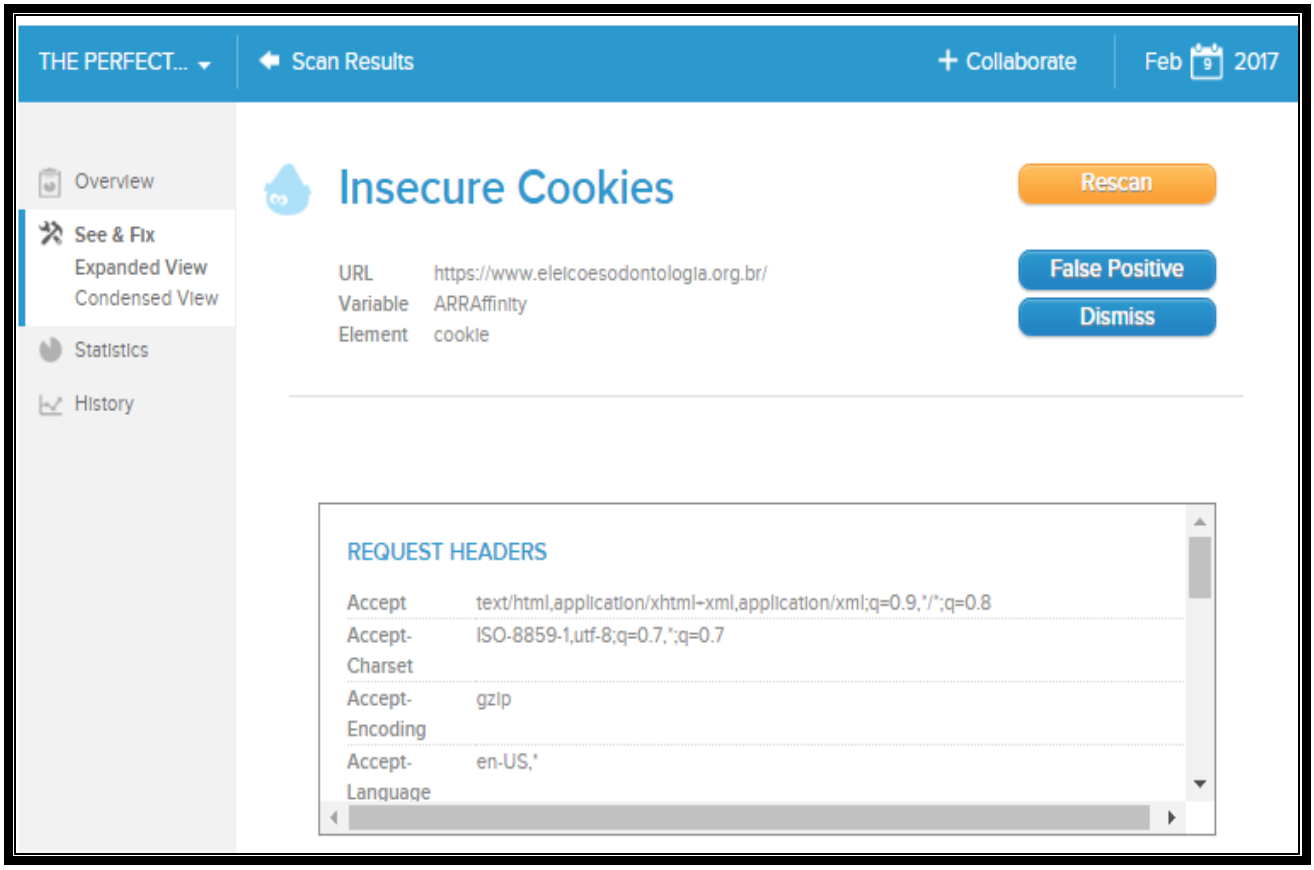
1.1 – Resumo dos testes:



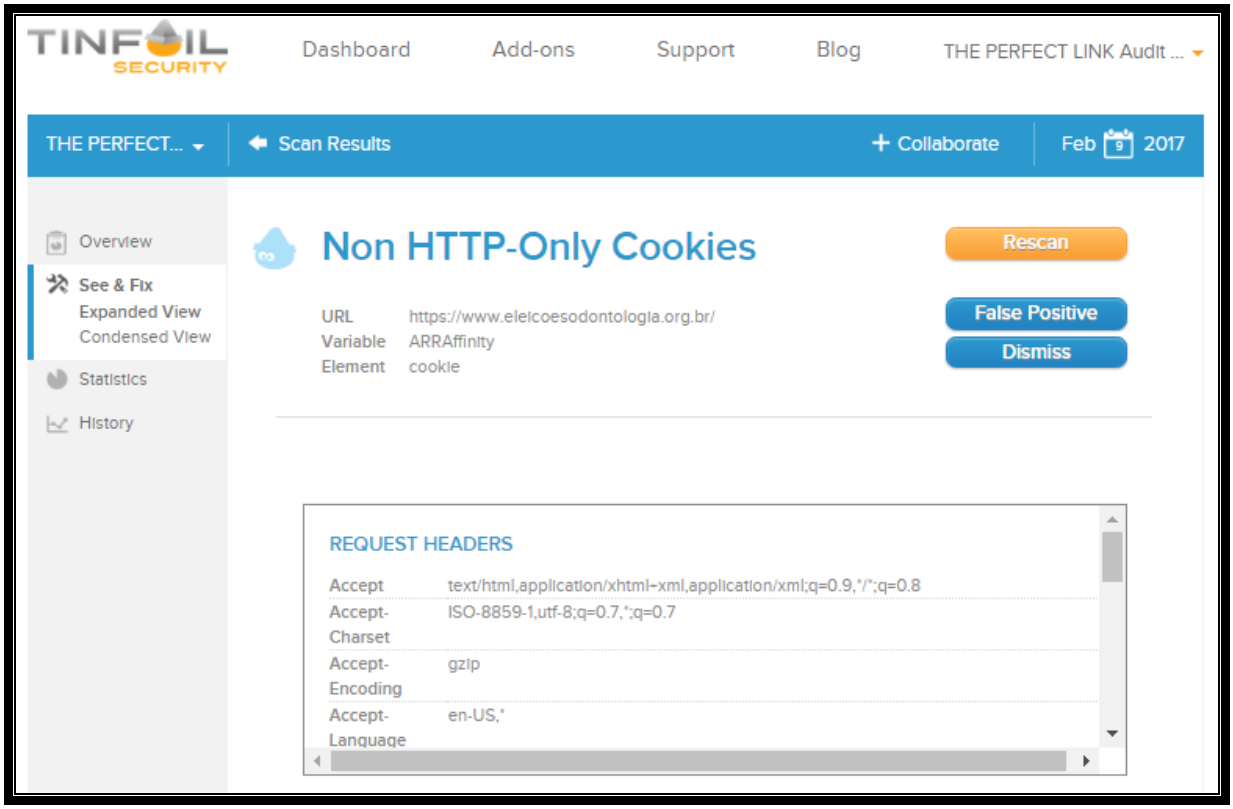
1.2 – Estatísticas:



1.3 – Itens Verificados - A:



1.3 – Itens Verificados - B:



1.4 – Itens Verificados:

1.4 – Itens Verificados:

Cross-Site Scripting in HTML "script" tag

Cross-Site Scripting in HTML tag

Cross-Site Scripting in HTML "vbscript" tag

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) in path

CVS/SVN user disclosure

Directory listing is enabled.

Disclosed e-mail address

Disclosed US Social Security Number

File Inclusion

Found a CAPTCHA protected form

Found an HTML object

Found Robots.txt

Found Stacktrace

HTTP PUT is enabled

Insecure Cookies

LDAP Injection

Misconfiguration in LIMIT directive of .htaccess file

Missing Subresource Integrity Protection

Mixed Resource

1.4 – Itens Verificados:

Non HTTP-Only Cookies

OpenSSL Heartbeat Extension Memory Leak (Heartbleed)

Operating system command injection

Password field with autocomplete

Password Submission via GET

Path Traversal

Persistent Cross-Site Scripting (XSS)

Private IP address disclosure

Remote file inclusion

Response splitting

Scriptless Cross-Site Scripting in attribute of HTML element

Server-Side Include Injection

Shellshock

Spammable contact form

SQL Injection

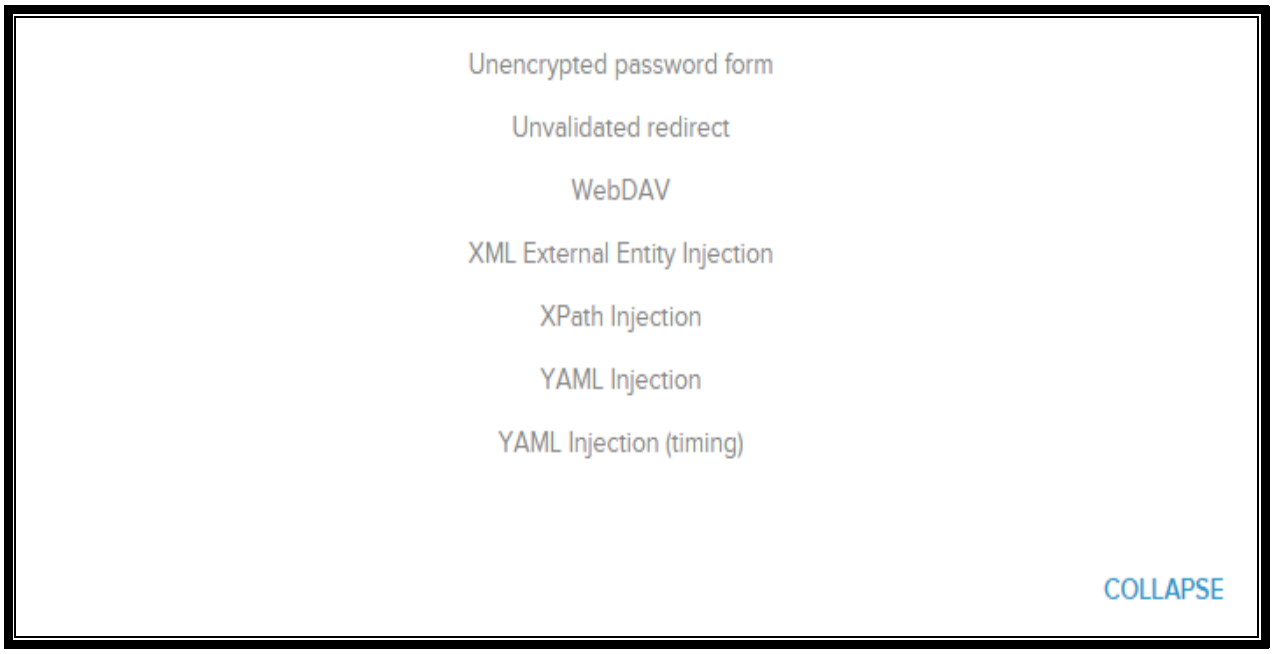
The TRACE HTTP method is enabled

TLS Fallback is not Supported

TLS Vulnerable to POODLE

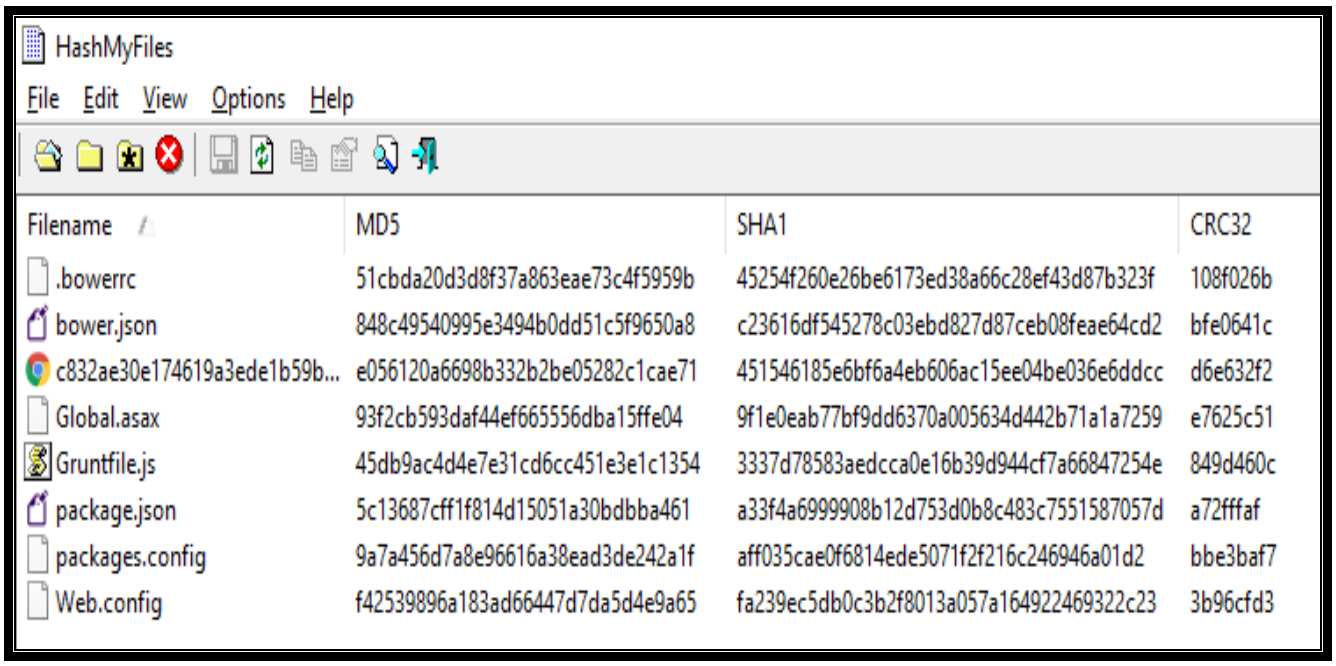
Unencrypted HTTP Basic Authentication

1.4 – Itens Verificados:

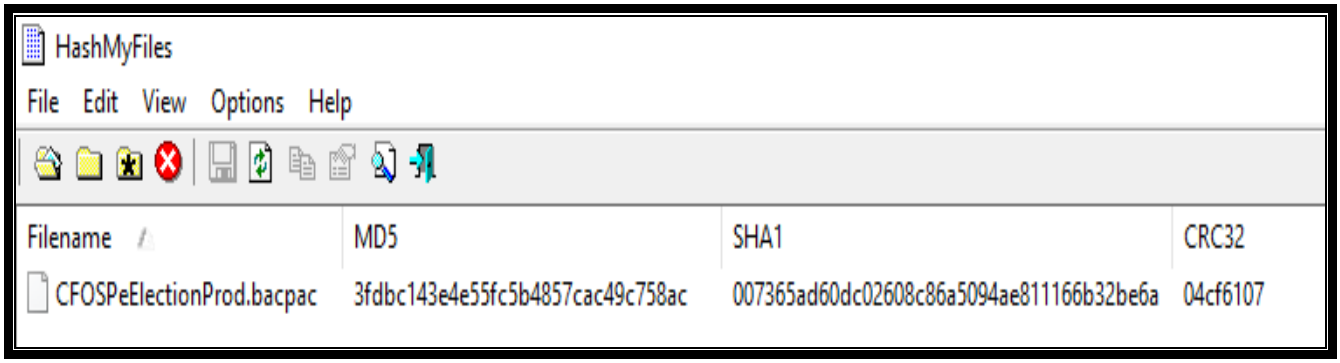


SEÇÃO V – HASHES E CONTROLES:

A – Hash dos Executáveis:

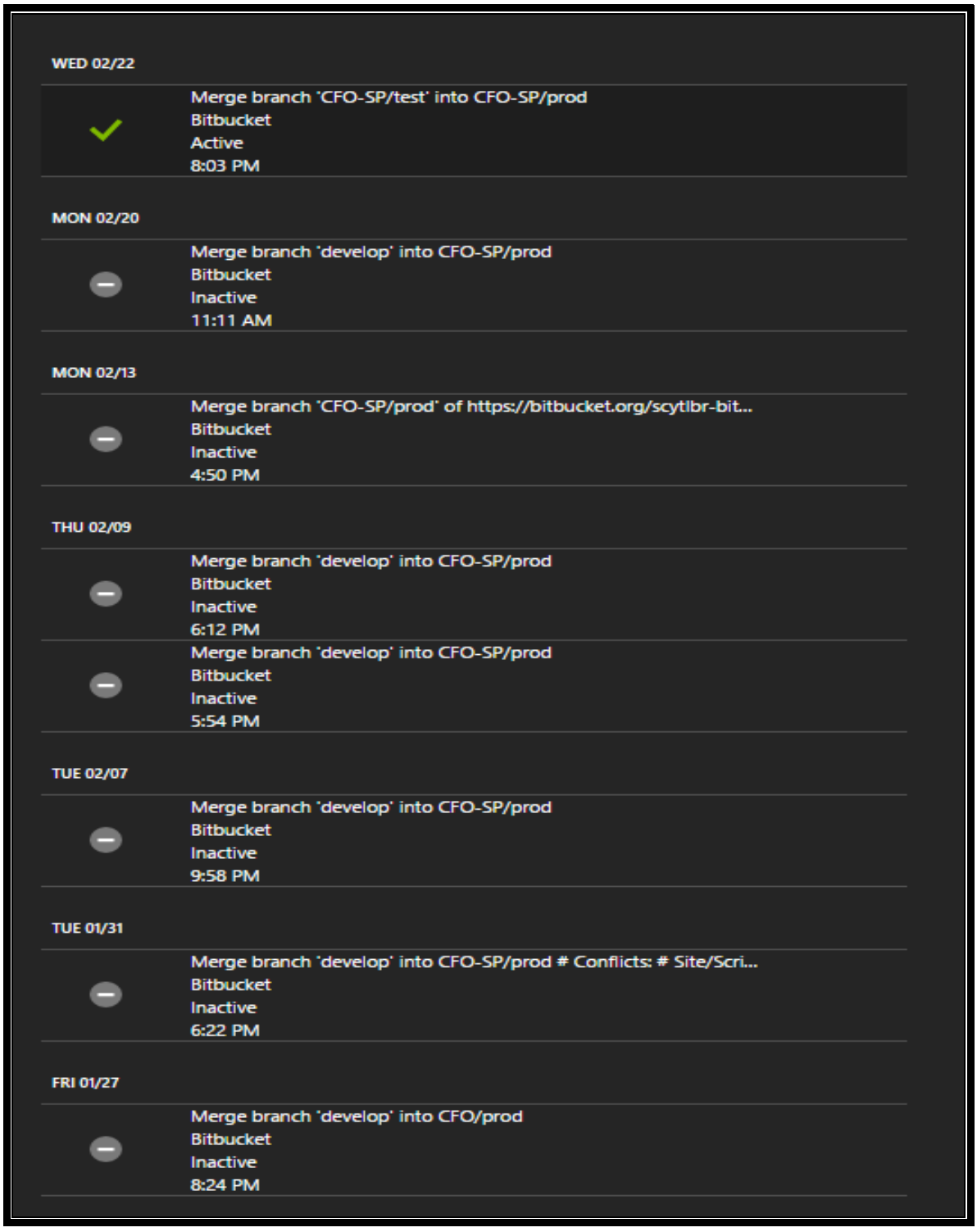


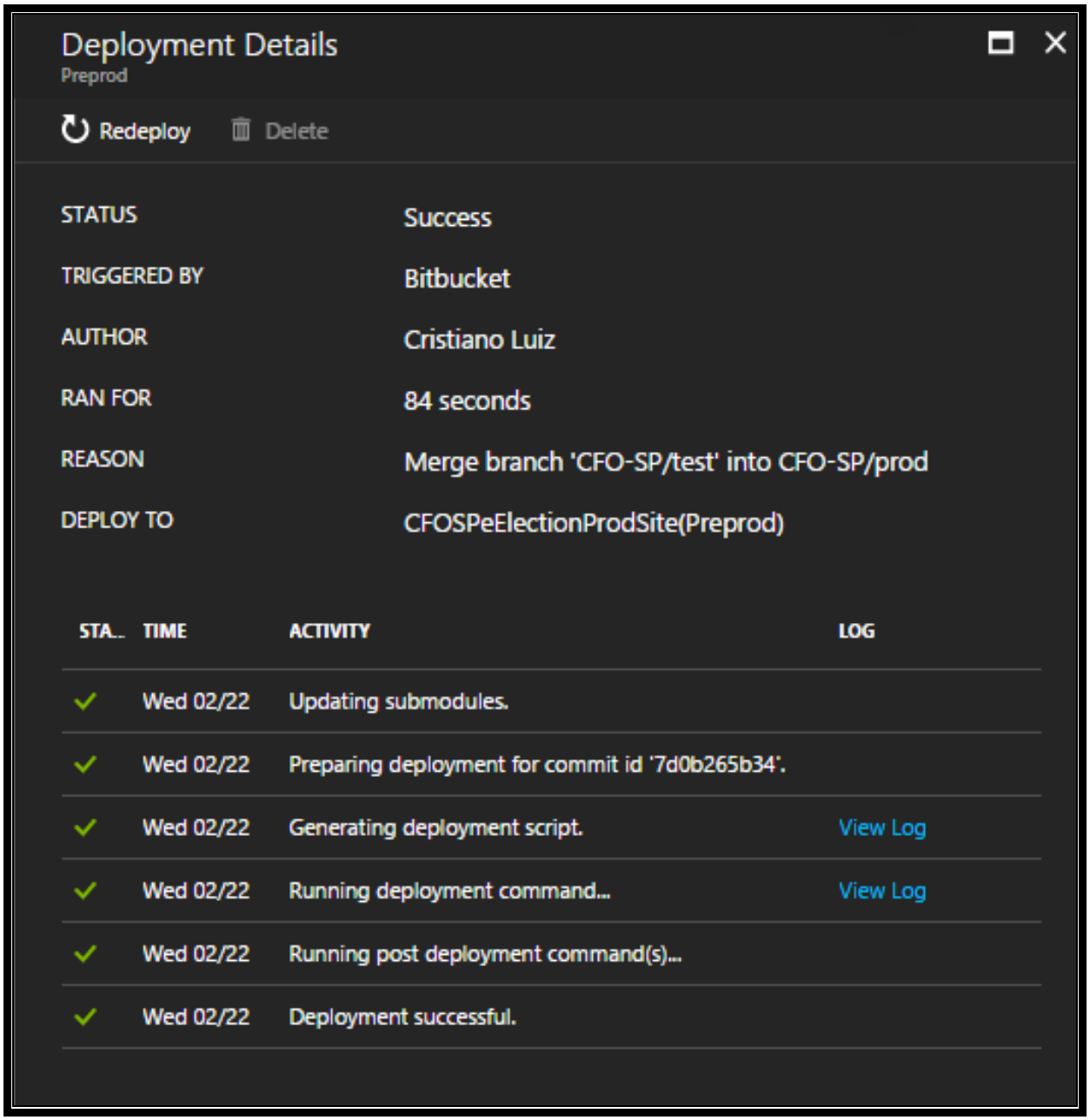
Filename	MD5	SHA1	CRC32
.bowerrc	51cbda20d3d8f37a863eae73c4f5959b	45254f260e26be6173ed38a66c28ef43d87b323f	108f026b
bower.json	848c49540995e3494b0dd51c5f9650a8	c23616df545278c03ebd827d87ceb08feae64cd2	bfe0641c
c832ae30e174619a3ede1b59b...	e056120a6698b332b2be05282c1cae71	451546185e6bf6a4eb606ac15ee04be036e6ddcc	d6e632f2
Global.asax	93f2cb593daf44ef665556dba15ffe04	9f1e0eab77bf9dd6370a005634d442b71a1a7259	e7625c51
Gruntfile.js	45db9ac4d4e7e31cd6cc451e3e1c1354	3337d78583aedcca0e16b39d944cf7a66847254e	849d460c
package.json	5c13687cff1f814d15051a30bdbba461	a33f4a6999908b12d753d0b8c483c7551587057d	a72fffaf
packages.config	9a7a456d7a8e96616a38ead3de242a1f	aff035cae0f6814ede5071f2f216c246946a01d2	bbe3baf7
Web.config	f42539896a183ad66447d7da5d4e9a65	fa239ec5db0c3b2f8013a057a164922469322c23	3b96cfd3



Filename	MD5	SHA1	CRC32
CFOSPeElectionProd.bacpac	3fdbc143e4e55fc5b4857cac49c758ac	007365ad60dc02608c86a5094ae811166b32be6a	04cf6107

B – Relatório da Última Publicação Antes da Votação:




Deployment Details
Preprod
Redeploy
Delete
STATUS
Success
TRIGGERED BY
Bitbucket
AUTHOR
Cristiano Luiz
RAN FOR
84 seconds
REASON
Merge branch 'CFO-SP/test' into CFO-SP/prod
DEPLOY TO
CFOSPeElectionProdSite(Preprod)
STA..
TIME
ACTIVITY
LOG
Wed 02/22
Updating submodules.
Wed 02/22
Preparing deployment for commit id '7d0b265b34'.
Wed 02/22
Generating deployment script.
View Log
Wed 02/22
Running deployment command...
View Log
Wed 02/22
Running post deployment command(s)...
Wed 02/22
Deployment successful.

C – Zerésima:

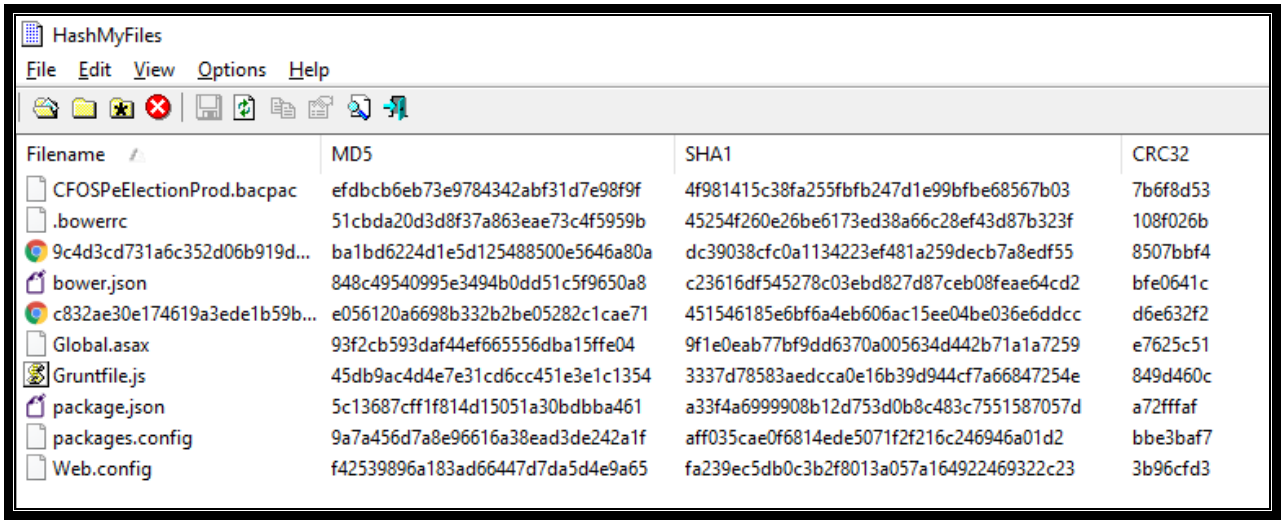
Resultados - MG

Apuração de 23/02/2017 18:22:41 (Horário de Brasília)

ELEIÇÃO CRO-MG			
Chapa	Votos	Percentual	% Válidos
Votos em Branco	0	0,00	-
Votos Nulos	0	0,00	-
CHAPA - 2	0	0,00	0,00
CHAPA - 1	0	0,00	0,00
Total	**0 (0 válidos)**	**100**	**100**

** %Validos não contabilizam votos brancos e/ou nulos*

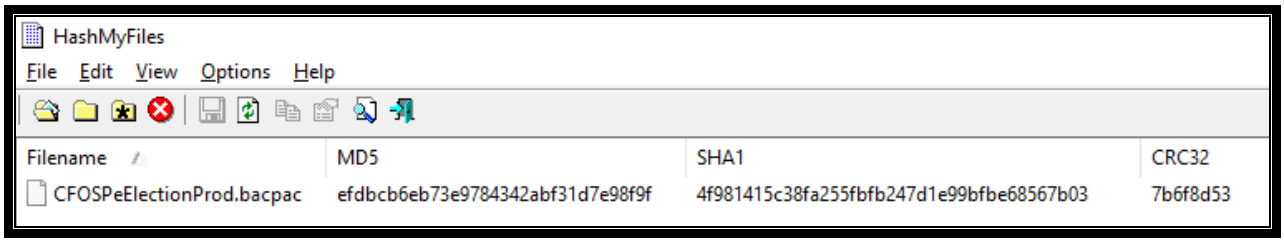
D – Hash dos Executáveis Após a Eleição:



HashMyFiles

File Edit View Options Help

Filename	MD5	SHA1	CRC32
CFOSPeElectionProd.bacpac	efdbcb6eb73e9784342abf31d7e98f9f	4f981415c38fa255fbfb247d1e99bfbe68567b03	7b6f8d53
.bowerrc	51cbda20d3d8f37a863eae73c4f5959b	45254f260e26be6173ed38a66c28ef43d87b323f	108f026b
9c4d3cd731a6c352d06b919d...	ba1bd6224d1e5d125488500e5646a80a	dc39038cfc0a1134223ef481a259decb7a8edf55	8507bbf4
bower.json	848c49540995e3494b0dd51c5f9650a8	c23616df545278c03ebd827d87ceb08feae64cd2	bfe0641c
c832ae30e174619a3ede1b59b...	e056120a6698b332b2be05282c1cae71	451546185e6bf6a4eb606ac15ee04be036e6ddcc	d6e632f2
Global.asax	93f2cb593daf44ef665556dba15ffe04	9f1e0eab77bf9dd6370a005634d442b71a1a7259	e7625c51
Gruntfile.js	45db9ac4d4e7e31cd6cc451e3e1c1354	3337d78583aedcca0e16b39d944cf7a66847254e	849d460c
package.json	5c13687cff1f814d15051a30bdbba461	a33f4a6999908b12d753d0b8c483c7551587057d	a72fffaf
packages.config	9a7a456d7a8e96616a38ead3de242a1f	aff035cae0f6814ede5071f2f216c246946a01d2	bbe3baf7
Web.config	f42539896a183ad66447d7da5d4e9a65	fa239ec5db0c3b2f8013a057a164922469322c23	3b96cfd3

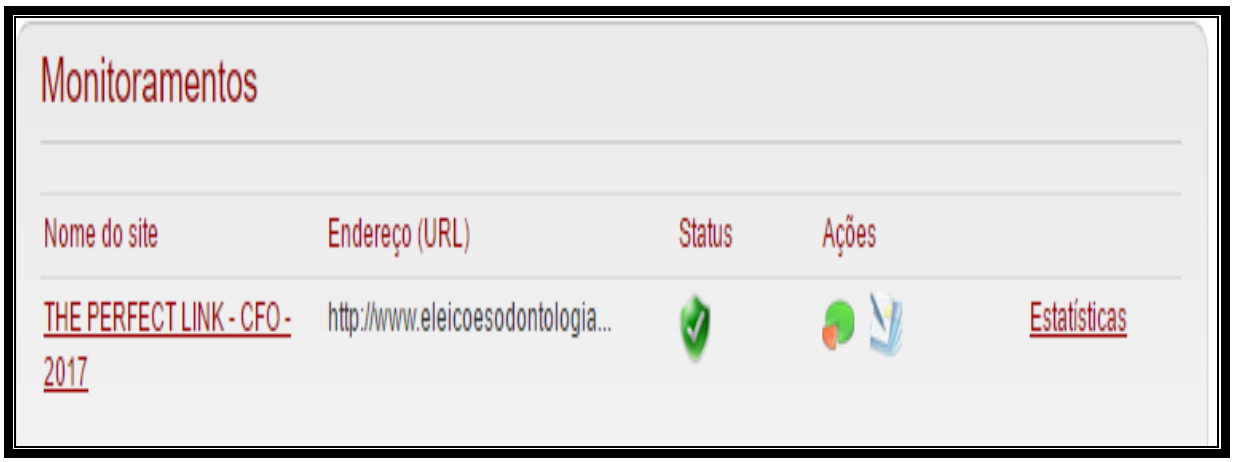


HashMyFiles

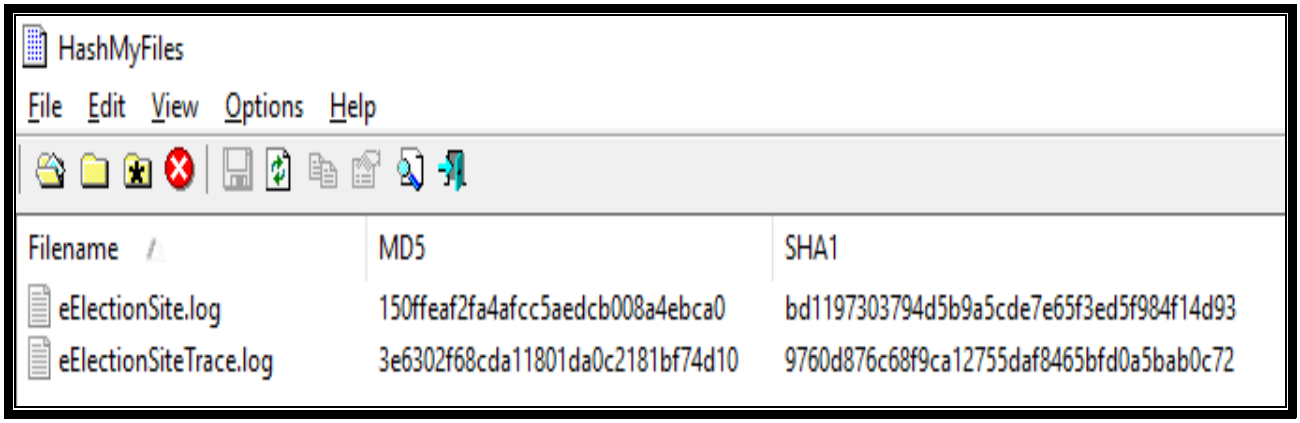
File Edit View Options Help

Filename	MD5	SHA1	CRC32
CFOSPeElectionProd.bacpac	efdbcb6eb73e9784342abf31d7e98f9f	4f981415c38fa255fbfb247d1e99bfbe68567b03	7b6f8d53

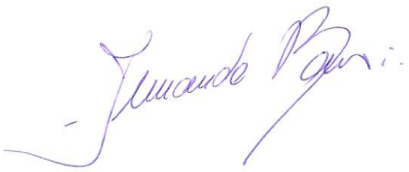
E – Resultado do Monitoramento:



F – Hash dos Logs de Votação:



Qualificação e Assinatura do Auditor:



Fernando De Pinho Barreira

Auditor e Perito Criminal em Forense Computacional
Técnico em Processamento de Dados
Analista de Sistemas
Administrador/Auditor de Empresas com Ênfase em Sistemas
Bacharel em Direito
Especialista em Direito Eletrônico
Especialista em Perícia Criminal
Especializado em Sociedade da Informação e Direito de Autor – Universidade de Lisboa
Membro da The British Society of Criminology - UK
Membro da HTCIA - High Technology Crime Investigation Association - EUA
Membro da ACJC – The Academy of Criminal Justice Sciences – EUA
Membro da IACIS - International Association of Computer Investigative Specialists - EUA
Membro da APDI - Associação Portuguesa de Direito Intelectual - POR.
CRA Nº 70.675
THE PERFECT LINK

THE PERFECT LINK Forensics Team

São Paulo, 24 de fevereiro de 2017.

http://www.theperfectlink.com.br
auditoria@theperfectlink.com.br
@PerfectLINK

Nossos Telefones:

São Paulo	**+5511 3663-6060**
São Paulo	**+5511 98540-0660**
Brasília	**+5561 99861-0660**