



**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA MECÂNICA**

**PROPOSTA DE PERFIL DE PROTEÇÃO PARA HOMOLOGAÇÃO E
CERTIFICAÇÃO DE PRODUTO CIBERNÉTICO: O CASO DOS
EQUIPAMENTOS DE VIDEOCONFERÊNCIA**

ARIANE CRISTINA BRITO FLORENTINO

**ORIENTADOR: SANDERSON CÉSAR MACÊDO BARBALHO
DISSERTAÇÃO DE MESTRADO EM SISTEMAS MECATRÔNICOS**

BRASÍLIA

2017

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA MECÂNICA**

**PROPOSTA DE PERFIL DE PROTEÇÃO PARA HOMOLOGAÇÃO E
CERTIFICAÇÃO DE PRODUTO CIBERNÉTICO: O CASO DOS
EQUIPAMENTOS DE VIDEOCONFERÊNCIA**

ARIANE CRISTINA BRITO FLORENTINO

**DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA
MECÂNICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE
BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A
OBTENÇÃO DO GRAU DE MESTRE EM SISTEMAS MECATRÔNICOS**

APROVADA POR:

**Prof. Dr. Sanderson César Macêdo Barbalho
(ORIENTADOR, FT/UnB)**

**Prof. Dr. Paulo Roberto de Lira Gondim
(EXAMINADOR INTERNO, ENE/UnB)**

**Prof. Dr. Raphael Machado
(EXAMINADOR EXTERNO, Inmetro)**

BRASÍLIA, NOVEMBRO, 2017

FICHA CATALOGRÁFICA

Florentino, Ariane Cristina Brito

Proposta de perfil para homologação e certificação de produto cibernético: o caso dos equipamentos de videoconferência / Ariane Cristina Brito Florentino; orientador Sanderson César Macêdo Barbalho. - Brasília, 2017.
141 f.

Dissertação (Mestrado - Mestrado em Engenharia Mecatrônica) -- Universidade de Brasília, 2017.

1. Homologação. 2. Segurança. 3. Common Criteria. 4. Videoconferência.
I. Barbalho, Sanderson César Macêdo, orient. II. Título

REFERÊNCIA BIBLIOGRÁFICA

FLORENTINO, Ariane Cristina Brito. **Proposta de perfil para homologação e certificação de produto cibernético: o caso dos equipamentos de videoconferência**. 2017. 141 f. Dissertação (Mestrado) - Curso de Engenharia Mecatrônica, Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2017.

CESSÃO DE DIREITOS

AUTOR: Ariane Cristina Brito Florentino

TÍTULO: Proposta de perfil para homologação e certificação de produto cibernético: o caso dos equipamentos de videoconferência

GRAU: Mestre Ano: 2017

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte desta dissertação de mestrado pode ser reproduzida sem autorização por escrito do autor.

Ariane Cristina Brito Florentino
arianecristin@hotmail.com

AGRADECIMENTOS

Agradeço primeiramente a Deus, por guiar meus passos a cada dia.

Ao meu orientador Prof. Dr. Sanderson César Macêdo Barbalho, pelo precioso período de aprendizado, pela confiança e pelas sábias palavras de orientação. Por proporcionar-me a oportunidade de atuar em estudos alinhados ao Programa de Defesa Cibernética Nacional.

Ao Prof. Dr. Edson Paulo da Silva, pelo direcionamento acadêmico.

Aos colegas e amigos que me acompanharam nesta caminhada, pelo companheirismo e motivação.

À minha família, pelo apoio sempre constante.

DEDICATÓRIA

À minha mãe Izabel, por todo apoio
e grandioso exemplo de vida.

RESUMO

O objetivo do trabalho é abordar a gestão da segurança da informação, propondo um perfil de proteção para homologação e certificação de produto de defesa cibernética na área de comunicações unificadas, mais especificamente nos equipamentos de videoconferência. A presente pesquisa apresenta a análise e definição do sistema de homologação cibernética da solução tecnológica, contemplando os principais pontos a serem considerados na aquisição e utilização desse produto mecatrônico. Serão abordados os seguintes aspectos: premissas de segurança da informação adequadas; normas técnicas, recomendações e melhores práticas internacionais de defesa cibernética. O estudo buscará elaborar um perfil de proteção segundo os critérios do *Common Criteria*, identificando principalmente quais os riscos de segurança da informação envolvidos e quais devem ser os parâmetros mínimos a serem exigidos nesses sistemas, quando de sua aquisição e utilização, considerando o grupo de consumidores da Administração Pública Federal.

Palavras-chave: Homologação. Segurança. *Common Criteria*. Videoconferência.

ABSTRACT

The objective of this work is to address the management of information security by proposing a protection profile for homologation and certification of a cyber defense product in the area of unified communications, more specifically in videoconferencing equipment. The present research presents the analysis and definition of the cybernetic homologation system of the technological solution, contemplating the main points to be considered in the acquisition and use of this mechatronic product. The following aspects will be addressed: adequate information security assumptions; Technical standards, recommendations and international best practices in cyber defense. The study will seek to elaborate a protection profile according to the criteria of the Common Criteria, identifying mainly the information security risks involved and what should be the minimum parameters to be required in those systems when they are acquired and used, considering the group of consumers of the Federal Public Administration.

Key words: Homologation. Security. *Common Criteria*. Videoconferencing.

SUMÁRIO

RESUMO.....	vi
LISTA DE FIGURAS	xi
LISTA DE QUADROS E TABELAS	xiii
LISTA DE ABREVIATURAS E SIGLAS	xiv
1. INTRODUÇÃO.....	18
1.1 DELIMITAÇÃO DO PROBLEMA.....	18
1.2 FORMULAÇÃO DA SITUAÇÃO PROBLEMA	19
1.3 OBJETIVOS.....	19
1.3.1 Objetivo Geral.....	19
1.3.2 Objetivos Específicos.....	20
1.4 JUSTIFICATIVA	20
1.5 SEÇÕES COMPONENTES DO TRABALHO	21
2 FUNDAMENTAÇÃO CONCEITUAL	22
2.1 DEFESA CIBERNÉTICA.....	22
2.2 PRODUTO MECATRÔNICO	24
2.3 COMUNICAÇÕES UNIFICADAS E VIDEOCONFERÊNCIA	25
2.4 PRINCÍPIOS DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO E COMUNICAÇÕES	27
2.4.1 Integridade	28
2.4.2 Confidencialidade	28
2.4.3 Disponibilidade	29
2.4.4 Autenticidade	29
2.4.5 Não-repúdio	29

2.5 PADRÕES DE HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC).....	29
2.5.1 Common Criteria.....	32
2.5.2 Metodologias de avaliação de segurança de sistemas de informação.....	34
3 MATERIAIS E MÉTODOS.....	49
3.1 ETAPAS DE EXECUÇÃO DO TRABALHO	49
3.2 FERRAMENTAS UTILIZADAS	51
3.3 PLANEJAMENTO DE EXPERIMENTOS CIENTÍFICOS	51
4 DESENVOLVIMENTO DO PROTECTION PROFILE.....	56
4.1 DEFINIÇÃO DO TOE	57
4.1.1 Instalação básica do TOE.....	59
4.1.2 Escopos físico e lógico do TOE.....	60
4.1.2.1 SUPORTE À CRIPTOGRAFIA	62
4.1.2.2 IDENTIFICAÇÃO E AUTENTICAÇÃO.....	62
4.1.2.3 AUDITORIA DE SEGURANÇA	62
4.1.2.4 PROTEÇÃO ÀS CONFIGURAÇÕES DE SEGURANÇA DO TOE ..	63
4.1.2.5 CONTROLE DE ACESSO	63
4.1.2.6 UTILIZAÇÃO DE CANAIS CONFIÁVEIS	63
4.2 REQUISITOS DE SEGURANÇA	63
4.2.1 Requisitos de segurança do ambiente operacional do TOE.....	63
4.2.2 Requisitos de segurança funcionais do TOE.....	64
4.3 DEFINIÇÃO DO AMBIENTE DE SEGURANÇA	65
4.3.1 Ameaças	66
4.3.2 Premissas.....	68
4.3.3 Política de segurança da informação.....	68

4.4 PERFIL DE PROTEÇÃO DO TOE.....	69
5. RESULTADOS E DISCUSSÕES.....	83
5.1 RESULTADOS DOS REGISTROS	84
5.1.1 Análise estatística dos dados.....	90
5.2 ANÁLISES E DISCUSSÕES	92
6. CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS.....	94
REFERÊNCIAS BIBLIOGRÁFICAS	101
APÊNDICES	109
APÊNDICE A	110
APÊNDICE B.....	118
APÊNDICE C.....	122
ANEXOS	124
ANEXO A.....	125
ANEXO B	138
ANEXO C	140

LISTA DE FIGURAS

Figura 1 – Estrutura do Sistema Brasileiro de Defesa Cibernética (CBSI, 2014)	23
Figura 2 – Elementos da Mecatrônica (COLITEC, 2015).....	24
Figura 3 – Elementos de um Produto Mecatrônico (BARBALHO, 2016)	25
Figura 4 – Equipamento de videoconferência Huawei TE30 (AV-iQ, 2017)	26
Figura 5 - O processo DSRM (SILVA, 2014).....	35
Figura 6 – Metodologia da Pesquisa.....	49
Figura 7 – Estrutura do Produto Mecatrônico Equipamento de Videoconferência.....	57
Figura 8 – Estrutura Funcional do Equipamento de Videoconferência.....	58
Figura 9 – Exemplo de <i>deploy</i> do TOE	59
Figura 10 – Esquema lógico do sistema de análise	83
Figura 11 – Consulta dos registros em MANUTENÇÃO > REGISTROS.....	85
Figura 12 – Consulta dos registros: início, término e falha de chamada (linhas 16, 26 e 25/28/35, respectivamente).....	86
Figura 13 – Consulta do arquivo XML: falha no registro no servidor (destacado em 1); reset e alteração de configurações de segurança (destacados em 2 e 3).	86
Figura 14 – Teste Qui Quadrado sem correção	91
Figura 15 – Teste Qui Quadrado com correção de Yates.....	92
Figura 16 – Vista frontal do TOE.....	110
Figura 17 – Instalação básica do TOE.....	110
Figura 18 – Login no console administrativo remoto.....	111
Figura 19 – Resposta de retorno ao inserir credenciais erradas de login no TOE.....	111
Figura 20 – Tela do console administrativo remoto após efetuar login com credenciais corretas no TOE	112

Figura 21 – Log contendo registros de ligar o TOE (linha 6), configuração de informações de segurança (endereçamento IP - linhas 4, 5, 14 à 17), login e logout no console administrativo (linhas 24, 25, 29 a 31)	112
Figura 22 – Controle de vídeo console administrativo do TOE	113
Figura 23 – Alterações das configurações de segurança: criptografia e alteração da palavra-passe.....	113
Figura 24 – Alterações da configuração de segurança uso do protocolo H.460.	114
Figura 25 – Tentativa de alteração de palavra-passe com senha atual incorreta.....	114
Figura 26 – Registro de chamada com criptografia ativa no TOE	115
Figura 27 – Registro de chamada com criptografia ativa.	115
Figura 29 – Recusa da chamada sem criptografia ativa no TOE.....	116
Figura 30 – Chamada concluída com sucesso com a criptografia desativada no destino (TOE) e na origem da chamada (<i>Jabber</i>).....	117
Figura 31 – Informações no TOE da chamada concluída com sucesso com a criptografia desativada no destino (TOE) e na origem da chamada (<i>Jabber</i>).....	117

LISTA DE QUADROS E TABELAS

Quadro 1 – Comparação dos níveis de segurança Common Criteria, TCSEC e ITSEC.....	30
Quadro 2 – Resumo de metodologias de avaliação de segurança	38
Quadro 3 – Resumo dos testes não-paramétricos (VIALI, 2008)	53
Quadro 4 – Especificações do TOE (BRASIL, 2015d; BRASIL, 2015e; CISCO, 2016).....	60
Quadro 5 – Componentes do Ambiente de TI (BRASIL, 2015d; BRASIL, 2015e; CISCO, 2016)	63
Quadro 6 – Requisitos do TOE (BRASIL, 2015d; BRASIL, 2015e; CISCO, 2016).....	65
Quadro 7 – Requisitos funcionais e eventos auditáveis	77
Quadro 8 – Eventos verificados.....	87
Tabela 1 – Eventos pesquisados e ocorrências.....	90

LISTA DE ABREVIATURAS E SIGLAS

AAA	<i>Authentication, Authorization, and Accounting</i>
ABNT	Associação Brasileira de Normas Técnicas
AEC	Cancelamento de Eco Automático
AES	<i>Advanced Encryption Standard</i>
AGC	Controle do Ganho Automático
ANS	Supressão de Ruídos Automática
APF	Administração Pública Federal
AS/NZS	<i>Australian/ New Zealand Standard</i>
BFCP	<i>Binary Floor Control Protocol</i>
BS	<i>British Standard</i>
BSMI	<i>Bureau of Standards, Metrology, and Inspection</i>
CC	<i>Common Criteria</i>
COBIT	<i>Control Objectives for Information and related Technology</i>
COMDCIBER	Comando de Defesa Cibernética
CSI/FBI	<i>Crime Scene Investigation/ Federal Bureau of Investigation</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
DIN	<i>Deutsches Institut für Normung</i> (tipo de conector)
DNS	<i>Domain Name System</i>
DoS	<i>Denial of service</i>
DSRM	<i>Design Science Research Methodology</i>
DVI – I	<i>Digital Visual Interface</i>
EAL	<i>Evaluation Assurante Level</i>
EIA	<i>Electronic Industries Association</i>
ENaDCiber	Escola Nacional de Defesa Cibernética
ENaDCiber-SHCDCiber@DCN	Escola Nacional de Defesa Cibernética e do Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética
FAU	<i>Family Security Audit</i>
FAU_GEN	<i>Family Security Audit Data Generation</i>
FCS	<i>Family Cryptographic Support</i>

<i>FCS_COP</i>	<i>Family Cryptographic Operation</i>
<i>FIA</i>	<i>Family Identification and Autentication</i>
<i>FIA_AFL</i>	<i>Family Authentication Failures</i>
<i>FIA_SOS</i>	<i>Family Specification of Secrets</i>
<i>FIA_UAU</i>	<i>Family User Authentication</i>
<i>FPT</i>	<i>Family Protection of the TSF</i>
<i>FPT_FLS</i>	<i>Family Fail Secure</i>
<i>FPT_TEE</i>	<i>Family Testing of External Entities</i>
<i>FTA</i>	<i>Family TOE Access</i>
<i>FTA_MCS</i>	<i>Family Limitation on Multiple Concurrent Sessions</i>
<i>FTA_SSL</i>	<i>Family Session Locking and Termination</i>
<i>FTP</i>	<i>Family Trusted Path/Channels</i>
<i>FTP_TRP</i>	<i>Family Trusted Path</i>
<i>GAISP</i>	<i>Generally Accepted Information Security Principles</i>
<i>GASPP/</i>	<i>Global Alliance for Project Performance Standards</i>
<i>GSIPR</i>	<i>Gabinete da Segurança Institucional da Presidência da República</i>
<i>HD</i>	<i>High Definition</i>
<i>HDMI</i>	<i>High-Definition Multimedia Interface</i>
<i>HTTPS</i>	<i>Hyper Text Transfer Protocol Secure</i>
<i>IEC</i>	<i>International Electrotechnical Commission</i>
<i>IEEE</i>	<i>Institute of Electrical and Electronics Engineers</i>
<i>IETF</i>	<i>Internet Engineering Task Force</i>
<i>iOT</i>	<i>Internet of Tthings</i>
<i>IP</i>	<i>Internet Protocol</i>
<i>IPv4</i>	<i>Internet Protocol version 4</i>
<i>IPv6</i>	<i>Internet Protocol version 6</i>
<i>ISO</i>	<i>International Organization for Standardization/</i>
<i>ITSEC</i>	<i>Information Technology Security Evaluation Criteria</i>
<i>ITU-T</i>	<i>International Telecommunications Union - Telecommunication Standardization</i>
<i>Sector</i>	
<i>MACBETH</i>	<i>Measuring Attractiveness by a Categorical Based Evolution Technique</i>

MCU	<i>Multipoint Control Unit</i>
NBR	Norma Brasileira
NDPP	<i>Protection Profile for Network Devices</i>
NRI	<i>Network Readiness Index</i>
NTP	<i>Network Time Protocol</i>
OCTAVE	<i>Operationally Critical Threat, Asset, and Vulnerability Evaluation</i>
OSI	<i>Open Systems Interconnection</i>
PC	<i>Personal Computers</i>
POSIC	Política de Segurança da Informação
PP	<i>Protection Profile</i>
PTZ	<i>Pan/Tilt/Zoom</i>
QoS	<i>Quality of Service</i>
RCA	<i>Radio Corporation of America</i> (tipo de conector)
RDS	Rádio Definido por Software
RENASIC	Rede Nacional de Segurança da Informação e Criptografia
RFC	<i>Request for Comments</i>
RJ45	<i>Registered Jack</i> (tipo de conector)
SGSI	Sistema de Gestão de Segurança da Informação
SHCDCiber Cibernética	Sistema de Homologação e Certificação de Produtos e Serviços de Defesa
SI	Segurança da Informação
SIC	Segurança da informação e Comunicações
SIP	<i>Session Initiation Protocol</i>
SIPEP	<i>Extended Package SIP Server</i>
SNMP	<i>Simple Network Management Protocol</i>
SRTTP	<i>Secure Real-time Transport Protocol</i>
SSE-CMM	<i>Systems Security Engineering Capability Maturity Model</i>
ST	<i>Security Targets</i>
SVGA	<i>Super Video Graphics Array</i>
TAG's	<i>Threshold Assessment Grid</i>
TCI	Tecnologias de Comunicação e Informação

<i>TCP</i>	<i>Transmission Control Protocol</i>
<i>TCSEC</i>	<i>Trusted Computer System Evaluation Criteria</i>
<i>TI</i>	Tecnologia da Informação
<i>TIA</i>	<i>Telecommunications Industry Association</i>
<i>TIC</i>	Tecnologia da Informação e Comunicação
<i>TLS</i>	<i>Transport Layer Security</i>
<i>TOE</i>	<i>Target of Evaluation</i>
<i>TSF</i>	<i>TOE Security Functionality</i>
<i>UDP</i>	<i>User Datagram Protocol</i>
<i>VGA</i>	<i>Video Graphics Array</i>
<i>VoIP</i>	<i>Voice Over IP</i>
<i>WEF</i>	<i>World Economic Forum</i>
<i>WWDG</i>	<i>Window Watchdog</i>
<i>XML</i>	<i>eXtensible Markup Language</i>
<i>XVGA</i>	<i>Extended Video Graphics Array</i>

1. INTRODUÇÃO

1.1 DELIMITAÇÃO DO PROBLEMA

Segundo JUNIOR (2011), a utilização dos sistemas de informação pelas organizações tornou-se questão de sobrevivência em meados de 1990. Sejam elas públicas ou privadas, a informação é extremamente valiosa para essas entidades, considerando que é a base de suas tomadas de decisões.

“À medida que cresce nossa capacidade de colher, processar e distribuir informações torna-se ainda maior a demanda por formas mais sofisticadas de processamento de informação” (TANENBAUM; WETHERALL, 2011).

O conhecimento dos melhores sistemas e processos para processar a informação, criando novas tecnologias, ou aprimorando as existentes, propicia às entidades maior competitividade.

Conforme o Índice de Tecnologia da Informação (*Network Readiness Index – NRI*) divulgado pelo *World Economic Forum* (Fórum Econômico Mundial – WEF) em abril/2015, o Brasil ocupa a 84ª posição no ranking entre 143 economias lideradas por Cingapura. Essa pontuação mede o preparo das nações em utilizar tecnologias de comunicação e informação (TCI).

O relatório emitido pelo WEF atesta a alta correspondência entre “a adoção das TCI por indivíduos, empresas e governos, e a capacidade de gerar o impacto econômico e social” (WEF, 2015). Ele ressalta ainda que “a liderança governamental é um requisito fundamental para todos os países na criação de um ambiente comercial e regulamentar favorável e de um mercado das TIC competitivo” (WEF, 2015).

Percebe-se o alto grau de dependência tecnológica brasileira ao observar também a balança econômica brasileira. Dentre os itens importados pelo país no último mês de julho de 2015 encontram-se químicos orgânicos/inorgânicos, equipamentos mecânicos, aparelhos eletroeletrônicos, veículos automóveis e partes (BRASIL, 2015c).

A ascensão econômica, a postura política, o desenvolvimento social e os grandes eventos que ocorreram no Brasil além de atrair turistas e investidores têm chamado a atenção dos hackers.

O número de incidentes reportados ao CERT.br em 2014 atingiu mais de um milhão de registros, quase triplicando os registros do ano anterior.

Ponderando o exposto, a inovação tecnológica, considerada extremamente vital ao desenvolvimento econômico das nações, requer atenção à segurança cibernética no que tange às pessoas, infraestruturas, informações e dados. Rússia, Índia, China e Estados Unidos são alguns dos países que já institucionalizaram o tema e determinaram órgãos exclusivos para tratar de estratégias nesse campo (JÚNIOR, 2013).

O Brasil tem realizado estudos recentes em defesa cibernética na Defesa Nacional no Ministério da Defesa por meio do Centro de Defesa Cibernética do Departamento de Ciência e Tecnologia do Exército. Seu principal objetivo é desenvolver elementos que possibilitem estruturar o Comando de Defesa Cibernética, pois devem ser considerados o risco à soberania do país.

1.2 FORMULAÇÃO DA SITUAÇÃO PROBLEMA

A questão central que será estudada é: o que deve conter em um perfil de proteção de homologação e certificação de equipamento de videoconferência, considerando as normas da Associação Brasileira de Normas Técnicas (ABNT) NBR 27001:2006 [ABNT, 2006], NBR 27002:2005 [ABNT, 2005], NBR 27005:2008 [ABNT, 2008], além das Normas Complementares 07 [DSIC/GSIPR, 2010a] e 17 [DSIC/GSIPR, 2013c] do Gabinete da Segurança Institucional da Presidência da República (GSIPR), e padrões internacionais como o *Common Criteria*?

Esta questão principal desdobra-se nas seguintes:

- 1) Quais são os critérios de segurança a serem considerados no modelo proposto?
- 2) É possível aplicar um modelo baseado no *Common Criteria* em um equipamento de vídeo conferência de uso comercial, em ambiente controlado?
- 3) Os resultados da aplicação do modelo proposto a um caso real validam o PP desenvolvido?

1.3 OBJETIVOS

1.3.1 Objetivo Geral

O objetivo geral dessa pesquisa é propor um perfil de proteção para homologação e certificação do produto mecatrônico equipamento de videoconferência, utilizando como base o padrão *Common Criteria*.

1.3.2 Objetivos Específicos

Os objetivos específicos desta pesquisa são:

- a) Identificar o estado da arte da literatura científica sobre homologação e certificação de produtos de defesa cibernética;
- b) Caracterizar o sistema de videoconferência como produto mecatrônico;
- c) Definir *protection profile* baseado no modelo *Common Criteria*;
- d) Levantar estado da arte da análise de equipamento de videoconferência sob aspecto da defesa cibernética;
- e) Analisar o produto equipamento de videoconferência com o *protection profile*.

1.4 JUSTIFICATIVA

A Tecnologia da Informação (TI) pode ser considerada a base para o modelo operacional de diversas entidades, além do que "A dependência frente à infraestrutura exige cada vez mais a participação dos gestores de TI no planejamento organizacional, bem como os gestores de telecomunicações na formulação de políticas públicas" (JUNIOR, 2011).

Diversos dados sensíveis trafegam pelos sistemas de comunicações unificadas, sejam em reuniões virtuais, videoconferências ou web chats realizados entre as diferentes entidades da APF.

Garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação é vital para o estabelecimento de estratégias e ao suporte à decisão, principalmente considerando o campo de atuação da administração pública federal (APF).

Assim, a proposta da pesquisa é definir um sistema para homologar e certificar um produto de defesa cibernética na área de comunicações unificadas, orientando as organizações da APF quando de sua aquisição.

Qualquer falha de gestão de segurança pode impactar negativamente a organização, alterando sua disponibilidade de serviços, trazendo prejuízos financeiros e de imagem, e até mesmo multas e sanções administrativas aos envolvidos.

Assim, a pesquisa que será produzida aborda a defesa cibernética nas homologações e certificações do produto mecatrônico "equipamento de videoconferência", uma tipologia de produto mecatrônico que apesar de não conter alto grau de automação é bastante crítico sob o aspecto da segurança de informação.

1.5 SEÇÕES COMPONENTES DO TRABALHO

As próximas seções deste trabalho são organizadas da seguinte forma: a segunda seção aborda a fundamentação teórica, incluindo conceitos de defesa cibernética, mecatrônica, comunicações unificadas e videoconferência, princípios de segurança em sistemas de informação e comunicações, padrões de homologação e certificação de produtos de tecnologia da informação e comunicação, e planejamento de experimentos científicos; enquanto a seção 3 apresenta a metodologia, os materiais e os métodos utilizados. Na quarta seção, é apresentado o desenvolvimento do *protection profile*. Na 5ª seção, os resultados e análises são tratados, e na 6ª seção as conclusões estão expostas.

2 FUNDAMENTAÇÃO CONCEITUAL

A presente pesquisa transitará pelos seguintes conceitos: defesa cibernética; produto mecatrônico; comunicações unificadas e videoconferência; princípios de segurança em sistemas de informação e comunicações; padrões de homologação e certificação de produtos de tecnologia da informação e comunicação (TIC).

2.1 DEFESA CIBERNÉTICA

A cibernética compreende a utilização de distintos meios tecnológicos, envolvendo sistemas de informação e comunicações. O setor cibernético é considerado pelo governo brasileiro como de importância estratégica – ao lado dos setores nuclear e espacial.

Após o governo brasileiro estabelecer, em dezembro de 2008, o setor cibernético como de importância estratégica, o Exército Brasileiro instituiu em 2009 o Setor Cibernético no âmbito da Força Terrestre sob determinação do Ministério da Defesa. Desde então, o Projeto Estratégico de Defesa Cibernética vem se consolidando devido à necessidade da existência de uma entidade para liderar os intervenientes nessa empreitada (BRASIL, 2015b).

Na figura 1 é exposta a estrutura do Sistema Brasileiro de Defesa Cibernética, dividida em três níveis: político, estratégico e operacional. O primeiro nível é realizado pelo Gabinete de Segurança Institucional (GSI) da Presidência da República, tratando da Segurança da Informação e segurança cibernética. No nível estratégico a coordenação é do Ministério da Defesa (MD), responsável pela defesa cibernética. Já em nível operacional é encabeçado pelo Comando de Defesa Cibernética das Forças Armadas, contando com diversas ações no campo da guerra cibernética. Tais ações são realizadas pelo Exército Brasileiro (EB), Força Aérea Brasileira (FAB) e Marinha do Brasil (MB) em cinco competências: Ciência e Tecnologia (C&T), Recursos Humanos (RH), Operacional (Op), Inteligência (Intlig) e Doutrina (Dout).



Figura 1 – Estrutura do Sistema Brasileiro de Defesa Cibernética (CBSI, 2014)

Com o objetivo de desenvolver medidas de proteção e mitigar ataques no campo cibernético, segundo Brasil (2015b), o Projeto Estratégico é composto por várias ações em nível operacional e estratégico, dentre essas: desenvolvimento de equipamento de Rádio Definido por Software (RDS), de uma Rede Nacional de Segurança da Informação e Criptografia (RENASIC); a produção de doutrina específica para este tipo de atividade; a criação do Comando de Defesa Cibernética (ComDCiber).

Considerando o risco à soberania do país, o ComDCiber possui em sua estrutura dois elementos importantes: a Escola Nacional de Defesa Cibernética (ENaDCiber) e o Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética (SHCDCiber).

A primeira visa capacitar recursos humanos permitindo dominar áreas multidisciplinares e implantar pesquisa científica voltada ao tema, dialogando com entidades civis corporativas e acadêmicas (BRASIL, 2015a).

Já o SHCDCiber objetiva se “constituir em um sistema nacional de homologação e certificação de produtos e serviços de defesa cibernética, que seja economicamente sustentável junto à Base Industrial de Defesa nacional, e em conformidade a padrões nacionais de segurança de equipamentos e serviços necessários à defesa do espaço cibernético” (BRASIL, 2015a).

A Fundação Universidade de Brasília (FUB) executou recentemente o projeto “Apoio ao Programa Defesa Cibernética na Defesa Nacional: Viabilidade e Concepção da Escola Nacional de Defesa Cibernética e do Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética - ENaDCiber-SHCDCIBER@DCDN”, atestando a viabilidade de implantação da ENaDCiber e do SHCDCiber. Diversos dos aspectos metodológicos aqui referenciados são oriundos desse estudo.

2.2 PRODUTO MECATRÔNICO

Mecatrônica é definida como “uma tecnologia que combina mecânica com eletrônica e tecnologia da informação para compor tanto uma interação funcional como uma integração espacial de componentes, módulos, produtos e sistemas” (BUUR; ANDREASEN; 1990, tradução nossa).

Para Behbahani e De Silva (2012), um produto mecatrônico é um sistema com múltiplos componentes e domínios, envolvendo elementos mecânicos, eletrônicos, de controles e engenharia da computação. A figura 2 ilustra essa sinergia entre os diversos campos de conhecimento da Mecatrônica.

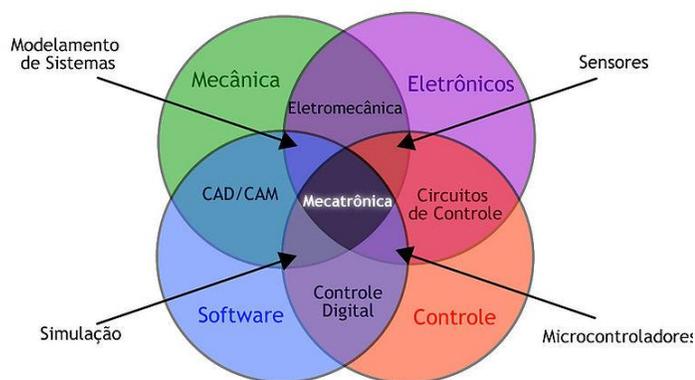


Figura 2 – Elementos da Mecatrônica (COLITEC, 2015)

Comparando-o com um produto não-mecatrônico que exige um nível similar de esforço em seu desenvolvimento, ele apresenta as seguintes características: maiores eficiência, precisão, exatidão, confiabilidade, flexibilidade, funcionalidade, segurança e “amigabilidade ao meio ambiente”; ser de baixo custo; ser menos complexo mecanicamente (DE SILVA; BEHBAHANI, 2012).

A multidisciplinaridade possibilita integrar as características de cada um de seus componentes, otimizando-o sinergicamente.

“O entendimento da mecatrônica como aplicação da eletrônica na engenharia mecânica explica um número considerável de aplicações da mecatrônica” (BARBALHO, 2016). Diversos produtos, como robôs, sistemas de manufatura automatizados, automação de produtos de consumo como automóveis e dispositivos *iOT* (*internet of things*) exemplificam tal definição.

Segundo Barbalho (2016), o esquema genérico de um produto mecatrônico pode ser exemplificado conforme a figura 3: as setas cheias representam o fluxo principal de informações, exceto as que estão identificadas com um asterisco (*), que podem representar fluxo de energia ou materiais. As setas na vertical, tracejadas, indicam eventuais fluxos de informação que fluem pelos sistemas de comunicação. Apesar do sistema mecatrônico geralmente ser comercializado como produto final, as aplicações representadas na figura três são exemplos da utilização de componentes mecatrônicos na indústria de processos (petróleo), de produtos de massa (carros) e de defesa (aviões militares).

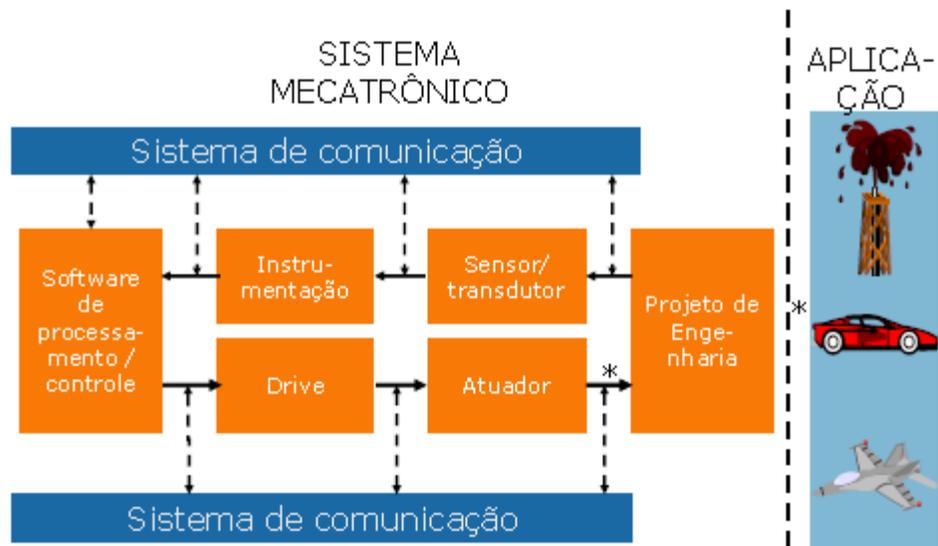


Figura 3 – Elementos de um Produto Mecatrônico (BARBALHO, 2016)

Outros produtos mecatrônicos têm origem em equipamentos eminentemente eletrônicos. Um exemplo dessas aplicações são os terminais de videoconferência.

2.3 COMUNICAÇÕES UNIFICADAS E VIDEOCONFERÊNCIA

Os equipamentos de videoconferência são considerados produtos mecatrônicos já que são formados por itens eletrônicos e mecânicos controlados por *software*.

Os terminais são compostos basicamente por: um codec (codificador/decodificador de áudio e vídeo); microfone(s); uma (ou mais) câmeras de vídeo (fixas ou com PTZ - *pan/tilt/zoom*); um monitor de vídeo (ao mínimo, ou um projetor de grandes dimensões); e uma câmara de documentos (opcional).



Figura 4 – Equipamento de videoconferência Huawei TE30 (AV-iQ, 2017)

Conforme Dias (2006), o codec pode ser entendido como um acrônimo de CODificador-DECodificador. Eles são responsáveis por codificar sequências de áudio ou vídeo para armazenamento ou transmissão, sendo que depois podem decodificá-las para exibição ou edição. São geralmente utilizados nas transmissões digitais de televisão e em videoconferências.

A solução tecnológica utiliza-se de redes convergentes. Convergência é o encaminhamento e tratamento de voz, dados e vídeo em uma infraestrutura única de rede, através de uma única modalidade de equipamento (STALLINGS, 2003).

Tecnologias que usam o protocolo IP (*Internet Protocol*) têm apresentado consolidação na área das telecomunicações e trazido facilidades para a convergência “tudo sobre IP”: vídeo, dados e voz sobre IP (CISCO, 2016).

Através da videoconferência é possível a comunicação com voz e vídeo entre pessoas dispersas geograficamente, inclusive com compartilhamento de conteúdo.

O sistema existe desde 1970, porém somente na última década se popularizou, devido aos avanços nas redes de comunicação e uso de tecnologias digitais.

As sessões de videoconferência podem ocorrer de duas formas: ponto-a-ponto ou multiponto. Na primeira forma, envolvem dois participantes remotos (chamados de sites). Já na segunda, há conexão simultânea de diversos sites através do uso de dispositivos conhecidos como *Multipoint Control Unit* (MCU). O MCU disponibiliza portas para conexões simultâneas às videoconferências, possibilitando configuração de sua velocidade. Porém, alguns equipamentos de videoconferência possuem tecnologia que já englobam o controle realizado pelo MCU (DIAS, 2006).

Os participantes podem acessar a conferência de qualquer lugar com acesso à Internet, usando seu próprio computador, com um microfone e uma webcam, ou seu dispositivo móvel *tablet* ou celular, por exemplo). Eles interagem por voz, texto (*chat*) e compartilhamento de arquivos (*slides*, planilhas).

Os sistemas de videoconferência proporcionam economia de tempo e recursos já que facilitam a comunicação em tempo real entre parceiros comerciais, clientes e fornecedores das organizações. Assim, o custo com deslocamentos e viagens é reduzido, aumentando a eficiência operacional.

Eles também são usados em ensino à distância, para o apoio ao ensino em escolas e universidades, na telemedicina e no poder judiciário, na realização de audiências.

2.4 PRINCÍPIOS DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO E COMUNICAÇÕES

Ao conjunto de artifícios de proteção contra o mau uso (acidental ou intencional) da informação por pessoas internas ou externas à instituição chamamos Segurança da Informação (SI) (STALLINGS, 2003).

Segundo Fontes (2008), proteger a informação:

- a) Não é um assunto somente de tecnologia, já que não é somente o ambiente computacional que deve ser protegido. A proteção tecnológica é fundamental, mas não é suficiente. Todo e qualquer ambiente em que informações operacionais e estratégicas são processadas e armazenadas deve ser protegido;
- b) É uma decisão empresarial, pois proteger a informação é proteger o negócio da organização.;
- c) Não acontece por milagre, exige dedicação de tempo e recursos;

- d) Deve fazer parte dos requisitos de negócio: a SI deve ser encarada como um elemento crítico que possibilita a realização do negócio;
- e) Exige postura profissional das pessoas: a SI deve ser tratada de forma profissional;
- f) É liberar a informação apenas para quem precisa;
- g) É implementar o conceito de Gestor da Informação: a TI é apenas a responsável pela custódia da informação;
- h) Deve contemplar todos os colaboradores: funcionários, prestadores de serviço, terceirizados, consultores e trabalhadores temporários devem ser igualmente comprometidos com o processo de SI;
- i) É considerar as pessoas um elemento vital: os conceitos de segurança devem ser internalizados pelos colaboradores.

Os princípios que pautam a SI são discutidos a seguir.

2.4.1 Integridade

É a garantia de que a informação permaneceu íntegra, ou seja, não foi modificada em seu armazenamento ou transmissão, sem que o autor da mensagem autorizasse.

Moraes (2010) relaciona a integridade à proteção da informação ou do processo contra alterações, intencionais ou acidentais, sem a autorização devida. É comparada ao controle de fraude.

A integridade é crítica em diversos sistemas, entre os quais constam: financeiros; de controle de tráfego aéreo; de fornecimento de energia elétrica, de água e de gás.

2.4.2 Confidencialidade

Stallings (2003) define confidencialidade como “a proteção dos dados transmitidos contra ataques passivos”.

Consiste basicamente em proteger a informação em processos e recursos, pelos quais passa durante seu ciclo de vida para que pessoas não autorizadas a acessem. Dessa forma, atua também como um mecanismo de garantia à privacidade dos dados.

Conforme Moraes (2012), a confidencialidade envolve três aspectos importantes: identificação, autorização e autenticação dos usuários e/ou sistemas.

A Recomendação X.800 ITU, conhecida como Arquitetura de Segurança OSI (*Security Architecture for Open Systems Interconnection*) (ITU, 1991) define orientações com foco em

ataques, mecanismos e serviços de segurança. A confidencialidade insere-se nos serviços de segurança, definidos como “serviços que garantam a segurança do processamento de dados dos sistemas e a transferência de informação de uma organização” (STALLINGS, 2003).

2.4.3 Disponibilidade

A norma NBR 27002:2005 (ABNT, 2005) define disponibilidade como a “propriedade de (a informação) estar acessível e utilizável sob demanda por uma entidade autorizada”.

A disponibilidade implica em garantir que o sistema sempre esteja acessível quando o usuário precisar.

A norma X.800 ITU (ITU, 1996) relaciona a disponibilidade aos ataques de segurança ativos, onde classifica-se a negação de serviço (*denial of service* – DoS). O DoS é uma das ameaças à disponibilidade, somada às perdas resultantes de desastres naturais.

2.4.4 Autenticidade

Segundo ABNT (2005), autenticidade é o princípio que garante a identificação e a segurança da origem da informação, ou seja, afiança que sua origem é autêntica e que os dados não foram alterados ao longo do processo.

2.4.5 Não-repúdio

Define-se como um serviço de segurança baseado em métodos e técnicas que evitam que o remetente de uma mensagem possa negar, no futuro, o envio dela (DSIC/GSIPR, 2015).

2.5 PADRÕES DE HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC)

Existem diversas abordagens internacionalmente aceitas para avaliação e certificação de produtos e sistemas de tecnologia da informação (TI), cada qual com seus critérios de avaliação, dentre as quais podem ser destacadas as seguintes:

a) TCSEC - *Trusted Computer System Evaluation Criteria (Orange book)*: abordagem voltada especificamente aos softwares. Possui sete níveis de notas (A1, B3, B2, B1, C2, C1 ou D). Apesar de ter sido desenvolvido há mais de 30 anos (começou a ser usado nos Estados Unidos, em 1985), ainda é utilizado.

b) ITSEC - *Information Technology Security Evaluation Criteria*: desenvolvido na Europa para avaliação de produtos e sistemas em ambientes comerciais. Possui os níveis: E0, E1, E2, E3, E4, E5 e E6. Apresenta paralelo com avaliação do TCSEC (o nível C2 no TCSEC equivale ao FC2/E2 ITSEC). Largamente aceito na Europa e no Reino Unido).

c) CC - *Common Criteria*: surgiu do esforço de padronização entre Estados Unidos, Europa e Reino Unido em alinhar TCSEC e ITSEC. Os requisitos de segurança funcional são regularmente atualizados no catálogo. É desenvolvido um *protection profile* (PP) com base nos requerimentos de segurança necessários (*security targets*) para avaliar o alvo de avaliação (*target of evaluation*) em questão. Níveis de garantia de avaliação (*Evaluation Assurance Levels*, EAL): de EAL1 (nível mais baixo) até EAL7 (o nível mais alto, equivalente ao T1 no TCSEC e ao E6 no ITSEC). Mais comumente aceito no Canadá, EUA, França, Alemanha e Reino Unido. O fato de um PP ser considerado EAL3 não quer dizer que ele é mais seguro que um perfil que foi considerado EAL 2, mas sim que os critérios utilizados na sua avaliação correspondem aos do EAL 2, ou seja, mais testes foram realizados na garantia dos requisitos de segurança.

No quadro 1 verificam-se as comparações entre os respectivos níveis do CC, TCSEC e ITSEC.

Quadro 1 – Comparação dos níveis de segurança Common Criteria, TCSEC e ITSEC

Common Criteria	TCSEC Norte-americano	ITSEC Europeu
-	D: Proteção mínima	E0
EAL1	-	-
EAL2	C1: Proteção de segurança discricionária	E1
EAL3	C2: Proteção de acesso controlado	E2
EAL4	B1: Proteção de segurança rotulada	E3
EAL5	B2: Proteção estruturada	E4
EAL6	B3: Domínios de segurança	E5
EAL7	A1: Projeto verificado	E6

A grande maioria das pesquisas acadêmicas reforça a ideia que a abordagem de avaliação e certificação deve ser holística, ou seja, aplicada à organização e seus sistemas informacionais

como um todo. Num sistema de telecomunicação, a segurança deve ter como objetivo prevenir acesso não-autorizado às áreas de segurança relacionadas às comunicações eletrônicas. A confiabilidade e a segurança do hardware e do software são importantes pontos a serem considerados.

Apesar da importância do assunto, os esforços internacionais na área são relativamente recentes. Para exemplificar essa situação: a norma ISO/IEC 27001, que prevê padrões de segurança de forma genérica a todas as organizações, é de 2005. Até 2011 mais de 17.500 certificações nesse padrão haviam sido alcançados em cerca de 100 países (DLAMINI *et al*, 2009). Embora seja um número expressivo, não é tão significativo quanto deveria ser devido à importância do tema (BRODERICK, 2006).

Somente em 2000 foi criado o Comitê Gestor da Segurança da Informação no Brasil. Esse órgão assessoria a Secretaria Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação e Comunicações voltada à administração pública federal (direta ou indireta). É subordinado diretamente à Presidência da República e auxilia o Departamento do Ministério da Defesa na elaboração e execução de diretivas no campo da defesa cibernética.

Países como China, Eslovênia, Estados Unidos, Hong Kong, Japão, Reino Unido, Taiwan e Turquia já estão preocupados com essa questão há mais tempo, inclusive já estudando e implementando, em alguns casos, políticas governamentais claras de regulação do mercado, abrangendo não somente a administração pública mas também o setor privado.

Estão em desenvolvimento alguns frameworks para gerenciamento da segurança dos sistemas de informação (TRČEK, 2003).

Há também estudos na área de ontologia, na tentativa de estabelecer um padrão para requerimentos de segurança da informação (BLANCO *et al*, 2011). Existem também grandes esforços ao redor do mundo na área de segurança cibernética em infraestruturas críticas, tais como sistemas de controle industrial (DISSO *et al*, 2015).

Encontramos, ainda, a Portaria Interministerial 141/2014 "que implementa a necessidade de certificação de todos os equipamentos e sistemas de TICs a serem vendidos para o governo e empresas públicas em relação à existência de *backdoors* e vulnerabilidades de segurança em equipamentos de rede, data center, comunicação etc. adotados pelo governo" (BRASIL, 2014). Trata-se de uma seara política e comercial: de um lado, o governo brasileiro disposto a proteger

seus dados deseja criar uma certificação própria; de outro, os fornecedores de tecnologia da informação e comunicação (TIC) querem que o governo adote o CC, considerado padrão internacional, alegando que o desenvolvimento de um padrão brasileiro próprio de certificação vai isolar o país, assim como acontece com a Índia e a China.

O presente trabalho não dialoga com essa temática diretamente, pois considera-se que o desenvolvimento de um perfil de proteção e de testes a ele relacionados contribuem com ambas as abordagens acima mencionadas já que o desenvolvimento de um sistema próprio de certificação e homologação demanda que se conheça com profundidade os sistemas já existentes.

2.5.1 Common Criteria

A Norma ISO/IEC 15408 *Common Criteria for Information Technology Security Evaluation* é também conhecida como *Common Criteria* sendo usada para avaliar segurança em produtos ou serviços de TI a partir de parâmetros comuns, definidos em determinados critérios, através do perfil de proteção (PP).

Os requisitos funcionais do Common Criteria são expressos em classes, famílias e componentes. As classes são (conforme COMMON CRITERIA, 2012a): *FAU – Security Audit; FCO – Communication; FCS – Cryptographic Support; FDP – User Data Protection; FIA – Identification and Authentication; FMT – Security Management; FPR – Privacy; FPT – Protection of the TSF; FRU – Resource Utilisation; FTA – Toe Access; FTP – Trusted Path/Channels.*

O PP relaciona os requisitos de segurança para o produto/serviço alvo da avaliação, incluindo seis aspectos (conforme COMMON CRITERIA, 2012b):

- a) *PP Introduction*: descreve o alvo da avaliação *TOE (target of evaluation)*;
- b) *Conformance Claims*: define as conformidades exigidas;
- c) *Security Problem Definition*: expõe o problema de segurança abordado;
- d) *Security Objectives*: define a resposta ao problema de segurança;
- e) *Extended Components Definition*: declara os requisitos estendidos de segurança;

f) *Security Requirements*: relaciona os requisitos de segurança funcional (SFRs) e os de garantia de segurança (SARs).

A norma permite avaliar o produto considerando as classes e as famílias acima citadas em até sete níveis (*Evaluation Assurance Levels*, EAL), que variam de EAL1 (nível inicial) até EAL7 (nível máximo) (MEAD, 2013):

a) EAL 1: Funcionalmente testado. Indica que o TOE foi funcionalmente testado, ou seja, atesta que suas funções estão consistentes com sua documentação, proporcionando um nível básico de segurança. Devem ser fornecidas neste teste, ainda, de que há proteção útil contra ameaças identificadas.

b) EAL 2: Estruturalmente testado. Fornece um nível de segurança de baixo a moderado. É utilizado quando não se tem acesso aos registros dos desenvolvedores, ou quando existem sistemas legados.

c) EAL 3: Metodicamente testado e verificado. Aplica-se quando é exigido um nível moderado de garantia de segurança, requerendo investigação profunda do TOE e seu desenvolvimento, sem a necessidade de reengenharia substancial.

d) EAL 4: Metodicamente projetado, testado e revisado. Apresenta nível de segurança de moderado a alto, geralmente incorrendo em custos adicionais de engenharia específicos de segurança.

e) EAL 5: Semi-formalmente projetado e testado. Neste nível é fornecido nível elevado de garantia de segurança, exigindo aumento significativo de segurança em relação ao EAL 4, já que são exigidas arquitetura mais estruturada e descrições do projeto semiformais. É utilizada abordagem de desenvolvimento rigorosa que não implique em custos irracionais de técnicas de engenharia de segurança especializadas.

f) EAL 6: Projeto semi-formalmente verificado e testado. As vulnerabilidades analisadas neste nível devem fornecer resistência à ataques de elevado potencial. Aplica-se quando são desenvolvidos TOEs para aplicação em situações de alto risco, em que o valor dos ativos protegidos justifica os custos adicionais.

g) EAL 7: Projeto oficialmente verificado e testado. É utilizado com o desenvolvimento TOE para aplicações em situações de risco extremo, bem como quando o alto valor dos ativos justifica os custos mais elevados.

O que diferencia cada um desses níveis corresponde a um pacote de requisitos de garantia de segurança, relacionando-se à extensão e profundidade dos testes realizados no TOE, que expressam sua garantia de atendimento aos requisitos de segurança. Ou seja, uma avaliação nível EAL1 requer um conjunto pequeno de atividades de garantia, fornecendo um nível de confiança na proteção do produto relativamente baixo, enquanto uma avaliação nível EAL7 exige um grande conjunto de atividades que proporcionam um nível de confiança muito alto (LISI, 2013).

2.5.2 Metodologias de avaliação de segurança de sistemas de informação

Vários são os trabalhos acadêmicos pesquisados cujo objeto era o estudo de metodologias de avaliação dos sistemas de informação, particularmente com relação à segurança.

Silva (2014) propôs um sistema de avaliação da segurança em sistemas de informação equivalentes (serviços de e-mail *cloud* e *in house*) usando metodologia multicritério de apoio à decisão MACBETH (*Measuring Attractiveness by a Categorical Based Evolution Technique*). O método utilizado descartou a utilização das boas práticas e normas como COBIT, ISO e similares pelo fato do autor considerar grande o esforço necessário em termos de tempo e dinheiro para aplicar essas normas de controle, além de achá-los bastante genéricos, não atendendo às especificidades da organização estudada. Os critérios de avaliação propostos por (SILVA, 2014) foram levantados a partir da revisão da literatura científica e das boas práticas existentes, e validados através de entrevistas aos responsáveis pela segurança nas organizações portuguesas (clientes, fornecedores e especialistas em segurança). O objeto de avaliação foi o serviço de e-mail, sendo que o Microsoft Office 365 apresentou-se como o serviço de e-mail na *cloud*.

O método de investigação utilizado foi o *Design Science Research Methodology* (DSRM), que é um processo iterativo formado por seis estágios, detalhados na figura abaixo. O autor utilizou duas iterações: a primeira para definir os critérios de avaliação de segurança, e a segunda para demonstrar o método na organização.

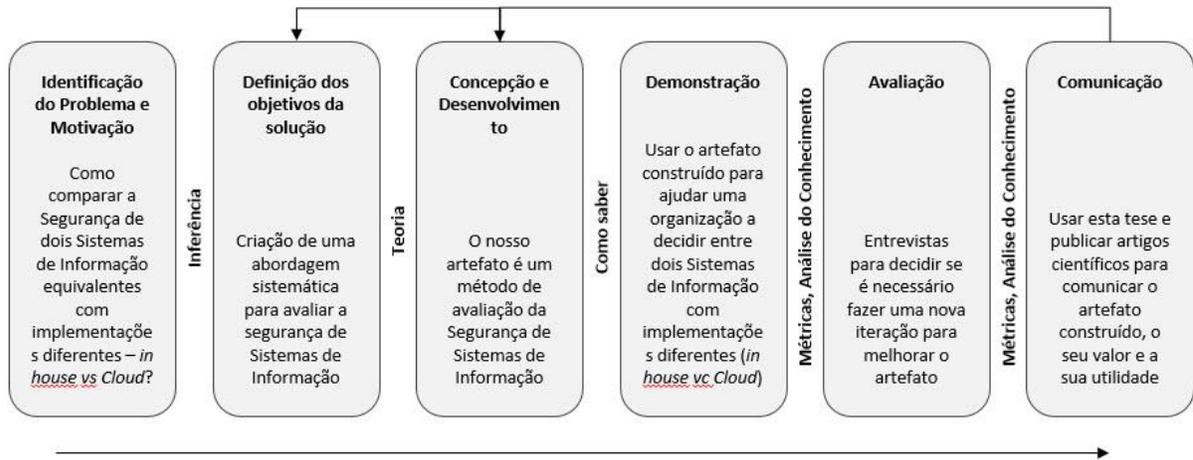


Figura 5 - O processo DSRM (SILVA, 2014)

Já Ohtoshi (2008) fez uma análise comparativa entre várias normas internacionais e boas práticas em segurança de sistemas de informação descrevendo as principais ferramentas e metodologias de análise e de gestão de riscos existentes. O autor concluiu demonstrando a tendência de convergência e de integração entre as metodologias.

Martins e Santos (2005) também utilizaram as principais normas e padrões de segurança para criarem um conjunto de diretrizes. A partir daí apresentaram uma proposta de metodologia para implantar um sistema de gestão de segurança da informação (SGSI) com o objetivo de garantir a segurança de um ambiente computacional disposto em rede. A metodologia utilizada foi um estudo de caso em uma empresa de proteção ambiental, predominantemente de capital privado. Como resultado foi implantado o SGSI na empresa, considerando as particularidades de seu negócio-fim.

D'ornellas e Kroll (2009) analisaram o processo de avaliação de riscos com foco no gerenciamento estratégico da segurança da informação de forma geral. Verificaram que há diferentes metodologias para avaliar os riscos, destacando dentre essas *TAG's Risk Assesment Process*, *OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation* e a norma *AS/NZS 4360:2004*. Como resultado dessa avaliação é implementada/otimizada a gestão da segurança da informação na corporação considerada.

Fontoura, Konzen e Nunes (2012) utilizaram a norma ISO/IEC 27005 como base para associar padrões de segurança, com o objetivo de facilitar a confecção do processo da norma e proporcionar maior garantia do uso de práticas de mercado recomendadas, enquanto que Santos e Filho (2013) usaram as normas ABNT NBR ISO/IEC 27001:2006 e 27002:2005, além da

27005:2008 para verificar a aderência de um sistema de gestão de segurança da informação (SGSI), conforme critérios definidos nestes normativos.

Amaral *et al* (2008) propuseram uma metodologia de avaliação de riscos baseada em Seis Sigma, consolidando uma política de segurança da informação ainda em validação em uma instituição hospitalar.

Eloff e Solms (2008) propuseram uma combinação de certificação e avaliação de sistemas computacionais, considerando aspectos de segurança com base na norma BS7799, enquanto que Trček (2003) apresentou uma proposta de framework multidisciplinar para o gerenciamento da segurança em sistemas informacionais, integrando interações humanas, homem-máquina, segurança física, aspectos organizacionais, legislação, entre outros.

Assim como Trček (2003), Akalp *et al* (2011) também se utilizaram de estudos estatísticos para avaliar as ameaças e riscos de segurança dos sistemas de gestão de SI. Enquanto o primeiro trabalho apenas apresenta o framework, sem validá-lo, o segundo utiliza como metodologia um estudo de caso em pequenas e médias empresas turcas.

Farn *et al* (2003) também usou a metodologia de estudo de caso usada por Akalp *et al* (2011), sugerindo uma certificação com cinco níveis do “Sistema de proteção de segurança da comunicação e da informação”, alinhada às políticas existentes de um escritório de normatização governamental em Taiwan, objeto de seu estudo.

A análise comparativa de alguns padrões de segurança de gerenciamento de sistemas de informação foi o estudo de Sipponen e Willison (2009), adotando como validação as boas práticas do mercado, enquanto que Tashi e Outi-Hélie (2008) buscaram analisar as métricas de avaliação de segurança adequadas conforme as normas ISO 17799:2005 e ISO 27001.

Os trabalhos de Broderick (2006), Kadobayashi e Takahashi (2015) apresentam em comum a utilização de normas internacionais de segurança e boas práticas de mercado. O primeiro autor utilizou-se do alinhamento a processos específicos do *Control Objectives for Information and related Technology*– COBIT para analisar os padrões e regulações de segurança em SGSI, enquanto que o segundo trabalho propõe uma ontologia de referência voltada às informações de *cybersegurança* operacionais. Disso *et al* (2015) também estudaram o campo da *cybersegurança*, mais especificamente a análise de gerenciamento de *cybersegurança* em sistemas de controle industriais. Porém utilizaram-se de normas e *frameworks* europeus e norte-americanos de segurança em controle de sistemas industriais, ao contrário de Kadobayashi e

Takahashi (2015) que usaram orientações dos centros de operação de segurança norte-americanos, japoneses e sul-coreanos.

Dlamini *et al* (2009) realiza uma revisão de literatura sobre segurança da informação, pesquisando as principais ameaças, os assuntos abordados e as tendências de pesquisa.

No campo da avaliação e certificação de equipamentos de TI, o trabalho mais próximo da pesquisa realizada pela autora foi a proposta de metodologia para certificação de computador desktop apresentada por Coelho e Silva (2013), usando ontologia própria e conforme normas internacionais e boas práticas de mercado. Para validação foi utilizado um laboratório com o item de avaliação, simulando-se condições reais de ameaças de segurança.

As pesquisas de Hou e Yu (2012) e Fernandez-Saavedra *et al* (2013) também se aproximam ao trabalho aqui realizado já que se utilizaram do *Common Criteria* como metodologia para avaliação de segurança em sistemas de informação. Hou e You (2012) avaliaram o uso da tecnologia RFID (*Radio Frequency Identification*) em ambiente médico-hospitalar, enquanto que Fernandez-Saavedra *et al* (2013) avaliam um sistema biométrico, ambos se utilizando de revisão de literatura e boas práticas de mercado no levantamento dos critérios de avaliação.

Abaixo segue quadro-resumo dos trabalhos acadêmicos pesquisados, relacionando as metodologias propostas para avaliar a segurança em sistemas de informação.

Quadro 2 – Resumo de metodologias de avaliação de segurança

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Martins e Santos (2005)	Metodologia teórico-conceitual, analisando as principais normas e padrões de segurança (TECSEC, ISO 15408:1999, ISO/IEC TR 13335:1998, BS7799-2:2001, ISO/IEC 17799:2001, IEC 61508:1998). A partir dessa análise, é proposta a implantação de um sistema de gestão de SI.	Sistema de gestão de SI (SGSI)	Análise da literatura e boas práticas de mercado.	Conformidade com as normas consideradas	Acompanhamento da implantação do SGSI, através de indicadores.
Silva (2014)	Metodologia multicritério de apoio à decisão (MMAD)	Serviço de e-mail: <i>cloud e in house</i>	Processo iterativo de seis estágios (<i>Design Science Research Methodology - DSRM</i>), literatura e boas práticas relacionadas com a segurança de SI. Critérios elencados são avaliados junto aos especialistas de segurança	Metodologia de apoio à decisão MACBETH (<i>Measuring Attractiveness by a Categorical Based Evolution Technique</i>): critérios são avaliados e ranqueados	Entrevistas e questionários comentários da comunidade científica; <i>Moody and Shanks Quality Framework</i> ; os Princípios de Österle

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Ohtoshi (2008)	Abordagem teórico- metodológica	Segurança de SI (em geral): organização e sistematização do conhecimento sobre a análise e a gestão de riscos aplicáveis à gestão da segurança da informação e comunicações.	Análise comparativa de normas e boas práticas	Normas e boas práticas: AS/NZS 4360; ISO/IEC 13335, atual ISO/IEC 27005; NBR ISO/IEC 17799 (BS7799-1); NBR ISO/IEC 27002 (NBR ISO/IEC 17799); <i>Austrian IT Security Handbook</i> ; <i>Coras</i> ; <i>Cramm</i> ; <i>Dutch</i> ; <i>Ebios</i> ; <i>Isam</i> .	Tabulação das informações em quadros comparativos com as principais Metodologias.
D'ornellas e Kroll (2009)	Avaliação de riscos, que pode ser realizada por diversas metodologias	Segurança da informação	Avaliação por etapas: identificação dos ativos; Mensuração da segurança; Avaliação de ameaças e vulnerabilidades; avaliação de riscos.	Metodologias (<i>TAG's Risk Assessment Process</i> ; <i>OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation</i> ; AS/NZS 4360:2004; entre outras)	Análise do custo- benefício; emissão de relatórios e recomendações; tomadas de decisão aliadas à estratégia da empresa

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Fontoura, Konzen e Nunes (2012)	Associação de padrões de segurança a ISO/IEC 27005	Segurança da informação	Uso das boas práticas de mercado e as especificidades do negócio das organizações	ISO/IEC 27005	Ilustração da utilização dos padrões de segurança em um sistema de gestão acadêmica de uma instituição de ensino privada
Amaral <i>et al</i> (2008)	Avaliação de riscos com a utilização de Seis Sigma	Segurança da informação	Elaboração de questionários, uso das boas práticas de mercado e das especificidades do negócio das organizações.	Ciclo de melhoria DMAIC (Definir, Medir, Analisar, Implementar e Controlar), FMEA (<i>Failure Mode and Effect Analyses</i>)	O trabalho atestava a eficiência da metodologia na condução do processo de implantação da segurança da Informação em uma instituição hospitalar

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Santos e Filho (2013)	Verificação do nível de aderência da gestão da segurança da informação de uma organização	Segurança da informação	Uso das boas práticas de mercado; análise de documentos e arquivos da organização; entrevistas com funcionários; observação direta dos sistemas de informação.	Normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008	Computação valorada dos critérios analisados conforme as atividades constantes dos processos de SGSI estabelecidos nas normas
Eloff e Solms (2008)	Combinação de processo de certificação e avaliação de sistemas computacionais	Produtos ou sistemas de segurança da informação (SI)	Uso das boas práticas de mercado	Norma BS7799	Estudo de caso hipotético na companhia X, verificando seus produtos/sistemas de SI

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Trček (2003)	Proposta de framework multidisciplinar para gestão de segurança	Sistema de informação	Uso das melhores práticas, normas e padrões internacionais e regulações europeias e norte-americanas.	Avaliação de ameaças e riscos com apoio de cálculos estatísticos	O framework é apresentado, porém o autor não valida o modelo proposto, apenas compara-o com os padrões internacionais
Farn <i>et al</i> (2003)	Estudo da certificação de sistemas de gerenciamento de segurança da informação	Sistemas de gerenciamento de SI	Uso das melhores práticas, normas e padrões internacionais e regulação chinesa	Especificações do <i>Bureau of Standards, Metrology, and Inspection</i> (BSMI), órgão governamental da República da China (Taiwan) responsável pela padronização, metrologia e inspeção de produtos	O framework é apresentado, porém o autor não valida o modelo proposto, apenas compara-o com os padrões internacionais e a regulação chinesa

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Sipponen e Willison (2009)	Comparação entre padrões de segurança de gerenciamento de sistema de informação	Sistemas de informação em geral	Análise das normas e boas práticas de mercado.	Padrões BS7799, BS ISO/IEC17799: 2000, GASPP/GAISP, e SSE-CMM	Resultados validados através das práticas comuns de mercado e autoridades de segurança
Tashi e Outi-Hélie (2008)	Avaliação de métricas de segurança para a avaliação de gestão de segurança da informação	Sistemas de informação em geral	Análise das normas e boas práticas de mercado.	Normas ISO 17799:2005 e ISO 27001	São expostas as principais métricas para avaliar a segurança, conforme as normas utilizadas

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Coelho e Silva (2013)	Proposta de metodologia para certificação de equipamento de tecnologia da informação (TI)	Equipamento de TI	Ontologia e metodologia próprias são criadas, conforme normas internacionais e boas práticas de mercado	Laboratório, simulando condição real de ameaças de segurança	Exemplo de certificação de um computador <i>desktop</i>
Broderick (2006)	Análise de padrões e regulações de segurança em sistemas de gerenciamento de SI	Sistemas de informação em geral	Critérios elencados conforme normas internacionais e melhores práticas, alinhados a processos específicos do COBIT	ISO-27001:2005; ISO/IEC-17799:2005; BS-7799-2:2002; ISO/IEC-17799:2000	A viabilidade do <i>framework</i> proposto é avaliada teoricamente

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Akalp <i>et al</i> (2011)	Estudo de caso: análise comparativa dos sistemas de gestão de SI de pequenas e médias empresas turcas em relação às empresas de outros países	Sistemas de informação em geral	Elaboração de questionários incluindo os aspectos: política de segurança; segurança organizacional; classificação e controle de ativos; segurança pessoal; segurança física e do ambiente; gerenciamento de operações e comunicações; controle de acesso; manutenção e desenvolvimento de sistema; gestão de continuidade de negócios.	Cálculo estatístico dos critérios	Resultados analisados estatisticamente (frequência de distribuição, análise de confiabilidade, análise de correlação)
Dlamini <i>et al</i> (2009)	Análise da evolução da segurança da informação/ estado da arte dos estudos em segurança da informação	Segurança da informação	Revisão de literatura	Análise qualitativa e quantitativa dos artigos pesquisados (principais ameaças, assuntos abordados, tendências de pesquisa)	Comparação do resultado do <i>survey</i> dos artigos com publicações e estudos do CSI/FBI e Instituto SAN

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Kadobayashi e Takahashi (2015)	Proposta de ontologia de referência voltada às informações de cybersegurança operacionais	Cybersegurança corporativa	Especificações industriais, orientações dos centros de operação de segurança norte- americanos, japoneses e sul-coreanos	Análise de literatura, boas práticas, e normas internacionais	Demonstração de aplicabilidade da ontologia proposta
Hou e Yu (2012)	Proposta de framework para avaliação da segurança de RFID (<i>Radio Frequency Identification</i>) utilizado em ambiente médico- hospitalar	Uso de RFID em ambiente de cuidados com a saúde	Revisão de literatura e boas práticas, chegando aos seguintes critérios: violação de privacidade; clonagem de <i>tag</i> ; vazamento/vulnerabil idade de senha de acesso	Metodologia de avaliação de segurança utilizando o padrão <i>Common Criteria</i> (ISO/IEC 15408) e normas ISO/IEC relacionados à tecnologia RFID	Análise da viabilidade técnica da utilização do <i>framework</i> proposto

Resumo de metodologias para avaliação da segurança de Sistemas de Informação (SI)					
Autores	Tipo de abordagem	Risco considerado/ objeto de avaliação	Método de levantamento dos critérios avaliados	Ferramenta de avaliação dos riscos/ameaças	Avaliação dos resultados
Disso <i>et al</i> (2015)	Análise de gerenciamento de cybersegurança em sistemas de controle industriais	Normas de segurança e cybersegurança em sistemas de controle industriais	Critérios: tipo de publicação; escopo; métricas qualitativas e quantitativas de disponibilidade; relação com segurança	Normas e frameworks europeus e norte-americanos de segurança em controle de sistemas industriais	Análise qualitativa e quantitativa das normas, comparando-as
Fernandez-Saavedra <i>et al</i> (2013)	Análise de performance de sistema biométrico usando o <i>Common Criteria</i>	Sistema biométrico	Revisão de literatura, normas de segurança e boas práticas	<i>Common Criteria</i> e ISO/IEC 19795	Verificação de viabilidade técnica da análise proposta

Percebeu-se na literatura acadêmica pesquisada a grande tendência de utilização de normas consolidadas internacionalmente para avaliação da segurança em sistemas de informação, tais como ISO/IEC 27000, 27001 e 27005. A metodologia predominante foi o estudo de caso com a análise da aderência dos sistemas considerados às normas em questão.

Utilizaram-se dessa metodologia os trabalhos de Martins e Santos (2005), Ohtoshi (2008), D'ornellas e Kroll (2009), Santos e Filho (2013), Trček (2003), Tashi e Outi-Hélie (2007), Broderick (2006), Dlamini et al (2009), Kadobayashi e Takahashi (2015), Hou e Yu (2012), Disso et al (2015), Fernandez-Saavedra et al (2013). Os demais, além de análises de aderência, apresentaram resultados de testes, validando as análises propostas em estudos de caso e validações práticas de mercado.

3 MATERIAIS E MÉTODOS

Pode-se definir a metodologia científica como “um conjunto de abordagens, técnicas e processos utilizados pela ciência para formular e resolver problemas de aquisição objetiva do conhecimento, de uma maneira sistemática” (GIL, 1999).

Segundo Yin (2001), as pesquisas científicas podem ser conduzidas de diversas formas. Pesquisas históricas, experimentos, levantamentos e análises de informações são alguns exemplos.

Cada pesquisa apresenta características próprias. Seus benefícios estão intimamente relacionados a três aspectos principais: o tipo de questão a ser respondida na pesquisa; o controle do pesquisador sobre as ocorrências comportamentais efetivas; e o foco nos fenômenos históricos, em contraposição aos fenômenos atuais (YIN, 2001).

A pesquisa quantitativa bibliográfica foi inicialmente realizada com enfoque em segurança cibernética de elementos de comunicação de rede e segurança da informação.

A metodologia empregada neste trabalho está apresentada na figura 6.

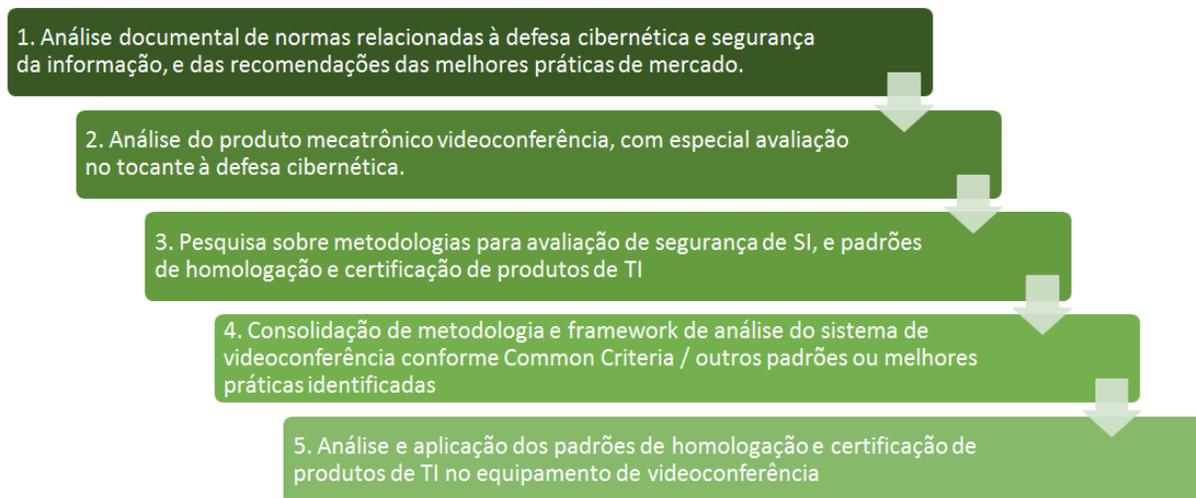


Figura 6 – Metodologia da Pesquisa

3.1 ETAPAS DE EXECUÇÃO DO TRABALHO

A pesquisa está estruturada nas seguintes etapas:

- a) Etapa 1 – estudo teórico sobre defesa cibernética e segurança da informação;

- b) Etapa 2 – estudo do produto mecatrônico videoconferência, especialmente no tocante à defesa cibernética;
- c) Etapa 3 – estudo de padrões de homologação e certificação de produtos de Tecnologia da Informação e Comunicações (TIC), incluindo o *Common Criteria*;
- d) Etapa 4 – consolidação de metodologia e framework de análise do sistema de videoconferência conforme *Common Criteria* / outros padrões ou melhores práticas identificadas;
- e) Etapa 5 – análise e aplicação dos padrões de homologação e certificação de produtos de TI no equipamento de videoconferência;
- f) Etapa 6 – consolidação dos resultados obtidos na dissertação.

Após realizada a pesquisa sobre os padrões de homologação e certificação de produtos de Tecnologia da Informação e Comunicações (TIC), definiu-se pela utilização do *Common Criteria* (norma ISO/IEC 15408:1999) para avaliar a segurança do terminal de videoconferência pelos motivos abaixo (COMMON CRITERIA, 2012c):

- a) É um *framework* flexível de avaliação de requisitos de segurança genérico, possibilitando sua utilização em diversos produtos de TI;
- b) O *CC* permite comparar resultados de avaliações de segurança independentes, já que dispõe de uma série de requisitos comuns para a funcionalidade de segurança de produtos de TI e para a garantia de medidas aplicadas a esses produtos durante a avaliação de segurança. Tais produtos podem ser implementados em *hardware*, *software* ou *firmware*;
- c) O processo de avaliação determina um nível de confiança para a funcionalidade segurança, além da garantia das medidas aplicadas aos produtos de TI que atendem a esses requisitos. Dessa forma, os resultados da avaliação podem auxiliar os consumidores a determinar se os produtos de TI preenchem suas necessidades de segurança;
- d) É útil como um manual de orientação para o desenvolvimento, a avaliação e/u aquisição de produtos de TI que dispõe de funcionalidades de segurança;
- e) Além da proteção dos ativos com relação à confidencialidade (divulgação não-autorizada), integridade (modificação) e disponibilidade (perda de uso), o *CC* pode ser

aplicado a outros aspectos de segurança. Por exemplo, riscos de atividades humanas (intencionais ou não-intencionais) ou não-humanas.

O estudo buscará identificar com o respaldo do *Common Criteria* (CC) quais os riscos de segurança da informação estão presentes nos equipamentos de videoconferência e quais devem ser os parâmetros mínimos a serem exigidos nesses sistemas, quando de sua fabricação, aquisição e utilização.

A partir desse levantamento inicial, e com o apoio das normas internacionais de segurança da informação, serão verificados os requisitos funcionais de garantia e de segurança, conforme especificados no CC, proporcionando o desenvolvimento de um *Protection Profile* (PP) para um equipamento de videoconferência genérico. Para realizar essa verificação será detectada a existência ou não dos parâmetros dos requisitos funcionais levantados em um produto real, utilizado por uma grande organização brasileira da área financeira, em ambiente controlado.

3.2 FERRAMENTAS UTILIZADAS

Para a realização dos testes desses requisitos, as ferramentas utilizadas foram:

- Equipamento de videoconferência modelo TE 30, do fabricante Huawei, na versão de firmware TEX0 V500R002C00SPCb00 Release 2.0.b00 Mar 6 2017;

- Aplicativo Cisco Jabber UC versão 11.11: aplicativo utilizado como comunicador pessoal instalado em computador desktop com sistema operacional Windows 7 Professional 64 bits, processador i5 3,00 GHz e memória RAM de 4,00 Gb;

- Rede LAN, fornecendo acesso à Internet para o computador desktop e o TOE.

3.3 PLANEJAMENTO DE EXPERIMENTOS CIENTÍFICOS

Segundo Neto, Scarminio e Bruns (2010), através dos planejamentos experimentais baseados em princípios estatísticos os pesquisadores podem obter do sistema em estudo o máximo de informação útil, realizando um número mínimo de experimentos. O planejamento dos experimentos permite que os pesquisadores consigam atingir seus resultados a custo e tempo menores.

É essencial planejar um experimento considerando que ele deve gerar o resultado procurado (NETO; SCARMINIO; BRUNS, 2010). Experimentos bem planejados facilitam a extração de informações válidas.

Conforme Reis (2017), variáveis são características que permitem medição, controle ou manipulação em uma pesquisa.

“Duas ou mais variáveis quaisquer estão relacionadas se em uma amostra de observações os valores dessas variáveis são distribuídos de forma consistente” (REIS, 2017). Considera-se que encontrar relações entre variáveis é o objetivo principal da análise científica.

Será realizada pesquisa correlacional, ou seja, apenas serão medidas e serão procuradas relações entre as variáveis.

A fim de obter significância estatística, ou seja, estimar o grau em que o resultado da análise é verdadeiro, dois aspectos devem ser considerados: a magnitude e a confiabilidade da relação entre as variáveis (REIS, 2017). A primeira diz respeito ao tamanho da relação, à grandeza. Já o segundo refere-se a quão representativo é o resultado encontrado em uma amostra específica da população considerada na pesquisa.

Conforme Viali (2008), a inferência estatística é um dos principais assuntos da Estatística moderna, dividindo-se em dois temas: os testes de hipóteses e a estimação de parâmetros.

As primeiras técnicas de inferência que surgiram realizavam hipóteses sobre a população de onde os dados eram extraídos, sendo que os parâmetros são valores relacionados com a população. Essas técnicas são chamadas de paramétricas.

Os testes considerados não-paramétricos não estão sujeitos aos parâmetros populacionais como média e variância (BEIGUELMAN, 1996).

Dentre as vantagens trazidas pelo uso desse tipo de teste, destacam-se as seguintes (VIALI, 2008): não dependem da população de onde a amostra foi retirada; demandam menos exigências que os testes paramétricos (dispensam a suas probabilidades das afirmativas não exatas, exceto em aproximações usadas em grandes amostras); são mais eficientes que os paramétricos, quando a população não apresenta distribuição de dados normal (quando a

população tem distribuição normal, sua eficiência é sutilmente menor); possibilitam atuar com dados de diversas populações; são úteis nas situações em que determinar uma escala de valores quantitativos não é trivial, pois permite que os dados sejam dispostos em uma ordem de classificação.

Segundo Viali (2008), há diversos testes paramétricos e não-paramétricos. Para se escolher o modelo mais adequado a determinada situação devem ser levados em conta: a forma como a amostra foi obtida, a natureza da população de onde se extraiu a amostra e o tipo de escala usado nos valores numéricos, além do tamanho da amostra.

No quadro 3 verifica-se um resumo dos principais testes estatísticos não-paramétricos, classificados conforme o tipo de amostra usado (uma, duas, k amostras) e o nível de mensuração (nominal, ordinal, intervalar).

A partir das observações dos eventos será realizado o teste Quiquadrado (χ^2) de hipóteses para verificar se há relação entre os mesmos. Este teste foi escolhido pelo fato de envolver variáveis nominais com 5 amostras independentes.

Quadro 3 – Resumo dos testes não-paramétricos (VIALI, 2008)

Nível de mensuração	TESTES ESTATÍSTICOS NÃO-PARAMÉTRICOS					Medidas de correlação não-paramétricas
	Caso de uma amostra	Caso de duas Amostras		Caso de k amostras		
		Amostras relacionadas	Amostras independentes	Amostras relacionadas	Amostras independentes	
Nominal	Binomial e χ^2	McNemar	Fisher e χ^2	Q de Cochram	χ^2	De contingência
Ordinal	Kolmogorov-Smirnov Iterações	Sinais Wilcoxon	Mediana U de Mann-Whitney Kolmogorov-Smirnov Iterações de Wald-Wolfowitz Moses	Friedman	Extensão da mediana Kruskal-Wallis	Por postos de Spearman Por postos de Kendall Parcial de postos de Kendall Concordância de Kendall
Intervalar		Walsh Aleatoriedade	Aleatoriedade			

Segundo Conti (2011), o teste Quiquadrado pode ser usado para encontrar um valor de dispersão para duas variáveis nominais e verificar a relação que existe entre as variáveis qualitativas. A partir dele é possível verificar se a frequência se desvia significativamente da frequência esperada.

Basicamente ele proporciona comparações entre proporções, ou seja, as eventuais divergências entre frequências observadas e esperadas para um determinado evento. Ele é usado para comparar se são diferenças significativas ou não, com relação às proporções dos

acontecimentos. Diz-se que os grupos se apresentam de forma similar se as frequências observadas e as esperadas tiverem diferenças pequenas, ou quase nulas.

Os eventos observados nesse trabalho satisfazem aos seguintes requisitos para a realização do teste Quiquadrado: os eventos são independentes, apresentando itens selecionados aleatoriamente; as observações são frequências ou contagens, e pertencem a somente uma categoria de evento; a amostra das observações é relativamente grande, com poucos grupos e no mínimo 5 observações em cada evento (CONTI, 2011).

As fórmulas utilizadas no cálculo dos testes, propostas por Karl Pearson, são:

$$x^2 = \sum [(o - e)^2 / e]$$

Onde:

o = frequência observada para cada classe

e = frequência esperada para aquela classe

Como $(o - e) = \text{desvio } (d)$, a fórmula também pode ser escrita como $x^2 = \sum (d^2 / e)$. É importante notar que o desvio é a diferença entre as frequências observada e a esperada numa classe. Quando essas frequências são muito próximas, o valor de x^2 é pequeno. Da mesma forma, quando a diferença é grande, conseqüentemente o desvio d também o é, fazendo x^2 assumir valores altos.

As seguintes hipóteses são trabalhadas (CONTI, 2011):

Hipótese nula (H_0): as frequências observadas não são diferentes das esperadas, ou seja, não há diferença entre as frequências (contagens) dos grupos. Portanto, não há relação entre os grupos estudados.

Hipótese alternativa: As frequências observadas são diferentes das esperadas, portanto existe diferença entre as frequências. Ou seja, há associação entre os grupos.

Utilizam-se duas estatísticas: x^2 calculado e x^2 tabelado (a tabela x^2 encontra-se no anexo B).

CONTI (2011) afirma que as frequências esperadas são calculadas a partir das observadas diretamente das amostras, ou seja, o χ^2 calculado vem dos experimentos, considerando os dados observados e esperados. O χ^2 tabelado é obtido da tabela χ^2 , e relaciona-se com o número de significância adotado e com os graus de liberdade.

As hipóteses são decididas ao comparar os valores de χ^2 calculado e χ^2 tabelado:

- a) Se χ^2 calculado $\geq \chi_c^2$ tabelado: *Rejeita-se* H_0 ;
- b) Se χ^2 calculado $< \chi_c^2$ tabelado: *Aceita-se* H_0 .

Quando não é possível calcular a frequência esperada é construída uma tabela de contingência. Neste caso, a frequência esperada (E) em cada classe e o número de graus de liberdade (G.L.) são calculados da seguinte forma:

$$E = \text{total marginal da linha} \times \text{total marginal da coluna} / \text{total} (N)$$

$$G.L. = (\text{número de linhas} - 1) \times (\text{número de colunas} - 1)$$

Caso o valor de χ^2 calculado $> \chi_c^2$ tabelado, ou o valor de amostras seja menor que 40, ou ainda haja ao mínimo uma classe com frequência esperada menor que 5, deve-se utilizar a correção de Yates nos cálculos (segue no anexo C explicação complementar da Correção de Yates).

4 DESENVOLVIMENTO DO PROTECTION PROFILE

Dois tipos de documentos são necessários para a avaliação dos requisitos de segurança no CC: o *PP* e o *Security Target (ST)*. Segundo Wheeler (2015), o primeiro é criado por um grupo de usuários (por exemplo, um grupo de consumidores ou uma grande organização) que identifica as propriedades de segurança desejadas no produto. Já o *ST* identifica o que o produto, ou seus componentes, realmente faz relacionado a itens relevantes de segurança. Geralmente um *ST* contém requisitos de um ou mais *PPs*.

Nessa tarefa um equipamento genérico de videoconferência foi considerado o *Target Of Evaluation (TOE)*, sendo que um dos objetivos específicos da pesquisa é o desenvolvimento de um *PP* para a avaliação do *TOE*.

Com o apoio do CC, as seguintes tarefas foram desenvolvidas para alcançar o objetivo da pesquisa: definição do *TOE*; identificação das vulnerabilidades de segurança onde o *TOE* está inserido; identificação e definição dos requisitos de segurança de TI, conforme as necessidades dos usuários, ou seja, criação de um *PP*; especificação dos requisitos de segurança que o *TOE* deve oferecer.

As seções estão divididas da seguinte forma: na 1ª seção expõe-se material introdutório para o *PP*, conforme definições presentes no *Common Criteria*; a 2ª seção trará a proposta geral do *PP* e a descrição do *TOE*; a 3ª seção discute o ambiente esperado para o *TOE*, define as ameaças relacionadas pelas medidas técnicas implementadas no hardware ou software do *TOE* ou através dos controles do ambiente, baseadas na experiência de uso de equipamentos de videoconferência e nas necessidades dos usuários; a seção 4 define os objetivos de segurança para o *TOE* e seu ambiente de operação; a seção 5 contém os requisitos de garantia e funcionais originados do *Common Criteria* que devem ser atingidos pelo *TOE*. A 6ª seção fornece explicações para demonstrar claramente que a segurança da tecnologia da informação atende às premissas, políticas e ameaças. É explicado então como o conjunto de requisitos está completamente relacionado aos objetivos, e que cada objetivo de segurança se refere a um ou mais requisitos.

4.1 DEFINIÇÃO DO TOE

Considerando que o CC é flexível quanto ao que avaliar, o framework não limita os produtos de TI que pode tratar. Assim, o termo *Target of Evaluation* é utilizado para definir o objeto de avaliação de segurança, e pode ser um componente de software, firmware e/ou hardware acompanhado de orientações.

Segundo o *Common Criteria* (2012c), pode-se entender o TOE como um produto, uma parte, um conjunto, uma única tecnologia de TI que nunca foi materializada em um produto, ou uma combinação desses. Deve-se ter em mente que “the evaluation of a TOE containing only part of an IT product should not be misrepresented as the evaluation of the entire IT product” (COMMON CRITERIA, 2006). Na pesquisa atual, o equipamento de videoconferência é o objeto de avaliação considerado, ou seja, o TOE.

Após a revisão bibliográfica dos conceitos fundamentais da pesquisa foram realizadas inicialmente as análises estrutural e funcional do equipamento de videoconferência.

Estruturalmente, o equipamento de videoconferência divide-se em: componentes ópticos, elétricos, eletroeletrônicos e de controle, conforme o esquema da figura 7.

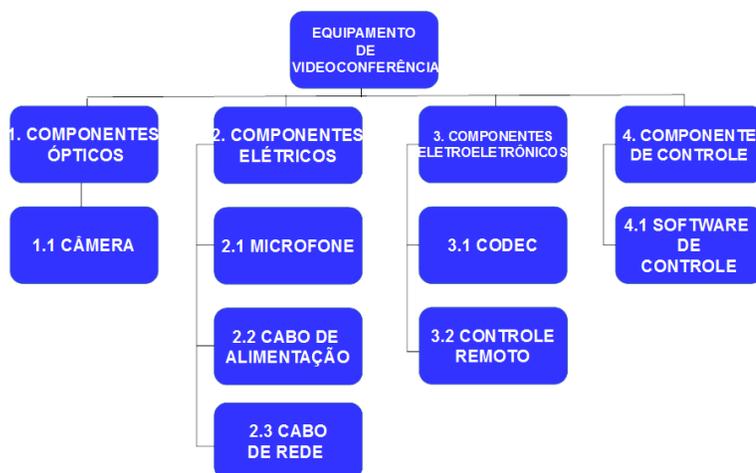


Figura 7 – Estrutura do Produto Mecatrônico Equipamento de Videoconferência

Como componente óptico tem-se a câmera de vídeo. Em componentes elétricos agrupam-se: microfone, cabos de alimentação e de rede. O controle remoto e o decodificador de vídeo são considerados componentes eletroeletrônicos, enquanto que o software de controle é o componente de controle do produto mecatrônico.

Conforme mostrado na figura 8, o produto mecatrônico apresenta dois sistemas principais: o sistema de alimentação e o sistema de controle.

O fluxo de energia entre esses sistemas e os componentes do equipamento estão representados pela linha tracejada. Dessa forma, estão diretamente associados ao sistema de controle o codec (codificador/decodificador) e o controle remoto. Ao sistema de alimentação relacionam-se diretamente: os cabos de alimentação e de rede, o microfone, a câmera e o monitor.

As setas de linha contínua representam o funcionamento essencial do sistema mecatrônico: os cabos de alimentação e de rede ligam-se diretamente ao microfone e câmera; o controle remoto direciona o software de controle do equipamento, que por sua vez controla o microfone, a câmera e o codec. Este último recebe instruções do software de controle, processando sinais de áudio e vídeo recebidos do microfone e da câmera e liberando-os ao monitor. Este último recebe instruções do software de controle, processando sinais de áudio e vídeo recebidos do microfone e da câmera e liberando-os ao monitor.

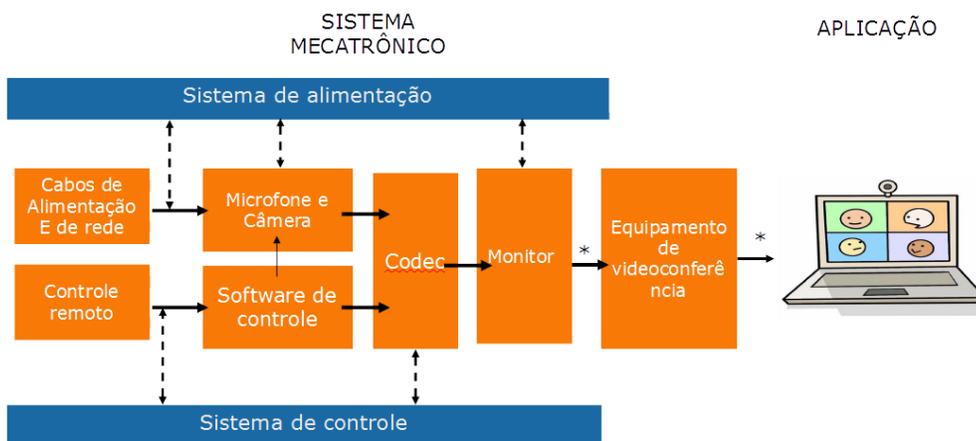


Figura 8 – Estrutura Funcional do Equipamento de Videoconferência

O funcionamento básico do terminal de videoconferência é:

- a) A imagem e o áudio locais são capturados pela (s) câmera(s) e pelo(s) microfone(s), que estão devidamente energizados e conectados ao codificador/decodificador.
- b) O áudio e a imagem recebidos pelo codificador são processados e codificados para serem transmitidos.

- c) O tráfego inverso da conexão (recebimento de áudio e vídeo de outro host) funciona de forma análoga: o decodificador recebe o sinal, decodifica a imagem e o áudio e os envia ao (s) monitor(es), exibindo os participantes de sites remotos.

O TOE é baseado em *hardware* otimizado e específico para as suas funcionalidades, controlado por *software*. Soluções de TOE baseadas exclusivamente em software ou em *desktops*/ computadores pessoais (*personal computers - PC*) não fazem parte do escopo dessa pesquisa.

4.1.1 Instalação básica do TOE

A figura 9 é a representação visual de um exemplo de implantação do TOE, cujas fronteiras estão delimitadas pela linha vermelha hachurada.

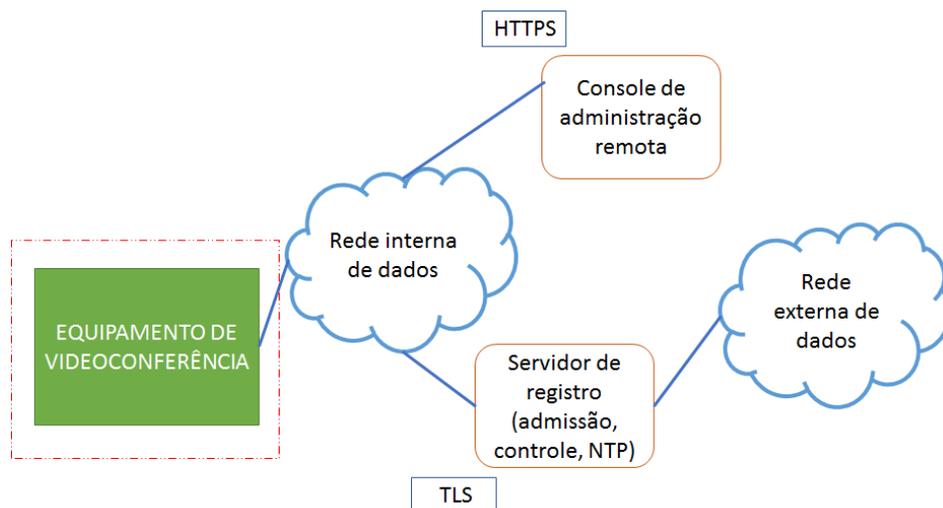


Figura 9 – Exemplo de *deploy* do TOE

O TOE inclui hardware e software de controle, conforme exposto na estrutura funcional da figura 8. O Servidor de registro e o console de administração são considerados presentes no ambiente de TI no qual o TOE está inserido.

O TOE conecta-se, através da rede interna (confiável) de dados via TLS, a um servidor de registro que atua com diversas funções: realiza a admissão e o controle do equipamento, permitindo sua administração e registro para possibilitar as conexões de videoconferência através da especificação das portas SIP ou H.323 (conforme o protocolo utilizado) e outras propriedades, como identificação e largura de banda a ser utilizada; configura serviços de data e hora através de um servidor NTP.

Através da rede interna o TOE também permite acesso ao seu console de gerenciamento, via HTTPS, onde é realizada a administração do equipamento. Já pela rede externa de dados ocorrem as conexões com a Internet.

A rede interna (confiável) de dados deve ser segregada para evitar acesso indevido e tráfego não-autorizado. Deve ser um ambiente controlado onde políticas de segurança são aplicadas.

4.1.2 Escopos físico e lógico do TOE

O TOE considerado neste trabalho é um equipamento de videoconferência genérico, tal como exposto anteriormente. Suas especificações físicas, lógicas e de controle estão descritas no quadro 4 abaixo.

Quadro 4 – Especificações do TOE (BRASIL, 2015d; BRASIL, 2015e; CISCO, 2016)

Componente	Requisitado	Uso/ Descrição proposta para o TOE
Modo de operação e largura de banda	Sim	O TOE deve operar a 30 quadros por segundo a partir de 768Kbps ou com menor largura de banda, respeitando os protocolos de vídeo utilizados.
Conector HDMI	Sim	O TOE deve apresentar interface intrínseca com conector HDMI, no mínimo três (uma conexão dedicada para a câmera e duas destinadas aos monitores). Deve seguir especificação HDMI Type A versão 1.2. As interfaces que serão usadas para a saída dos monitores (principal e secundário) devem suportar resoluções de até 1080p.
Porta Serial	Não	O TOE não deve possuir porta serial.
Conector padrão DVI-I	Sim	O TOE deve apresentar, intrinsecamente, no mínimo uma interface para entrada/saída de vídeo. Deve seguir especificação WWDG, revisão 1.0 ou 1 (um) conector padrão DE15 (D-Sub), com soquete fêmea padrão DIN 41652.
Conector duplo padrão RCA	Sim	O TOE deve apresentar um conector duplo padrão RCA, para transmissão de sinais em 2 (dois) canais (“estéreo”) ou 1(um) conector P2 estéreo com adaptador para padrão RCA.
Padrões ITU-T H.263 e ITU-T H.264	Sim	O TOE deve suportar os padrões ITU-T H.263 e ITU-T H.264.
Padrões H.225 e H.245	Sim	O TOE deve suportar os padrões H.225 e H.245.
Resoluções ativas 1920 x 1080 (1080p30), 1280 x 720 (720p30), 1024 x 576 (w576p), 704 x 576 (4CIF), 768 x 448 (w448), 512 x 288 (w288p) e 352 x 288 (CIF) a 30 (trinta) “fps” (“frames per second”)	Sim	O TOE deve suportar tais resoluções.

Resolução de vídeo “ <i>High Definition</i> ” (“HD”) 720p (1280x720) a uma taxa mínima de 30(trinta) “fps” (“ <i>frames per second</i> ”) para transmissão e recepção a 512 kbps para 30 Hz e 896 kbps para 60 Hz	Sim	O TOE deve suportar tais resoluções.
Upgrade para resolução 1080p (1920x1080 – Resolução de vídeo <i>Full HD</i>) a 1200Kbps ou 1400Kbps e 30 (trinta) fps	Sim	O TOE deve suportar tal upgrade sem alteração no hardware, por meio de inserção de licença.
Controle do ganho (AGC) Automático	Sim	O TOE deve apresentar AGC automático, ou o ambiente de TI onde o TOE está inserido deve prover ao mesmo.
Cancelamento de eco (AEC) automático	Sim	O TOE deve apresentar essa funcionalidade, ou o ambiente de TI onde o TOE está inserido deve prover ao mesmo.
Supressão de ruídos (ANS) automática	Sim	O TOE deve apresentar essa funcionalidade, ou o ambiente de TI onde o TOE está inserido deve prover ao mesmo.
Suporte às resoluções de vídeo VGA (640x480); SVGA (800x600); XGA (1024x768)	Sim	O TOE deve suportar essas resoluções quando utilizar fontes de conteúdo adicionais, a uma taxa mínima de 30 fps.
Operações através do controle remoto sem fio	Sim	O TOE deverá permitir as seguintes operações através do controle remoto: estabelecer chamada de videoconferência; controlar posição e zoom da câmera local e do site remoto; controlar o volume do som; controlar a função “mudo” do microfone local; acessar as configurações do TOE; ligar/desligar o TOE; encerrar chamada.
Uso simultâneo do áudio e do vídeo secundários e primários	Sim	O TOE deve permitir o uso simultâneo do áudio e vídeo proveniente da câmera principal e dos microfones junto à câmera, ao áudio e ao vídeo secundários.
Independência da câmera principal	Sim	O corpo do TOE não deve ser dependente do corpo da câmera principal.
Controle das câmeras	Sim	O TOE deve permitir os seguintes controles sobre as câmeras: de foco automático; de faixa de posição panorâmica horizontal (<i>pan</i>) de -90 até +90 graus, e faixa de inclinação vertical (<i>tilt</i>) de -15 até +15 graus.
Zoom óptico nas câmeras	Sim	O TOE deve possuir câmeras com zoom óptico. De aproximação mínima de 10 vezes.
Resolução das câmeras	Sim	O TOE deve possuir câmeras com resolução mínima de “ <i>Full High Definition</i> ” (1920X1080), a 30 (trinta) <i>frames per second</i> em modo “ <i>progressive scan</i> ” (1080p).
Campo de visão das câmeras	Sim	O TOE deve possuir câmeras com suporte a um campo de visão vertical total de 39 graus e um campo de visão horizontal total de 65 graus.
Controle de branco das câmeras	Sim	O TOE deve apresentar câmeras com controle de branco manual e automático.
Fonte de alimentação elétrica	Sim	O TOE deve receber energia elétrica provida por fonte de alimentação bivolt (110/220 Volts) e com frequência de 60 Hertz.

Capacidade de resolução e taxa de quadro da(s) câmera que acompanha o TOE	Sim	A(s) câmera (s) que acompanha(m) o TOE devem ser capazes de prover resolução e taxa de quadro compatíveis com o TOE. Ela(s) atuará (rão) como câmera(s) principal(is) do equipamento.
Microfone omnidirecional	Sim	O TOE deve ser acompanhado de no mínimo um microfone omnidirecional, que deve estar conectado a ele, podendo ser expandido para dois ou mais em cascata ou paralelo.
Porta física RJ45	Sim	O TOE deve apresentar ao menos uma porta física RJ45, segundo normas EIA/TIA-568-A/B, e com conexões físicas em conformidade com o padrão IEEE 802.3ab (10/100/1000 Mbps) ou superior.
Interfaces de operação com usuário e de gerenciamento e configuração	Sim	O TOE deve apresentar interface de operação com usuário pelo menos nas línguas inglesa (Estados Unidos) e portuguesa (Brasil).
Conteúdo de vídeo e áudio adicional	Sim	O TOE deve permitir a transmissão de conteúdo de vídeo e áudio adicional, gerado por fonte externa, através da utilização dos conectores de entrada e saída especificados sob os padrões ITU-T H.239 (protocolo ITU-T H.323) e BFCP (protocolo SIP). A visualização de ambos os vídeos deverá ser através de um único monitor. O TOE deve ser capaz de transmitir o som proveniente do vídeo adicional, misturado com o som capturado pelos microfones do canal principal.

Adicionalmente, conforme especificações do fabricante, *Quick Start Guide Huawei TE 30* e *datasheet* do equipamento, disponíveis no anexo A, o TOE possui vários recursos de segurança sendo que cada um deles consiste em uma funcionalidade de segurança apresentada: suporte à criptografia; identificação e autenticação; auditoria de segurança; proteção às configurações de segurança do TOE; controle de acesso; utilização de canais confiáveis.

4.1.2.1 SUPORTE À CRIPTOGRAFIA

O suporte à criptografia deve ser provido pelo TOE, de forma a proteger os dados trafegados por ele (áudio, vídeo, senhas, informações de rede).

4.1.2.2 IDENTIFICAÇÃO E AUTENTICAÇÃO

Os usuários que acessam o TOE, de forma local e remota, devem ser identificados e autenticados

4.1.2.3 AUDITORIA DE SEGURANÇA

O TOE deve permitir auditoria de segurança, através do rastreamento das atividades, logs de acessos de seus usuários e administradores, registros de chamadas.

4.1.2.4 PROTEÇÃO ÀS CONFIGURAÇÕES DE SEGURANÇA DO TOE

As configurações de segurança do TOE devem estar protegidas de acessos indevidos, evitando que quaisquer desses parâmetros sejam alterados ou excluídos, impactando em suas funcionalidades de segurança e deixando-o vulnerável à ataques cibernéticos.

4.1.2.5 CONTROLE DE ACESSO

O TOE deve possuir controle de acesso físico e lógico, impedindo que pessoas não-autorizadas o utilizem indevidamente, capturando informações sensíveis da rede onde ele se encontra e da conferência sendo transmitida.

4.1.2.6 UTILIZAÇÃO DE CANAIS CONFIÁVEIS

Devem ser utilizados canais de comunicação confiáveis na instalação do TOE, mitigando o risco de acesso físico e lógico indevidos.

4.2 REQUISITOS DE SEGURANÇA

Os requisitos de segurança são necessários para garantir um nível de segurança mínimo ao TOE. Eles envolvem os requisitos de segurança do ambiente operacional e os requisitos de segurança funcional do TOE, estando diretamente relacionados com as ameaças identificadas.

4.2.1 Requisitos de segurança do ambiente operacional do TOE

Os componentes do ambiente de TI no qual está inserido o equipamento de videoconferência genérico deve prever os seguintes requisitos expostos no quadro 5.

Quadro 5 – Componentes do Ambiente de TI (BRASIL, 2015d; BRASIL, 2015e; CISCO, 2016)

Componente	Requisitado	Uso/ Descrição proposta para o TOE
Gerenciamento da estação de trabalho via <i>web browser</i> por HTTPS	Sim	Inclui qualquer gerenciamento da estação de trabalho no ambiente de TI usando um navegador instalado que é usado pelo administrador de TOE para fornecer suporte de administração através de canais protegidos HTTPS.
Servidor NTP	Sim	O TOE suporta comunicação com um servidor NTP para sincronizar sua data e seu horário com a data e o horário do servidor.
Servidor AAA <i>Radius</i> ou <i>Tacacs+</i>	Não	Inclui qualquer servidor AAA <i>Radius</i> ou <i>Tacacs+</i> do ambiente de TI que provê mecanismos de autenticação individuais.
Servidor <i>syslog</i>	Sim	Inclui qualquer servidor <i>syslog</i> para o qual o TOE possa transmitir mensagens <i>syslog</i> referentes à auditoria das atividades.
Servidor de administração remota	Sim	Inclui qualquer unidade com o qual o TOE se comunica sobre um canal protegido TLS.
Protocolo H.323 e SIP	Sim	O TOE deve estar inserido num ambiente de TI no qual possa atender às especificações previstas no padrão ITU-

		T H.323 versão 4 e ao padrão SIP (“ <i>Session Initiation Protocol</i> ”), conforme RFC3261 do IETF, ambos para redes baseadas no protocolo <i>Internet Protocol</i> (IP).
Autenticidade e segurança	Sim	O ambiente de TI no qual o TOE está inserido deve permitir suporte à autenticidade e segurança das conexões H.323 (padrão ITU-T H.235 v3/AES).
Protocolo SNMP	Sim	Uso do protocolo SNMP, definido pelas RFC 3411 (atualizada pela RFC 5343 e RFC 5590) e 3418, como protocolo de gerência de rede. Versão 3.
Gerenciamento remoto da estação de trabalho através de SSH	Sim	O ambiente de TI onde o TOE está inserido deve permitir acesso remoto via protocolo SSH visando administração e suporte técnico.
Endereçamento de rede IPv4 e IPv6	Sim	O componente de TI onde o TOE está inserido deve prover endereçamento de rede IPv4 e IPv6. O TOE também deve suportar tais endereçamentos.
Protocolos DHCP, DNS, TCP/IP e UDP/IP	Sim	O ambiente de TI onde o TE está inserido deve prover suporte aos protocolos DHCP, DNS, TCP/IP e UDP/IP, permitindo que o TOE possa: obter endereçamento IP de forma automática através do servidor DHCP, obter resolução de nomes através do servidor DNS, obter/fornecer serviços providos pelos protocolos TCP/IP e UDP/IP. O TOE também deve estar habilitado a trabalhar com tais protocolos.
Protocolo Telnet	Não	O TOE não deve possuir habilitação para acesso remoto via TELNET.
Sessões de videoconferência	Sim	O TOE deve estar inserido em um ambiente de TI que permita o estabelecimento de: sessões entre dois TOEs conectados diretamente entre si (chamada ponto a ponto); sessões entre dois ou mais TOEs conectados via MCU (via sala virtual); sessões com até outros 3 TOEs conectados diretamente ao TOE (multiponto).
Qualidade de Serviço (QoS)	Sim	O TOE deve estar inserido no ambiente de TI que permita no mínimo o uso do padrão de qualidade DiffServ (RFC 2472 e 2475 do IETF).
Suporte aos protocolos 802.1q e 802.1x	Sim	O TOE deve suportar os protocolos 802.1q (RFC 4675 do IEEE) e 802.1x (RFC 3748 do IEEE).

4.2.2 Requisitos de segurança funcionais do TOE

Segundo *Common Criteria* (2012a), existem três grupos com interesse geral na avaliação das propriedades de segurança dos TOEs: consumidores, avaliadores e desenvolvedores. Os critérios de avaliação contidos no CC estão estruturados de forma a atender às necessidades dos três grupos mencionados.

A proposta fundamental e a justificativa do processo de avaliação é atestar que a avaliação preenche as necessidades dos consumidores. Eles podem usar os resultados dessa avaliação no auxílio à decisão de qual TOE atende às suas necessidades de segurança, as quais geralmente são identificadas a partir da análise de riscos e do direcionamento das políticas de segurança.

Esses requisitos de segurança dos consumidores (ou de grupos e comunidades de interesse) são expressos de forma clara e dispostos estruturalmente de forma independente de implementação através de perfis de proteção (*Protection Profile - PP*).

No quadro 6 os requisitos de segurança do TOE encontram-se detalhados.

Quadro 6 – Requisitos do TOE (BRASIL, 2015d; BRASIL, 2015e; CISCO, 2016)

Componente	Requisitado	Uso/ Descrição proposta para o TOE
Autenticação e registro em gatekeeper	Sim	O ambiente de TI onde o TOE está inserido deve prover a esse o seu registro e sua autenticação nos protocolos H.323 e SIP, simultaneamente.
Suporte aos protocolos H.460.18 e H.460.19	Sim	O ambiente de TI onde o TOE está inserido deve prover suporte aos protocolos H.460.18 e H.460.19, possibilitando a travessia transparente de firewalls nas comunicações estabelecidas pelo TOE.
Capacidade de ter as atividades auditadas/rastreáveis	Sim	O TOE deve permitir o registro de logs com suas atividades, possibilitando a rastreabilidade e a auditoria de segurança.
Criptografia ativa	Sim	O TOE deve possuir criptografia ativa em suas comunicações, mitigando o risco de seu tráfego de áudio e vídeo ser interceptado por elementos não-autorizados.
Autenticação e identificação de usuários	Sim	O TOE deve possuir usuários de gerenciamento com diferentes níveis de acesso, autenticando e identificando todo e qualquer acesso ao seu console administrativo.
Proteção contra acesso indevido	Sim	O TOE deve apresentar proteção contra acesso indevido (físico e lógico). O acesso físico refere-se à sua guarda e utilização em sala mantida a salvo de usuários não-autorizados. Já o acesso lógico refere-se à utilização de usuários e credenciais para acessar seu console de administração.

4.3 DEFINIÇÃO DO AMBIENTE DE SEGURANÇA

Considerando o TOE um dispositivo conectado à rede de telecomunicação, o ambiente de segurança no qual ele está inserido provê uma quantidade mínima de requisitos de segurança, conforme a política de segurança da informação (POSIC) da organização, que apresenta funcionalidades de segurança.

Dessa forma, o TOE estará exposto às mesmas ameaças e às mesmas funcionalidades de segurança as quais a rede de dados estiver exposta, assim como qualquer outro dispositivo de rede.

Tais ameaças e premissas são abordadas neste trabalho, pois relacionam-se ao TOE, direta ou indiretamente, ou seja, referem-se ao ambiente, físico e lógico, no qual o TOE está inserido.

São boas práticas de mercado adotadas pelos administradores de segurança, recomendadas também pelas normas NBR 27001:2006, NBR 27002:2005, NBR 27005:2008, além das Normas Complementares 07 e 17 do Gabinete da Segurança Institucional da Presidência da República (GSIPR), e padrões internacionais como o *Common Criteria*.

Segundo Cisco (2016), as funcionalidades comuns de segurança ao TOE e à rede de dados são: a comunicação (autorizada e não-autorizada); a capacidade de auditar as atividades dos elementos; a habilidade de executar atualizações válidas ou seguras; o armazenamento seguro dos dados e sua utilização através de credenciais de administrador; a habilidade de criticar a auto verificação de seus componentes contra falhas, através de monitoramento.

4.3.1 Ameaças

As ameaças consideradas neste trabalho relacionam-se às ameaças externas, tentativas de acesso e modificação de dados não-autorizadas, além de outros tráfegos críticos de rede, tais como dados de transações bancárias e de informações pessoais. A sensibilidade das informações trafegadas depende da avaliação de cada instituição.

Conforme os requisitos do *Common Criteria*, seguem as ameaças de segurança consideradas nesse trabalho:

- a) FAU – *Family Security Audit (Família de Auditoria de Segurança)* - Auditoria de segurança/ rastreabilidade (T.UNDETECTED_ACTIVITY)

A auditoria das atividades auxilia o administrador de rede a monitorar o status dos equipamentos, analisar problemas e registrar eventos de segurança. É importante que as atividades possam ser rastreadas, gerando relatórios, pois a partir deles podem ser detectados indícios ou falhas de funcionalidades de segurança.

Os dados de auditoria registrados devem ser armazenados em local seguro, de forma a evitar acesso indevido e exclusão/alteração não autorizada.

Um agente invasor pode buscar o acesso ao TOE e modificar suas funcionalidades de segurança sem que o administrador tome conhecimento. Assim, o TOE se torna vulnerável a ataques, sendo que seu administrador sequer toma conhecimento.

- b) FCS – *Family Cryptographic Support* (Família de Suporte à Criptografia): Criptografia falha (T.WEAK_CRYPTOGRAPHY)

O uso de algoritmos criptográficos fracos ou a ausência de criptografia não protege de forma eficaz os dispositivos contra acesso indevido, já que o tráfego de dados não é protegido. Assim, o TOE fica exposto às ameaças de leitura, escrita e manipulação dos dados críticos.

- c) FIA/ FTA – *Family Identification and Authentication/ Family TOE Access* (Família Identificação e Autenticação/ Família Acesso ao TOE) - Acesso indevido (físico/lógico) (T. UNAUTHORIZED_ADMINISTRATOR_ACCESS/ T. PASSWORD_CRACKING)

Através de um acesso indevido, um intruso pode acessar o TOE como administrador, mascarando-se como tal ou reproduzindo sessões de acesso administrativas. Com esse acesso as funcionalidades de segurança são comprometidas, pois ações mal-intencionadas podem partir desse acesso.

Agentes indevidos podem aproveitar-se de senhas fracas e acessar o controle administrativo do TOE. Dessa forma, o invasor pode acessar a rede, seu tráfego, e as ligações do TOE com outros dispositivos de rede.

- d) FPT – *Family Protection of the TSF (TOE Security Functionality)* – Família Proteção do TSF (Funcionalidades de Segurança do TOE) (T.SECURITY_FUNCTIONALITY_FAILURE)

O TOE pode falhar durante o seu reinício ou sua operação, o que pode comprometer as funcionalidades de segurança do dispositivo deixando-o susceptível a ataques. Um auto teste de seus componentes mais críticos colaboraria para garantir a confiabilidade das suas funcionalidades de segurança.

- e) FTP – *Family Trusted Path/Channels* – Família Canais de Comunicação Confiáveis (T.UNTRUSTED_COMMUNICATION_CHANNELS)

Com a utilização de canais de comunicação não-confiáveis, o tráfego de dados do TOE fica exposto a ataques, facilitando a captura de seus pacotes. Além disso, o acesso ao seu console administrativo também pode ser alvo de invasores, e suas funcionalidades de segurança estarão expostas.

4.3.2 Premissas

As premissas a seguir elencadas referem-se aos requisitos de segurança utilizados no desenvolvimento do TOE e as condições essenciais do ambiente no qual está sendo utilizado. Elas são admitidas como boas práticas na maioria dos PPs dos dispositivos de rede.

Assume-se que o ambiente operacional provê ao TOE as seguintes funcionalidades:

- a) Proteção física (OE.PHYSICAL): somente pessoas autorizadas terão acesso físico ao TOE, que permanece em sala de reunião com dispositivo de tranca à chave;
- b) Proteção ao tráfego de dados (OE.NO_THRU_TRAFFIC_PROTECTION): a rede na qual o TOE atua apresenta proteção ao tráfego de dados, ou seja, os dados que trafegam pela rede de comunicação de dados na qual o TOE se insere são protegidos contra acesso indevido;
- c) Acesso de administrador realizado via credenciais seguras (OE.TRUSTED_ADMIN/OE.ADMIN_CREDENTIALS_SECURE): o ambiente de operação no qual o TOE está inserido deve possuir senha de acesso administrador, protegendo-o contra acesso indevido e garantindo rastreabilidade às atividades de auditoria. Assim garante-se a autenticidade do usuário que acessa o ambiente, protegendo-se o TOE de acesso malicioso;
- d) Atualizações de firmware dos elementos de rede (OE.UPDATES): o ambiente operacional do TOE deve estar com o firmware dos seus elementos de rede atualizados, de forma a manter o ambiente protegido contra vulnerabilidades conhecidas.

4.3.3 Política de segurança da informação

Políticas de segurança da informação e comunicações (POSIC) norteiam as atividades relacionadas ao ciclo de vida da informação nas organizações.

Considerando que cada entidade possui atividade-fim distinta, segundo suas especificidades a POSIC é elaborada e adotada.

O TOE deve apresentar um *banner* de segurança assim que for acessado logicamente (via Web/Telnet), mostrando que aquele acesso somente deve ser realizado conforme as instruções da POSIC da organização (P.ACCESS_BANNER). Essa política é usada como melhores práticas pelos administradores de infraestrutura de rede (CISCO, 2016).

4.4 PERFIL DE PROTEÇÃO DO TOE

Esta seção apresenta de fato o perfil de proteção para o TOE abordado nesse trabalho com base nos requisitos, ameaças, premissas e políticas de segurança da informação descritas anteriormente. A fim de verificar os requisitos de segurança descritos acima, serão detalhadas as atividades necessárias para avaliá-los.

- 1) *FAU – Family Security Audit* (Família Auditoria de Segurança): O avaliador deverá verificar a capacidade do TOE ter suas atividades rastreadas.

FAU_GEN.1 - Family Security Audit Data Generation (Família Geração de Dados de Auditoria de Segurança): Devem ser gerados e gravados dados auditáveis no TOE para atividades específicas.

1.1.FAU_GEN.1.1: Seguem as atividades que deverão ser auditadas:

- ligar, desligar e reiniciar o TOE;
- iniciar, manter e encerrar chamadas de videoconferência;
- logar e deslogar do console administrativo (individualmente, se o sistema permitir um login individual);
- alterar as configurações de segurança (habilitação/desabilitação de criptografia; habilitação/desabilitação do protocolo H460), mantendo registro do usuário que efetuou a mudança e os valores modificados;
- resetar/alterar senhas de login administrativo (individualmente, se o sistema permitir um login individual).

O TOE deve permitir alteração e configuração do nível de auditoria desejado: leve, moderado e severo. Tais níveis de auditoria são configurados da forma que o administrador de segurança definir: caso ele deseje que a criticidade do registro seja baixa, média ou alta, respectivamente.

1.2.FAU_GEN.1.2: Deve ser registrada uma gravação de cada uma das atividades/eventos, com informações de data, hora e o tipo do evento detectados, segundo exposto no quadro 5.

1.3. FAU_GEN.2: Cada registro gravado deve ser capaz de associar o usuário individual responsável pelo evento.

- 2) *FCS – Family Cryptographic Support* (Família de Suporte à Criptografia): o avaliador deverá verificar se o TOE emprega funcionalidades criptográficas, de modo a atingir os níveis de segurança desejados.

As funções de criptografia podem ser aplicadas através de hardware, software ou firmware.

FCS_COP - Family Cryptographic Operation (Família de Operação Criptográfica): verifica o uso operacional das chaves criptográficas.

O evento “Alteração de configurações de segurança” na geração de dados auditáveis **FAU_GEN.2** deve trazer as seguintes informações: sucesso/ falha (mínimas), tipo de operação criptográfica (mínimas), modo de operação criptográfica (básicas), atributos (básicas).

1.4. FCS_COP.1: o avaliador deve verificar se o TOE apresenta chamadas com criptografia ativa (suporte a H.235 e fluxo de mídia AES – Advanced Encryption Standard, se a chamada for realizada em H.323; suporte à sinalização TLS – *Third-Level Support* e fluxos de mídia SRTP – *Secure Real-Time Transport Protocol*, se em SIP). Deve ser avaliado também o tamanho da chave criptográfica (mínimo de 128 bits).

- 3) *FIA/ FTA – Family Identification and Authentication/ Family TOE Access* (Família Identificação e Autenticação/ Família Acesso ao TOE) - Acesso indevido (lógico) (T. UNAUTHORIZED_ADMINISTRATOR_ACCESS/ T. PASSWORD_CRACKING): O avaliador deverá verificar se o TOE permite identificar e constatar a identidade dos usuários que realizam acesso administrativo lógico, determinando a qual nível de

privilégios ele faz parte e seu nível de interação com o TOE. Além disso, o avaliador também deve atestar que o TOE controla o estabelecimento de uma sessão de usuário.

O avaliador deve verificar, ainda, se o TOE provê mecanismo de *login* baseado em usuário/senha, onde tal senha deve ser mantida obscura durante o *logon*, evitando que ela seja visualizada por um possível invasor enquanto é digitada, e durante seu armazenamento. Essa credencial deve ser considerada forte, mantendo uma combinação de letras maiúsculas/letras minúsculas/números e caracteres especiais.

Por último, ele deve atestar que o TOE apenas realiza chamadas de videoconferência se estiver autenticado no servidor da solução tecnológica. Tal autenticação é baseada em *white list*, ou seja, apenas se os dados do TOE estiverem inseridos na *white list* ele se registrará.

FIA_AFL – *Family Authentication Failures* (Família Falhas de Autenticação): o avaliador deve verificar se há algum mecanismo no TOE que realize a detecção de falhas de autenticação.

1.5. FIA_AFL.1: o avaliador deve verificar um número máximo de tentativas sem sucesso de autenticação ao TOE, e quais ações devem ser tomadas no caso desse número de tentativas ser alcançado.

O evento “Logar e deslogar do console administrativo” na geração de dados auditáveis **FAU_GEN.2** deve trazer as seguintes informações mínimas: quantidade de tentativas sem sucesso de *logon*; ações básicas a serem tomadas.

FIA_ATD – *Family User Attribute Definition* (Família Definição de Atributos do Usuário): O avaliador deve verificar se existem atributos definidos para os acessos administrativos (lógicos) dos usuários.

1.6. FIA_ATD.1: o avaliador deve verificar a existência da definição de níveis de acesso para os usuários, ou seja, o acesso às configurações administrativas de segurança do TOE está segmentado pelo tipo de usuário (comum/administrador).

FIA_SOS – *Family Specification of Secrets* (Família Especificação de Senhas): deve ser constatado se há gerenciamento sobre as definições de senhas, ou seja, se há mecanismos para garantir as métricas de qualidade definidas pelo administrador de segurança.

1.7. FIA_SOS.1: o avaliador deve analisar se o TSF provê mecanismos para verificar se as senhas atendem às especificações das métricas de qualidade.

1.8. FIA_SOS.2: o avaliador deve analisar se as seguintes métricas determinadas pelo administrador de segurança estão habilitadas: se as senhas usadas são validadas pelo TSF (*TOE Security Functionality*) com relação à força (possuem quantidade mínima de caracteres, números, letras maiúsculas e minúsculas); se ao digitar a senha, a mesma é apresentada obscura (representada por “*” asteriscos); se a senha é armazenada obscura.

O evento “Resetar/alterar senhas de *login* administrativo” na geração de dados auditáveis **FAU_GEN.2** deve trazer as seguintes informações: rejeição pelo TSF da senha testada (mínimas); rejeição ou aceitação de qualquer senha testada (básicas); identificação de mudanças às métricas de qualidade adotadas (detalhadas).

FIA_UAU– *Family User Authentication* (Família Autenticação de Usuário): avalia-se os mecanismos de autenticação dos usuários suportados pelo TSF.

1.9. FIA_UAU.1: o avaliador deve verificar se o TOE permite gerenciar os dados de autenticação do usuário, assim como as ações que podem ser tomadas antes do usuário se autenticar.

O evento “Logar e deslogar do console administrativo” na geração de dados auditáveis **FAU_GEN.2** deve trazer as seguintes informações: insucesso no uso do mecanismo de autenticação (mínima); utilização do mecanismo de autenticação (básica); ações intermediadas pelo TSF realizadas antes da autenticação do usuário.

1.10. FIA_UAU.2: o avaliador deve validar que o usuário somente consegue acessar o menu administrativo e alterar suas configurações do TOE após a sua autenticação, conforme definido no TSF.

O evento “Alterar as configurações de segurança” na geração de dados auditáveis **FAU_GEN.2** deve trazer as seguintes informações: insucesso no uso do mecanismo de autenticação (mínima); utilização do mecanismo de autenticação (básica).

1.11. FIA_UAU.3: o avaliador deve verificar se há mecanismo que detecta e evita que os dados de autenticação dos usuários sejam copiados ou forjados.

1.12. FIA_UAU.4: o avaliador deve averiguar se há mecanismo que habilite o *single sign on* do usuário.

1.13. FIA_UAU.5: o avaliador deve verificar se há mecanismos de autenticação múltipla, para prover a autenticação dos usuários em eventos específicos.

Deve ser verificado também se apenas após o registro do TOE no servidor *gatekeeper* da solução (*white list*) o TOE está habilitado para realizar chamadas de videoconferência.

O evento “Alterar as configurações de segurança” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: o resultado final da autenticação (mínima); o resultado de cada mecanismo ativado (básica).

O evento “Iniciar, manter e encerrar chamadas de videoconferência” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: o resultado final da autenticação no *gatekeeper*, com data e hora (mínima); o resultado de cada mecanismo ativado – tentativa de chamada/em chamada/encerramento de chamada (básica).

1.14. FIA_UAU.6: o avaliador deve verificar se, para os eventos especificados pelo administrador de segurança, a reautenticação dos usuários está ativa.

O evento “Alterar as configurações de segurança” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: a falha na reautenticação (mínima); todas as tentativas de reautenticação (básica).

1.15. FIA_UAU.7: o avaliador deve verificar se somente as informações permitidas pelo administrador de segurança são retornadas aos usuários durante a autenticação.

FTA – Family TOE Access (Família Acesso ao TOE): avalia-se a autenticação e identificação de usuários no acesso lógico ao TOE, controlando o estabelecimento das sessões do usuário.

FTA_MCS – *Family Limitation on Multiple Concurrent Sessions* (Família Limitação em Múltiplas Sessões Concorrentes): avalia-se os requisitos para estabelecer limites no número de sessões concorrentes de um mesmo usuário.

1.16. FTA_MCS.1: o avaliador deve verificar se o administrador de segurança previu limitação no número de acessos simultâneos de um mesmo usuário.

1.17. FTA_MCS.2: o avaliador deve verificar se o número de limitações de acessos simultâneos definido pelo administrador de segurança está sendo verificado.

O evento “Logar e deslogar do console administrativo” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: rejeição de uma nova sessão decorrente da limitação de sessões múltiplas concorrentes (mínima); captura do número de sessões simultâneas do usuário (básica).

FTA_SSL – *Family Session Locking and Termination* (Família Travamento de Sessão e Término): avalia requisitos para o TSF prover travamento, destravamento, início e término de sessões interativas do usuário.

1.18. FTA_SSL.1: o avaliador deve verificar se está previsto no TSF: travar a sessão interativa após um certo período de inatividade do usuário; se esse tempo de inatividade é padrão para todos os usuários ou se é possível especificar tempos específicos para cada usuário; se deve ocorrer algum evento antecipadamente ao travamento da sessão.

1.19. FTA_SSL.2: o avaliador deve verificar se é possível o usuário travar e destravar sua própria sessão interativa.

O evento “Logar e deslogar do console administrativo” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: travamento de sessão pelo mecanismo de travamento (mínima); destravamento de sessão (básica); qualquer tentativa de destravamento de sessão (detalhada).

1.20. FTA_SSL.3: o avaliador deve verificar se está previsto no TSF encerrar a sessão interativa após um certo período de inatividade do usuário; se esse tempo de inatividade é padrão para todos os usuários ou se é possível especificar tempos específicos para cada usuário; se deve ocorrer algum evento antecipadamente ao término da sessão.

O evento “Logar e deslogar do console administrativo” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: término de sessão pelo mecanismo de travamento (mínima).

1.21. FTA_SSL.4: o avaliador deve verificar se é possível o usuário encerrar sua própria sessão interativa.

O evento “Logar e deslogar do console administrativo” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: término de sessão pelo usuário (mínima).

- 4) *FPT – Family Protection of the TSF (TOE Security Functionality)* – Família Proteção do TSF (Funcionalidades de Segurança do TOE) (T.SECURITY_FUNCTIONALITY_FAILURE): o avaliador deverá verificar os requisitos funcionais relacionados à integridade dos dados e ao gerenciamento dos mecanismos do TSF.

FPT_FLS – Family Fail Secure (Família Falha de Segurança): o avaliador deve verificar requisitos que o TOE sempre conterà em seus requisitos SFRs nos eventos identificados como falhas no TSF.

1.22. FPT_FLS.1: O avaliador deve verificar se o TSF preserva um estado seguro em caso de falhas identificadas.

Os eventos “Ligar, desligar e reiniciar o TOE” e “Iniciar, manter e encerrar chamadas de videoconferência” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: falha apresentada (mínima).

FPT_TEE - Family Testing of External Entities (Família Teste de Entidades Externas): o avaliador deve verificar em testes que o TOE consegue conectar-se a entidades externas, tais como servidores de tempo e de registro.

1.23. FPT_TEE.1: O avaliador deve verificar que o TOE realiza testes de comunicação com o servidor de horários da rede através do protocolo NTP (Network Time Protocol) para sincronização de seu relógio, realizados a cada 1 hora.

O evento “Alterar as configurações de segurança” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: falha em receber informações do teste do servidor de horários (mínima).

1.24. FPT_TEE.2: O avaliador deve verificar que o TOE realiza testes de comunicação com o servidor de registro/*gatekeeper*, realizados a cada 5 minutos.

O evento “Iniciar, manter e encerrar chamadas de videoconferência” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: falha em receber informações do teste de registro no *gatekeeper* (mínima).

- 5) *FTP – Family Trusted Path/Channels*– Família Canais de Comunicação Confiáveis (T.UNTRUSTED_COMMUNICATION_CHANNELS): o avaliador deverá verificar se o TOE realiza as suas comunicações com os demais dispositivos de rede utilizando-se de canais de comunicação confiáveis.

FTP_TRP – Family Trusted Path (Família Canal Confiável): o avaliador deve verificar que o TOE apresenta suporte à utilização de canais de comunicação confiáveis.

1.25. FTP_TRP.1: o avaliador deve verificar que o TOE apresenta suporte aos protocolos H.460.18 e H.460.19, possibilitando a realização das chamadas de videoconferência em redes que possuem firewalls.

O evento “Iniciar, manter e encerrar chamadas de videoconferência” na geração de dados auditáveis FAU_GEN.2 deve trazer as seguintes informações: ativação do protocolo H.460 (mínima).

O quadro 7 reúne os requisitos funcionais do PP, assim como os eventos auditáveis relacionados a cada um dos requisitos, além das informações adicionais ao registro do evento.

Alguns eventos podem ser classificados em três níveis de auditoria, conforme desejado pelo administrador de segurança do ambiente: leve, moderado ou severo. Outros exigem ainda a data e a hora em que ocorreram. Tais informações são tratadas como adicionais ao seu registro.

Quadro 7 – Requisitos funcionais e eventos auditáveis

Requisito de segurança	Evento auditável	Informações adicionais ao registro do evento	
Família Geração de Dados de Auditoria de Segurança (Family Security Audit Data Generation – FAU-GEN)	1.1. FAU_GEN.1.1	Ligação, desligamento e reinício do TOE	Nível de auditoria desejado: leve/moderado/severo
		Início, manutenção e encerramento da chamada	Nível de auditoria desejado: leve/moderado/severo
		<i>Login</i> e <i>logout</i> do console administrativo	Nível de auditoria desejado: leve/moderado/severo
		Alteração de configurações de segurança	Nível de auditoria desejado: leve/moderado/severo
		Reset/alteração de senhas de login administrativo	Nível de auditoria desejado: leve/moderado/severo
	1.2. FAU_GEN.1.2	Ligação, desligamento e reinício do TOE	Data, hora e tipo do evento
		Início, manutenção e encerramento da chamada	Data, hora e tipo do evento
		<i>Login</i> e <i>logout</i> do console administrativo	Data, hora e tipo do evento
		Alteração de configurações de segurança	Data, hora e tipo do evento
		Reset/alteração de senhas de login administrativo	Data, hora e tipo do evento
	1.3.FAU_GEN.2	Ligação, desligamento e reinício do TOE	Usuário individual responsável pelo evento
		Início, manutenção e encerramento da chamada	Usuário individual responsável pelo evento
		<i>Login</i> e <i>logout</i> do console administrativo	Usuário individual responsável pelo evento

		Alteração de configurações de segurança	Usuário individual responsável pelo evento
		Reset/alteração de senhas de login administrativo	Usuário individual responsável pelo evento
Família de Suporte à Criptografia – Operação Criptográfica (<i>Family Cryptographic Support_ Cryptographic Operation – FCS_COP</i>)	1.4.FCS_COP.1	Criptografia ativa em suas comunicações	Sucesso/falha; modo de operação criptográfica
Família de Identificação e Autenticação - Falhas de Autenticação – (<i>Family Identification and Authentication - Authentication Failures - FIA_AFL</i>)	1.5.FIA_AFL.1	Logar e deslogar do console administrativo	Quantidade de tentativas sem sucesso de <i>logon</i> ; ações básicas a serem tomadas
Família de Identificação e Autenticação - Definição de Atributos do Usuário (<i>Family Identification</i>)	1.6.FIA_ATD.1		

<i>and Authentication - Family User Attribute Definition - FIA_ATD)</i>			
Família de Identificação e Autenticação - Especificação de Senhas (<i>Family Identification and Authentication - Family Specification of Secrets – FIA_SOS</i>)	1.7.FIA_SOS.1	Resetar/alterar senhas de login administrativo	Rejeição pelo TSF da senha testada (mínimas); rejeição ou aceitação de qualquer senha testada (básicas); identificação de mudanças às métricas de qualidade adotadas (detalhadas)
	1.8.FIA_SOS.2		
Família de Identificação e Autenticação - Autenticação de Usuário (<i>Family Identification and Authentication - Family User Authentication – FIA_UAU</i>)	1.9.FIA_UAU.1	Logar e deslogar do console administrativo	Insucesso no uso do mecanismo de autenticação (mínima); utilização do mecanismo de autenticação (básica); ações intermediadas pelo TSF realizadas antes da autenticação do usuário
	1.10.FIA_UAU.2	Alterar as configurações de segurança	Insucesso no uso do mecanismo de autenticação (mínima); utilização do mecanismo de autenticação (básica)
	1.11.FIA_UAU.3		
	1.12.FIA_UAU.4		
	1.13.FIA_UAU.5	Alterar as configurações de segurança	O resultado final da autenticação (mínima); o resultado de cada mecanismo ativado (básica)

		Iniciar, manter e encerrar chamadas de videoconferência	O resultado final da autenticação no <i>gatekeeper</i> , com data e hora (mínima); o resultado de cada mecanismo ativado – tentativa de chamada/em chamada/encerramento de chamada (básica)
	1.14.FIA_UAU.6	Alterar as configurações de segurança	A falha na reautenticação (mínima); todas as tentativas de reautenticação (básica)
	1.15.FIA_UAU.7		
Família Acesso ao TOE - Limitação em Múltiplas Sessões Concorrentes (<i>Family TOE Access - Family Limitation on Multiple Concurrent Sessions – FTA_MCS</i>)	1.16.FTA_MCS.1		
	1.17.FTA_MCS.2	Logar e deslogar do console administrativo	Rejeição de uma nova sessão decorrente da limitação de sessões múltiplas concorrentes (mínima); captura do número de sessões simultâneas do usuário (básica)
Família Acesso ao TOE - Travamento de Sessão e Término (<i>Family TOE Access - Family Session Locking and Termination – FTA_SSL</i>)	1.18.FTA_SSL.1		
	1.19.FTA_SSL.2	Logar e deslogar do console administrativo	Travamento de sessão pelo mecanismo de travamento (mínima); destravamento de sessão (básica); qualquer tentativa de destravamento de sessão (detalhada)
	1.20.FTA_SSL.3	Logar e deslogar do console administrativo	Término de sessão pelo mecanismo de travamento
	1.21.FTA_SSL.4	Logar e deslogar do console administrativo	Término de sessão pelo usuário
	1.22.FPT_FLS.1	Ligar, desligar e reiniciar o TOE	Falha apresentada

<p>Família Proteção do TSF - Funcionalidades de Segurança do TOE/ Falha de Segurança (<i>Family Protection of the TSF - TOE Security Functionality/ Family Fail Secure – FPT_FLS</i>)</p>		<p>Iniciar, manter e encerrar chamadas de videoconferência</p>	
<p>Família Proteção do TSF - Funcionalidades de Segurança do TOE/ Família Teste de Entidades Externas (<i>Family Protection of the TSF - TOE Security Functionality/ Family Testing of External Entities – FPT_TEE</i>)</p>	<p>1.23.FPT_TEE.1</p>	<p>Alterar as configurações de segurança</p>	<p>Falha em receber informações do teste do servidor de horários</p>
	<p>1.24.FPT_TEE.2</p>	<p>Iniciar, manter e encerrar chamadas de videoconferência</p>	<p>Falha em receber informações do teste de registro no <i>gatekeeper</i></p>
<p>Família Canais de Comunicação Confiáveis/ Canal Confiável (<i>Family Trusted Path/Channels – Trusted Path - FTP_TRP</i>)</p>	<p>1.25.FTP_TRP.1</p>	<p>Iniciar, manter e encerrar chamadas de videoconferência</p>	<p>Ativação do protocolo H.460</p>

A coluna “evento auditável” explicita qual é o evento relacionado ao requisito identificado no PP. Por exemplo, o requisito FIA_ UAU.2 é auditado através do evento “Alterar as configurações de segurança”.

5. RESULTADOS E DISCUSSÕES

Nos testes deste trabalho busca-se comparar o TOE ao perfil de proteção elaborado, com a finalidade de atestar se o primeiro está ou não conforme o PP.

Em ambiente controlado, num laboratório, será montada uma rede de dados simulando o ambiente de operação do TOE. O equipamento de videoconferência será configurado conforme a POSIC utilizada em determinada organização financeira da APF.

O próximo passo é simular as condições de uso do terminal, realizando e recebendo chamadas de videoconferência, a fim de verificar se os requisitos de segurança relacionados no PP são atendidos pelo TOE. Os parâmetros considerados nos requisitos de segurança serão tratados como variáveis.

A fim de validar o *protection profile* desenvolvido, serão realizados testes dos requisitos levantados, verificando se os eventos auditáveis relacionados no quadro 6 estão ou não presentes no TOE.

Primeiramente, definiu-se o TOE como o equipamento de videoconferência TE30, marca Huawei, levando-se em conta a disponibilidade de tal terminal para a realização do trabalho.

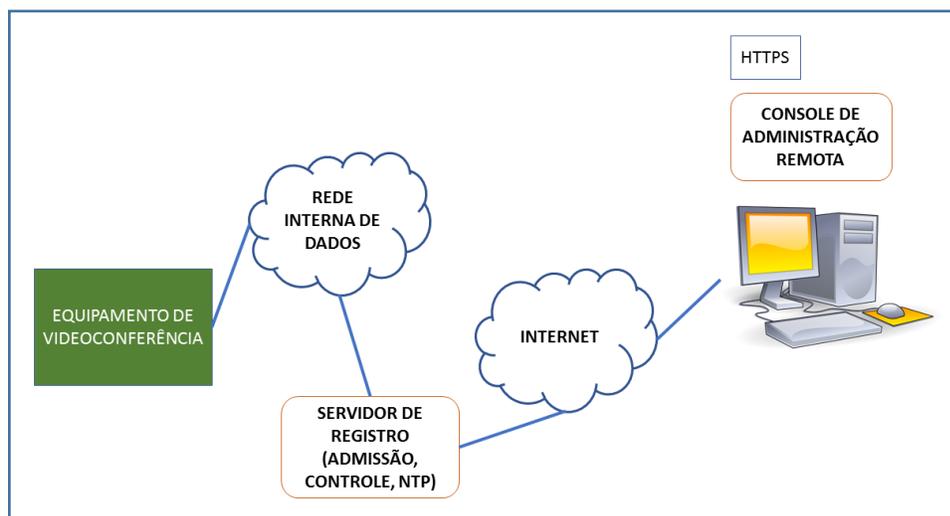


Figura 10 – Esquema lógico do sistema de análise

O sistema considerado neste trabalho está representado na figura 10.

Em seguida, o TOE foi instalado e configurado de forma a simular as seguintes condições através do console de administração remota, conforme estabelecido no PP (item 4.4), já que os cinco eventos relacionados a seguir cobrem os 25 requisitos levantados:

- a) ligar, desligar e reiniciar o TOE;
- b) iniciar, manter e encerrar chamadas de videoconferência;
- c) logar e deslogar do console administrativo (individualmente, se o sistema permitir um *login* individual);
- d) alterar as configurações de segurança (habilitação/desabilitação de criptografia; habilitação/desabilitação do protocolo H460), mantendo registro do usuário que efetuou a mudança e os valores modificados;
- e) resetar/alterar senhas de login administrativo (individualmente, se o sistema permitir um *login* individual).

Serão realizadas cinco simulações de cada uma das situações de uso do equipamento de videoconferência descritas no perfil de proteção exposto. As simulações serão apenas para os cinco eventos, já que os registros gerados pelo TOE geram um único log para as funções contidas no mesmo evento. Por exemplo, para as atividades “ligar, desligar e reiniciar” é criado um mesmo tipo de registro.

5.1 RESULTADOS DOS REGISTROS

Os eventos estão registrados em arquivo no formato *XML (eXtensible Markup Language)*, gerado pelo TOE, disponíveis para consulta nos apêndices B e C.

Os níveis de auditoria são: informações, erro e crítico. Não é possível alterar esses níveis, pois o TOE não permite. Apenas é possível consultá-los, conforme a determinação do fabricante.

São sete as categorias dos registros, que são chamadas de módulos: Controle principal, *WEB*, *IU*, *BSP*, Áudio, Vídeo e Protocolo.

O Controle principal contém comandos administrativos para controlar o funcionamento do TOE, tais como ligá-lo, desligá-lo, iniciar e encerrar chamadas. Em *WEB* ficam condensadas as opções de configuração relacionadas à conectividade do TOE, ou seja, basicamente informações de sua rede de dados.

IU é referente à interface do usuário (*interface user*): quais são os menus disponíveis para o usuário interagir com o TOE. BSP detalha o status da placa processadora do TOE, ou seja, tudo relacionado ao hardware do equipamento mecatrônico. Os módulos Áudio e Vídeo trazem informações sobre áudio e vídeo do TOE, respectivamente, enquanto que Protocolo contém informações dos protocolos de chamada usados pelo TOE.

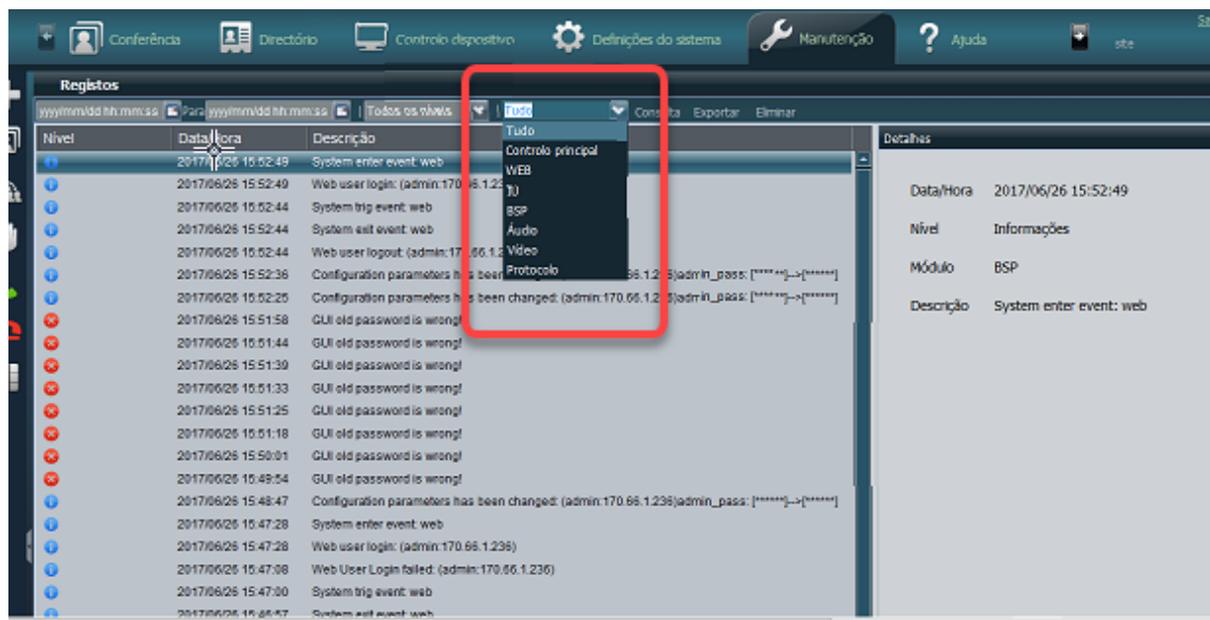


Figura 11 – Consulta dos registos em MANUTENÇÃO > REGISTROS.

Conforme exposto na figura 11, é possível consultar os registos no log informando o período desejado, o nível e a categoria do evento auditado.

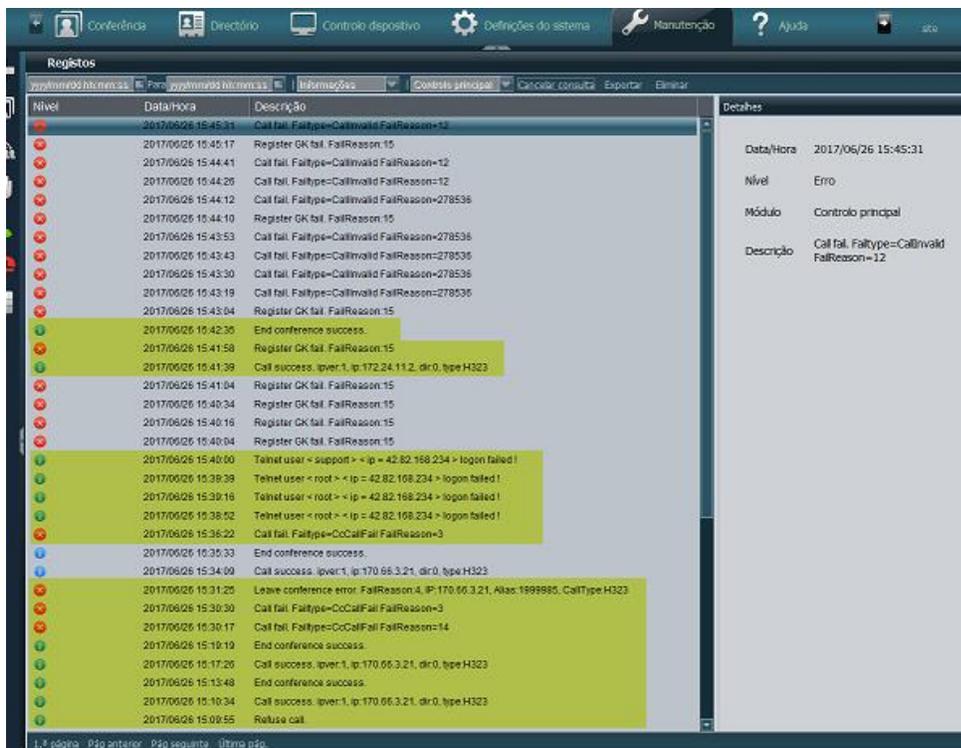


Figura 12 – Consulta dos registos: início, término e falha de chamada (linhas 16, 26 e 25/28/35, respectivamente).

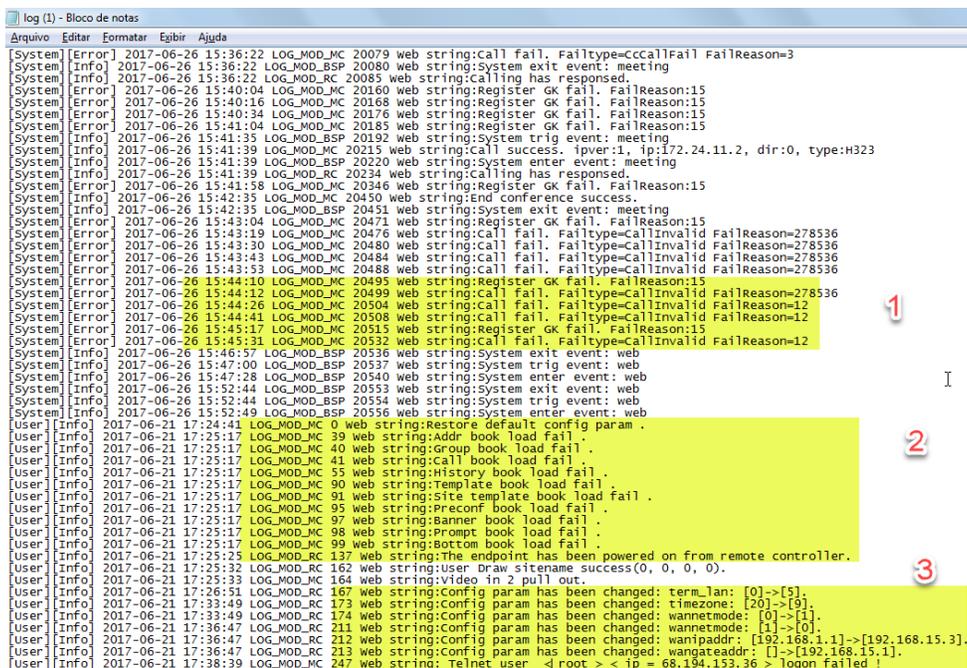


Figura 13 – Consulta do arquivo XML: falha no registo no servidor (destacado em 1); reset e alteração de configurações de segurança (destacados em 2 e 3).

As evidências obtidas verificando os eventos relacionados a cada requisito de segurança estão consolidadas no quadro 8.

Quadro 8 – Eventos verificados

Evento auditado	Informações localizadas no registro do log	Requisito de segurança
Ligação, desligamento e reinício do TOE	Módulo BSP - Nível de auditoria: informações sobre ligação, desligamento e reinício do TOE/equipamento	1.1.FAU_GEN.1.1
Início, manutenção e encerramento da chamada	Módulo: Controlo principal - Níveis de auditoria: informações (início/término), erro (falha, reportada quando estava sem registro e foi solicitado o início de uma chamada).	1.1.FAU_GEN.1.1
<i>Login</i> e <i>logout</i> do console administrativo	Módulo: WEB - Nível de auditoria: informações (em caso de sucesso), erro (em caso de falha)	1.1.FAU_GEN.1.1
Alteração de configurações de segurança	Módulo: BSP – Nível de auditoria: informações de configurações de segurança (criptografia ativa ou não, protocolo H460 ativo ou não)	1.1.FAU_GEN.1.1
<i>Reset</i> /alteração de senhas de login administrativo	Módulo: BSP – Nível de auditoria: informações (se alterações com sucesso), erro (se insucesso na alteração)	1.1.FAU_GEN.1.1
Ligação, desligamento e reinício do TOE	Data, hora e tipo do evento	1.2.FAU_GEN.1.2
Início, manutenção e encerramento da chamada	Data, hora e tipo do evento	1.2.FAU_GEN.1.2
<i>Login</i> e <i>logout</i> do console administrativo	Data, hora e tipo do evento	1.2.FAU_GEN.1.2
Alteração de configurações de segurança	Data, hora e tipo do evento	1.2.FAU_GEN.1.2
<i>Reset</i> /alteração de senhas de login administrativo	Data, hora e tipo do evento	1.2.FAU_GEN.1.2
Ligação, desligamento e reinício do TOE	É registrado o evento, porém o usuário administrativo é um único, já que inexistem usuários individuais	1.2.FAU_GEN.2
Início, manutenção e encerramento da chamada	É registrado o evento, porém o usuário administrativo é um único, já que inexistem usuários individuais	1.2.FAU_GEN.1.2
<i>Login</i> e <i>logout</i> do console administrativo	É registrado o evento, porém o usuário administrativo é um único, já que inexistem usuários individuais	1.2.FAU_GEN.1.2

Alteração de configurações de segurança	É registrado o evento, porém o usuário administrativo é um único, já que inexistem usuários individuais	1.2.FAU_GEN.1.2
<i>Reset</i> /alteração de senhas de <i>login</i> administrativo	É registrado o evento, porém o usuário administrativo é um único, já que inexistem usuários individuais	1.2.FAU_GEN.1.2
Criptografia ativa em suas comunicações	Sucesso/falha; modo de operação criptográfica	1.4.FCS_COP.1
Logar e deslogar do console administrativo	Módulo: <i>WEB</i> – Há registro de todas as tentativas sem sucesso de <i>logon</i> , porém não aparece a informação da quantidade de vezes nem tampouco as ações básicas a serem tomadas	1.5.FIA_AFL.1
	Não há definição de níveis de acesso para os usuários, ou seja, o acesso às configurações administrativas de segurança do TOE é realizado somente pelo usuário administrador	1.6.FIA_ATD.1
Resetar/alterar senhas de login administrativo	Apenas há rejeição pelo TSF quando a senha antiga, necessária para alterar para a nova senha, é informada errada. A única crítica feita é com relação ao número de caracteres mínimo, que deve ser 5. Inexiste métrica de qualidade adotada para o cadastro da senha.	1.7.FIA_SOS.1 1.8.FIA_SOS.2
Logar e deslogar do console administrativo	Há registro do insucesso de <i>login</i> no console administrativo, sendo que o TSF apenas permite que as ações no console sejam realizadas após o <i>login</i> no mesmo pelo administrador.	1.9.FIA_UAU.1
Alterar as configurações de segurança	Após o login administrativo, apenas as opções de alteração de senha de login exigem novo credenciamento pelo usuário.	1.10.FIA_UAU.2
	A senha utilizada na credencial de login é exibida através de sinais asterisco “*”, tantos quantos forem os caracteres digitados	1.11.FIA_UAU.3
	Ocorre o <i>single sign on</i> do usuário administrador	1.12.FIA_UAU.4
Alterar as configurações de segurança	O resultado final da autenticação do usuário administrador é registrado	1.13.FIA_UAU.5
Iniciar, manter e encerrar chamadas de videoconferência	O TOE registra <i>log</i> com informações de sucesso e falha do registro de autenticação no servidor <i>gatekeeper</i> , com data e	1.13.FIA_UAU.5

	hora; o log registra informações do TOE de tentativa de chamada, em chamada e de encerramento de chamada	
Alterar as configurações de segurança	O TOE registra as falhas na reautenticação dos usuários, além de todas as tentativas de reautenticação	1.14.FIA_UAU.6
	A única informação retornada ao usuário quando do seu <i>login</i> incorreto é “Erro de nome de utilizador ou palavra-passe”, conforme exposto na figura 16	1.15.FIA_UAU.7
	Há controle de login simultâneo de mais de um administrador ao console administrativo	1.16.FTA_MCS.1
Logar e deslogar do console administrativo	O TOE rejeita uma nova sessão decorrente da limitação de sessões múltiplas concorrentes, porém não ocorre a captura do número de sessões simultâneas do usuário administrador	1.17.FTA_MCS.2
	Está previsto no TSF travar a sessão interativa após 5 minutos de inatividade do usuário no console administrativo	1.18.FTA_SSL.1
Logar e deslogar do console administrativo	Não é possível o usuário travar a sua sessão, a não ser por inatividade, quando é deslogado do console, o que exige que ele logue novamente ao console para continuar sua sessão	1.19.FTA_SSL.2
Logar e deslogar do console administrativo	O TOE registra término de sessão do administrador pelo mecanismo de travamento	1.20.FTA_SSL.3
Logar e deslogar do console administrativo	O TOE registra término de sessão pelo usuário	1.21.FTA_SSL.4
Ligar, desligar e reiniciar o TOE	O <i>log</i> registra tais eventos	1.22.FPT_FLS.1
Iniciar, manter e encerrar chamadas de videoconferência		1.22.FPT_FLS.1
Alterar as configurações de segurança	Não há teste do servidor de horários. Após a inclusão de seus dados, o horário já é exibido automaticamente	1.23.FPT_TEE.1
Iniciar, manter e encerrar chamadas de videoconferência	Não há teste de registro no <i>gatekeeper</i> . Após a inclusão de suas informações, o TOE já realiza a tentativa de conexão ao mesmo	1.24.FPT_TEE.2
Iniciar, manter e encerrar chamadas de videoconferência	O TOE registra em seu log a ativação e a desativação do protocolo H.460	1.25.FTP_TRP.1

No apêndice A encontram-se as telas com as evidências coletadas no TOE.

5.1.1 Análise estatística dos dados

A tabela 1 relaciona os eventos pesquisados e a quantidade de suas respectivas ocorrências.

Os cinco eventos pesquisados estão dispostos nas colunas da tabela 1, enquanto que as observações realizadas estão dispostas nas linhas. Cada evento foi observado trinta vezes, permitindo a criação de série histórica, conforme as técnicas recomendadas de planejamento de experimentos (REIS, 2017) explicitadas no item anterior 4.5.

Quanto mais análises realizadas no conjunto de dados maior a probabilidade de os resultados terem alto índice de significância. Dessa forma, foram coletadas 30 (trinta) observações de cada um dos 5 (cinco) eventos, formando-se uma amostra de 150 (cento e cinquenta) elementos.

Foram observadas a ocorrência e a não-ocorrência dos eventos.

Tabela 1 – Eventos pesquisados e ocorrências

	Ligar, desligar e reiniciar o TOE	Iniciar, manter e encerrar chamadas de videoconferência	Logar e deslogar do console administrativo	Alterar as configurações de segurança	Resetar/alterar senhas de login administrativo
Ocorrência	30	30	30	30	30
Não-ocorrência	0	0	0	0	0

A fim de verificar se há relação entre os eventos observados foi utilizado o teste estatístico quiquadrado, em tabelas de contingência, com correção de *Yates*.

As hipóteses testadas foram:

a) Hipótese nula, H_0 : Não há associação entre os eventos, ou seja, as variáveis são independentes.

b) Hipótese alternativa, H_a : Há associação entre os grupos, ou seja, as variáveis são dependentes.

Os dados coletados na tabela 1 relacionam os eventos verificados nas observações. Para calcularmos os esperados multiplicamos os totais parciais relativos a cada casela, dividindo-se pelo total geral (N). Em seguida, calculam-se os quiquadrados parciais usando-se $(o-e)^2 / e$.

Após, a parcela de χ^2 de cada casela é calculada, conforme equação abaixo, somando-se ao final as parcelas e obtendo-se o χ^2 .

$$\chi^2 = \sum [(o - e)^2 / e]$$

Nota: o11 = observado da classe 1; e11 = esperado da classe 1...									
									Totais
o11 =	30	o12 =	30	o13 =	30	o14 =	30	o15 =	30
o21 =	0	o22 =	0	o23 =	0	o24 =	0	o25 =	0
Totais	30		30		30		30		30
Cálculo dos Esperados									
e11 =	30	e12 =	30	e13 =	30	e14 =	30	e15 =	30
e21 =	0	e22 =	0	e23 =	0	e24 =	0	e25 =	0
Cálculo dos Qui parciais									
(o11-e11) ² /e11	0,0000	(o12-e12) ² /e12	0,0000	(o13-e13) ² /e13	0,0000	(o14-e14) ² /e14	0,0000	(o15-e15) ² /e15	0,0000
(o21-e21) ² /e21	0,0000	(o22-e22) ² /e22	0,0000	(o23-e23) ² /e23	0,0000	(o24-e24) ² /e24	0,0000	(o25-e25) ² /e25	0,0000
Valor de Qui Quadrado =	0,0000								

Figura 14 – Teste Qui Quadrado sem correção

Como o número de grau de liberdade (GL) em tabelas 5 x 2 é GL= (5-1) x (2-1) = 4, com o auxílio da tabela quiquadrado vê-se que $\chi^2=9,488$. Já que o valor de QuiQuadrado calculado é menor que o crítico a hipótese H_0 é aceita, ou seja, os desvios são devidos ao acaso e não há associações entre os eventos.

Porém:

a) Há classes/eventos com frequências esperadas menores que 5.

Dessa forma, aplica-se a correção de Yates: $\chi^2 = \sum [(|o_n - e_n| - 0,5)^2 / e_n]$

Nota: o11 = observado da classe 1; e11 = esperado da classe 1...									
									Totais
o11 =	30	o12 =	30	o13 =	30	o14 =	30	o15 =	30
o21 =	0	o22 =	0	o23 =	0	o24 =	0	o25 =	0
Totais	30		30		30		30		30
Cálculo dos Esperados									
e11 =	30	e12 =	30	e13 =	30	e14 =	30	e15 =	30
e21 =	0	e22 =	0	e23 =	0	e24 =	0	e25 =	0
Cálculo dos Qui parciais com correção									
(o11-e11 -0,5): 0,0083		(o12-e12 -0,5): 0,0083		(o13-e13 -0,5): 0,0083		(o14-e14 -0,5): 0,0083		(o15-e15 -0,5): 0,0083	
(o21-e21 -0,5): 0,0000		(o22-e22 -0,5): 0,0000		(o23-e23 -0,5): 0,0000		(o24-e24 -0,5): 0,0000		(o25-e25 -0,5): 0,0000	
Valor de Qui Quadrado =			0,0417						

Figura 15 – Teste Qui Quadrado com correção de Yates

Agora, após ter sido aplicada a correção, $x^2 = 0,0417$, ou seja, x^2 continuou menor que x_c^2 , confirmando a aceitação da hipótese H_0 , ou seja, os desvios são devidos ao acaso e não há associações entre os eventos.

5.2 ANÁLISES E DISCUSSÕES

Analisando os resultados encontrados, verifica-se que o TOE atendeu à maioria dos requisitos foram atendidos: dos 25 requisitos levantados, apenas 8 não foram completamente atendidos. Ou seja, o PP teve 68% de aprovação nos seus parâmetros.

Os requisitos FAU_GEN.1.1 e FAU_GEN.1.2 foram atendidos parcialmente, enquanto que o parâmetro FAU_GEN.2 não foi atendido em sua totalidade, já que se verificou que inexistem usuários individuais para logar no console do TOE e efetuar as alterações em sua configuração. Há somente o usuário administrativo, que é único.

O parâmetro FIA_AFL.1 não foi atendido totalmente, pois ao logar e deslogar do console administrativo, não aparece a informação da quantidade de *logins* nem tampouco as ações básicas a serem tomadas.

O requisito FIA_ATD.1 não foi atendido por não existir definição de níveis de acesso para os usuários.

As condições FIA_SOS.1 e FIA_SOS.2 não foram atendidas, pois ao resetar/alterar senhas de login administrativo inexistem métrica de qualidade adotada para o cadastro da senha.

O parâmetro FIA_UAU.2 não foi atendido porque, ao alterar as configurações de segurança, apenas as opções de alteração de senha de login exigem novo credenciamento pelo usuário.

Com o apoio da análise estatístico do teste Quiquadrado constatou-se que não há relação entre os cinco eventos pesquisados: ligar, desligar e reiniciar o TOE; iniciar, manter e encerrar chamadas de videoconferência; logar e deslogar do console administrativo; alterar as configurações de segurança; resetar/alterar senhas de login administrativo.

Os seguintes princípios de segurança em sistemas de informação e comunicações, relacionados no item 2.4, foram atendidos nesta avaliação do TOE: integridade, disponibilidade, autenticidade e não-repúdio. A confidencialidade pode ser afetada, já que os requisitos não atendidos no TOE estão relacionados diretamente com a identificação, autorização e autenticação dos usuários.

6. CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS

O *protection profile* ora desenvolvido está em conformidade com os seguintes documentos e perfis:

- a) *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, September 2012, Part 1: Introduction and General Model, Part 2: Security Functional Components e Part 3: Security Assurance Components;*
- b) *Protection Profile for Network Devices (NDPP), Version 1.1, 08 June 2012;*
- c) *Security Requirements for Network Devices Errata, Version #3, 03 November 2014;*
- d) *Network Device Protection Profile Extended Package SIP Server (SIPEP), Version 1.1, 05 November 2014;*
- e) *Protection Profile for Voice Over IP (VoIP) Applications, Version 1.3, 03 November 2014.*

É importante destacar que o simples fato de se utilizar o *Common Criteria*, sem qualquer metodologia, ou com propriedades de segurança ou metodologias inapropriadas, poderia resultar em um sistema de certificação e homologação incorreto, sem qualquer funcionalidade. Nessa pesquisa a metodologia e os requisitos de segurança foram cuidadosamente determinados, descartando-se a possibilidade de resultar num sistema de certificação ineficiente. Os requisitos utilizados no PP desenvolvido neste trabalho foram relacionados considerando-se parâmetros de segurança definidos na POSIC da entidade da APF, diretamente elencados das necessidades deste grupo específico de usuários e das boas práticas de mercado.

Está fora do escopo do CC as situações que envolvem técnicas especializadas ou que estão em áreas periféricas da segurança em TI. Os critérios de segurança pertinentes aos procedimentos administrativos, por exemplo, não são relacionados diretamente com funcionalidades de segurança de TI. Aspectos técnicos como controle de emissão eletromagnética são um exemplo de técnicas especializadas que não são consideradas nessa avaliação.

O *protection profile* ora desenvolvido é passível de atualizações, à medida que as necessidades do grupo de usuários sofrerem alterações e que as boas práticas de mercado forem atualizadas.

A questão central estudada foi: o que deve conter em um perfil de proteção de homologação e certificação de equipamento de videoconferência, considerando as normas da Associação Brasileira de Normas Técnicas (ABNT) NBR 27001:2006 [ABNT, 2006], NBR 27002:2005 [ABNT, 2005], NBR 27005:2008 [ABNT, 2008], além das Normas Complementares 07 [DSIC/GSIPR, 2010a] e 17 [DSIC/GSIPR, 2013c] do Gabinete da Segurança Institucional da Presidência da República (GSIPR), e padrões internacionais como o *Common Criteria*? Verificou-se que o perfil de proteção elaborado nesta pesquisa relacionou requisitos de segurança conforme a necessidade do grupo de usuários considerado, que são os usuários finais do equipamento de videoconferência, entidade da APF em questão, conforme detalhado no item 4.2.2.

As perguntas acessórias à principal foram:

1) Quais são os critérios de segurança a serem considerados no modelo proposto?

Os critérios de segurança considerados no modelo proposto estão diretamente relacionados às necessidades do grupo de usuários considerado nesta pesquisa, ou seja, a administração pública federal. Os parâmetros estão relacionados no quadro 7.

2) É possível aplicar um modelo baseado no *Common Criteria* em um equipamento de vídeo conferência de uso comercial, em ambiente controlado?

O sistema de homologação e certificação utilizando o *Common Criteria* é altamente viável, com grandes possibilidades de avaliação e ponderação do produto mecatrônico no que diz respeito à segurança da informação e comunicações.

Conforme exposto neste trabalho, foi possível aplicar um modelo baseado no CC em um equipamento de uso comercial, em ambiente controlado.

Após levantados os requisitos de segurança, e dispostos conforme as famílias do sistema de avaliação *Common Criteria*, o TOE foi instalado em ambiente controlado, a fim de verificar os parâmetros elencados.

3) Os resultados da aplicação do modelo proposto a um caso real validam o PP desenvolvido?

Sim, os resultados da aplicação do modelo proposto a um caso real validam o perfil de proteção desenvolvido. Ao aplicar o PP a um equipamento de videoconferência real, utilizando parâmetros de segurança baseados na POSIC de uma entidade da APF, os resultados obtidos foram genuínos e autênticos, permitindo validar o perfil elaborado.

Os requisitos de segurança reunidos no PP ora desenvolvido foram elencados das melhores práticas de mercado e de normas complementares do GSI/PR, além de padrões internacionais de segurança. Tais requisitos são frequentemente usados nos editais de aquisição de equipamentos de videoconferência para a APF. É possível utilizá-lo para avaliar outros equipamentos de videoconferência, de diversos fabricantes, já que os requisitos de segurança relacionados neste perfil são comuns e genéricos aos equipamentos desta natureza.

O perfil elaborado neste trabalho relaciona-se com o PP de VoIP, citado no item e) dessa conclusão (*Protection Profile for Voice Over IP (VoIP) Applications, Version 1.3, 03 November 2014*) à medida que o TOE considerado no presente estudo apresenta funcionalidades semelhantes da solução tecnológica. Porém, o perfil de VoIP está diretamente relacionado à infraestrutura do serviço, enquanto que o PP desenvolvido nesta pesquisa reúne requisitos de segurança dos equipamentos de videoconferência que se utilizam da estrutura dos servidores de VoIP, exigindo particularidades em seu levantamento e verificação.

Desenvolver o sistema não é das tarefas mais simples, pois devem-se considerar sempre as necessidades de determinado grupo de usuários. As boas práticas de mercado podem não ser convenientes a específicos grupos de usuários em função da criticidade da segurança da informação dos dados envolvidos. Os desafios e a criticidade da segurança da informação para o grupo de usuários da APF certamente são distintos dos considerados pelas entidades privadas.

Aplicar o PP no TOE pode-se considerar uma atividade não tão trivial, pois as condições elencadas no perfil devem ser reproduzidas da mesma forma em que foram levantadas, o que nem sempre pode ser possível em função de eventuais dificuldades na reprodução do ambiente operacional dos sistemas computacionais envolvidos.

Consultando a lista de produtos avaliados em relação ao CC, no Portal *Common Criteria* na web (www.commoncriteriaportal.org), verifica-se o número reduzido de produtos avaliados com níveis de garantia de segurança mais elevados EAL6 e EAL7 (BROWN, STALLINGS;

2014). Certamente isso se deve aos requisitos exigidos nesses níveis, que limitam o tipo e a complexidade de produtos que podem ser avaliados em relação a eles.

As funções mecânicas do TOE não foram alvo de avaliação nesse trabalho. Apenas funções de software foram relacionadas no perfil. Haveria diferenciação se as primeiras fossem avaliadas, já que as questões referentes à mecânica do TOE dizem respeito diretamente ao funcionamento mecânico e eletrônico dos elementos constituintes do produto, sendo que sua implementação reflete em mudanças significativas quanto à segurança da informação.

Por exemplo, o posicionamento correto do motor que posiciona a câmera pode afetar ou ser afetado, prejudicando o funcionamento correto da câmera e causando eventual perda de privacidade, além do vazamento de informações da sala. Com o microfone do equipamento pode ocorrer situação semelhante: caso o elemento atue de forma indevida, o áudio da reunião pode ser captado de forma clandestina, ocasionando falha de segurança.

Para o requisito "criptografia ativa", foi-se considerado o uso de criptografia em todas as comunicações, ou seja, não foram aprofundados aspectos como: se chave assimétrica ou simétrica; algoritmos e sistemas criptográficos usados. Futuras atualizações do perfil desenvolvido neste trabalho podem incluir tais aspectos nas implementações dos testes de requisitos.

Segundo o CC, o EAL (*Evaluation Assurance Level* – Nível de Garantia de Avaliação) deste perfil é considerado 3, pois a avaliação atinge os requisitos de segurança contemplados neste *package*.

O TOE foi estruturalmente testado, conforme EAL 3, envolvendo análise de sua documentação além dos testes funcionais metodologicamente realizados. Dessa forma, nível moderado de garantia de segurança foi investigado minuciosamente no TOE, considerando diversas premissas de segurança do ambiente onde o TOE está inserido, segundo a POSIC das entidades da APF, dispensando reengenharia significativa do objeto avaliado. Seria importante elevar esse nível para EAL4 até 7, pois assim mais parâmetros e requisitos de segurança seriam testados.

Percebeu-se a grande importância do tema defesa cibernética na solução tecnológica comunicações unificadas, considerando que informações sensíveis podem trafegar em

videoconferências, *webchats* e audioconferência. É extremamente vital que tal solução tecnológica seja analisada no campo de segurança cibernética.

Nos Estados Unidos verifica-se a existência de laboratórios certificadores do CC. A *National Security Agency* (NSA) têm desenvolvido vários perfis de proteção, muitos deles em conjunto com o *National Institute of Standards and Technology* (NIST) (MEAD, 2013). Há um grupo de trabalho chamado *Protection Profile Review Board* (PPRB), voltado especificamente para revisar todos os PPs propostos e trabalhar junto com os autores visando maior consistência dos perfis.

A maturidade do CC e a consciência dos gestores norte-americanos e europeus têm levado as instituições nos Estados Unidos (EUA) e na Europa (LISI, 2013) a considerar essa importante avaliação de requisitos de segurança em seus produtos, principalmente em sistemas considerados como infraestrutura crítica (links de comunicação de dados em sistemas de aviação, comunicação via satélite).

Um exemplo disso é o estudo de caso da FAA Telecom (HERRMANN, KEITH; 2001), nos EUA. Neste estudo, o projeto de Infraestrutura de Telecomunicações da *Federal Aviation Administration* (FTI/FAA) fornece como exemplo um contrato de serviços que usa o CC. A FTI fornece serviços integrados de telecomunicações de voz, dados e vídeo no continente americano, com conectividade com os territórios do Havaí e do Alasca. Os requisitos do FTI são expressos em termos de classes de serviço e interfaces de serviço. Neste caso específico, o fornecedor é obrigado a demonstrar o nível EAL3 (MEAD, 2013).

Aguarda-se, porém, que os usuários finais da solução e os gestores do serviço nas entidades reconheçam a importância da conscientização sobre a política de defesa cibernética no produto mecatrônico, e a apliquem em seu cotidiano. O presente trabalho apresenta 68% de aprovação aos parâmetros do PP, ou seja, muitos requisitos não estão atendidos no TOE, necessitando de implementação.

Existem normas brasileiras de segurança de TIC, inclusive voltadas especificamente à APF, definidas em função da criticidade dos elementos envolvidos, orientando sobre a importância de certificar e homologar soluções de TI.

Se há regulamentação clara e precisa sobre segurança da informação e comunicações (SIC) é possível definir-se um modelo nacional de certificação e homologação de produto de

defesa cibernética. A pesquisa realizada neste trabalho serve para direcionar esse tipo de desenvolvimento.

Internacionalmente, podem-se observar vários padrões e recomendações de melhores práticas no campo da defesa cibernética.

Similar ao presente trabalho, Silva (2014) utilizou-se de uma metodologia multicritério de apoio à decisão (MMAD) para avaliar o serviço de e-mail (*cloud* e *in house*), tendo seus critérios avaliados por especialistas de segurança após serem elencados.

Utilizando várias ferramentas, Amaral et al (2008) avaliou riscos de segurança da informação através das ferramentas Seis Sigma, Ciclo de Melhoria DMAIC (Definir, Medir, Analisar, Implementar e Controlar) e FMEA.

Os trabalhos dos seguintes pesquisadores utilizaram-se basicamente das boas práticas aliadas às normas internacionais de segurança: Santos e Filho (2013); Eloff e Solms (2008); Fontoura, Konzen e Nunes (2012); Martins e Santos (2005); Trček (2003); Farn *et al* (2003); Sipponen e Willison (2009); Tashi e Outi-Hélie (2008); Broderick (2006); Kadobayashi e Takahashi (2015); Disso *et al* (2015).

Coelho e Silva (2013), além de aplicarem as boas práticas e as normas de segurança, criaram ontologia e metodologia próprias para certificação de um computador desktop.

A presente pesquisa apresenta relação com os trabalhos apresentados por Akalp *et al* (2011), Hou e Yu (2012) e Fernandez-Saavedra et al (2013). Os primeiros aliaram análise estatística em seus critérios, comparando sistemas de gestão de SI de diversas empresas. Os dois últimos usaram CC em suas análises, porém Hou e Yu (2012) formularam um *framework* de sua avaliação de segurança, enquanto que os últimos analisaram um sistema biométrico.

Há também várias instruções normativas norteadoras de aquisição de produtos voltadas aos profissionais da área de SIC.

Apesar da grande diversidade de produtos mecatrônicos, a usabilidade desse sistema de certificação e homologação, ora proposto, ao produto mecatrônico de comunicações unificadas pode ser considerada satisfatória, considerando-se a especificidade do produto mecatrônico.

Como trabalhos futuros pode-se considerar a avaliação da infraestrutura central da solução de videoconferência utilizando-se desse sistema proposto, considerando que os componentes dessa infraestrutura são os servidores responsáveis pelo controle, estabelecimento, configuração e armazenamento dos dados que trafegam pelos equipamentos de videoconferência. É possível realizar análises separadas, abordando requisitos específicos relacionados à segurança da informação nos servidores.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - Associação Brasileira de Normas Técnicas. NBR 27002:2005- Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. 2a. ed. Rio de Janeiro: ABNT, 2005.

_____. NBR 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. 1a. ed. Rio de Janeiro: ABNT, 2006.

_____. NBR 15999-1:2007 – Gestão de Continuidade de Negócios – Código de Prática. Rio de Janeiro: ABNT, 2007.

_____. Gestão de continuidade de negócios: Parte 1 - Código de Prática: ABNT NBR 15999-1:2007. Errata 1, de 01.02.2008. Rio de Janeiro: ABNT, 2008.

_____. NBR 15999-2: Gestão de continuidade de negócios – Parte 2: Requisitos. Rio de Janeiro: ABNT, 2008a.

_____. NBR 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação. 1a. ed. Rio de Janeiro: ABNT, 2008b.

AKALP, G.; AYTAC, S.; BAYRAM, N.; YILDIRIM, E. Y. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, Elsevier, n. 31, p. 360–365, 2011.

AMARAL, E. M. H.; NUNES, R. C.; OLIVEIRA, M. A. F.; PEREIRA, S. N. ; ZEN, E. Uma metodologia de gestão de segurança da informação direcionada a riscos baseado na abordagem Seis Sigma. In ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO, 22, 2008, Rio de Janeiro. Anais... Rio de Janeiro: 2008.

AV-iQ. Disponível em < <http://www.av-iq.com/avcat/ctl1642/index.cfm?manufacturer=huawei-enterprise-usa&product=te40-720p30-w-p-02>>. Acesso em Jul.2017.

BARBALHO, S.C.M. Modelo de referência para o desenvolvimento de produtos mecatrônicos: conceitos e aplicações. 1ª ed.: Ed. Novas Edições Acadêmicas, 2016.

- BEIGUELMAN, B. Curso prático de Bioestatística. 4^a ed. rev. Ribeirão Preto/SP: Sociedade Brasileira de Genética, 1996.
- BLANCO, C.; LASHERAS, J.; FERNÁNDEZ-MEDINA, E.; TOVAL, A.; VALENCIA-GARCÍA, R. Basis for an integrated security ontology according to a systematic review of existing proposals. *Computer Standards & Interfaces*, n. 33, p. 372–388, 2011.
- BRASIL. MINISTÉRIO DA DEFESA. Estudo de Viabilidade do SHCDCiber no Âmbito do Projeto EnaDCiber-SHCDCiber@DCDN. Brasília: UnB, 2015a.
- _____. MINISTÉRIO DA DEFESA, EXÉRCITO BRASILEIRO. 2015b. Disponível em <<http://www.epex.eb.mil.br/index.php/projetos/defesa-cibernetica.html>>. Acesso em Dez. 2015.
- _____. MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA E COMÉRCIO EXTERIOR – MDIC. 2015c. Disponível em: <<http://www.desenvolvimento.gov.br/sitio/interna/interna.php?area=5&menu=567>>. Acesso em 27 Jul. 2015.
- _____. MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. Edital Pregão Eletrônico para Registro de Preços nº 03/2015. 2015d. Disponível em: <<http://www.planejamento.gov.br/aceso-a-informacao/licitacoes-e-contratos/licitacoes/preg>>. Acesso em Out. 2016.
- _____. MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO - MPOG. E-PING Padrões de Interoperabilidade de Governo Eletrônico – Documento Referência. Brasília, DF, 2015e. Disponível em: <<http://eping.governoeletronico.gov.br>>. Acesso em 27 Out. 2016.
- _____. MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO - MPOG. Portaria Interministerial nº 141. Dispõe sobre comunicação de dados e serviços de tecnologia da informação. *Diário Oficial da União*, Brasília, DF, 5 mai. 2014. Seção 1, p. 83.
- BRODERICK, J. S. ISMS, security standards and security regulations. *Information Security Technical Report*, Elsevier, n. 2, p. 26–31, 2006.

- BROWN, L.; STALLINGS, W. Segurança de computadores: Princípios e Práticas. 2ª ed.; Editora Campus/Elsevier, 2014.
- BUUR, J.; ANDREASEN, M. M. A theoretical Approach to Mechatronics Design. Kgs. Lyngby, Denmark: Technical University of Denmark (DTU), 1990.
- CBSI – COMUNIDADE BRASILEIRA DE SISTEMAS DE INFORMAÇÃO. Disponível em <http://www.cbsi.net.br/2014/12/guerra-cibernetica-eua-x-coreia-do.html#.Vm3W5L_26r4>. Acesso em Dez. 2014.
- CISCO, Systems Inc. Cisco Unified Communications Manager Security Target. Version 1.0. San Jose, CA, Estados Unidos. Disponível em:<https://www.commoncriteriaportal.org/files/.../st_vid10646-st.pdf>. Acesso em Set. 2016.
- COELHO, M. P.; SILVA, R. M. Trustiness Certification of Information Technology Equipment. IJCSNS International Journal of Computer Science and Network Security, v.13, n. 12, 2013.
- COLITEC Áudio Vídeo e Informática. Disponível em < <http://www.colitec.com.br/o-que-e-macatronica.htm>>. Acesso em 17 Dez. 2015.
- COMMON CRITERIA. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4; 2012a.
- COMMON CRITERIA. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4; 2012b.
- COMMON CRITERIA. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4; 2012c.
- CONTI, F. Biometria – Qui quadrado. Belém/PA: 2011. Disponível em: < <http://ufpa.br/dicas/biome/bioqui.htm>>. Acesso em 15 Jul. 2017.
- DE SILVA, C.W.; BEHBAHANI S. A design paradigm for mechatronic systems. Mechatronics Journal, Elsevier, Volume 23, Issue 8, p.960 - 966, dez. 2012. Disponível em: < <http://dx.doi.org/10.1016/>>. Acesso em 03 Dez. 2015.

- DIAS, T. V. A. C. Codificação de Vídeo em H.264. In XIV Seminário de Iniciação Científica da PUC-Rio. Departamento de Engenharia Elétrica, Pontifícia Universidade Católica – PUC, 2006, Rio de Janeiro. Anais... Rio de Janeiro: 2006.
- DISSO, J. F. P.; JONES, K.; HUTCHISON, D.; PRINCE D. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, Elsevier, n. 9, p. 52–80, 2015.
- DLAMINI, M. T.; ELOFF, J. H. P.; ELOFF, M. M. Information security: The moving target. *Computers & Security*, Elsevier, n. 28, p. 189-198, 2009.
- D'ORNELLAS, M. C.; KROLL, K. O gerenciamento estratégico da segurança da informação. In *Simpósio Brasileiro de Pesquisa Operacional. - Pesquisa Operacional na Gestão do Conhecimento*, 61, 2009, Bahia. Anais... Porto Seguro: 2009.
- DSIC/GSIPR - Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República. Norma Complementar 07/IN01/DSIC/GSIPR - Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações; nos órgãos e entidades da Administração Pública Federal; direta e indireta – APF [Internet]. Jun 10; 2010a. Disponível em: <<http://dsic.planalto.gov.br>> Acesso em 03 Mar. 2015.
- _____. Norma Complementar 17/IN01/DSIC/GSIPR - Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF) [Internet]. Oct 4; 2013c. Disponível em: <<http://dsic.planalto.gov.br>> Acesso em 03 Mar. 2015.
- ELOFF, M. M.; SOLMS, S. H. Information security management: an approach to combine process certification and product evaluation. *Computers & Security*, Elsevier Science, n. 19, p. 698-709, 2000.
- FARN, K.; FUNG, A. R. ; LIN, A. C. Paper: a study on the certification of the information security management systems. *Computer Standards & Interfaces*, Elsevier, n. 25, p. 447–461, 2003.

- FERNANDEZ-SAAVEDRA, B.; LIU-JIMENEZ, J.; MIGUEL-HURTADO, O; SANCHEZ-REILLO, R. Evaluation of biometric system performance in the context of Common Criteria. *Information Sciences*, Elsevier, n. 245, p. 240–254, 2013.
- FILHO, R. B.; SANTOS, V. O. Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008. *Revista Telecomunicações*, v. 15, n. 1, 2013.
- FONTES, E. *Praticando a segurança da informação*. Rio de Janeiro: Brasport, 2008.
- FONTOURA, L. M.; KONZEN, M. P.; NUNES, R. C. Gestão de riscos de segurança da informação baseada na norma ISO/IEC 27005 usando padrões de segurança. In *SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA – SEGET*, 9, 2012, Rio de Janeiro. Anais... Resende: 2012.
- GIL, A. C. *Métodos e técnicas de pesquisa social*. São Paulo, Brasil: Atlas, 1999.
- HERRMANN, D.; KEITH, S. Application of Common Criteria to Telecom Services: A Case Study. 21-28. *Computer Security Journal*. XVII. 2. Spring, p. 21-28, 2001. Disponível em <
https://www.researchgate.net/publication/248543258_Application_of_Common_Criteria_to_Telecomm_Services_A_Case_Study>. Acesso em Nov. 2017.
- ITU – International Telecommunication Union. *Data communication networks: Open Systems Interconnection (OSI); Security, structure and applications. Security architecture for open systems interconnection for CCITT applications. Recommendation X.800*. Geneva: ITU, 1991. Disponível em: <<http://www.itu.int/rec/T-REC-X.800-199103-I>>. Acesso em 30 Jul. 16.
- JUNIOR, C.C. *Sistemas Integrados de Gestão – ERP: Uma abordagem gerencial*. 4. ed. Curitiba: Ibpex, 2011.
- JUNIOR, S.C.C. *A Segurança e Defesa Cibernética no Brasil e Uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual*. Brasília/DF: IPEA, 2013.
- KADOBAYASHI, Y.; TAKAHASHI, T. Reference Ontology for Cybersecurity. *Operational Information*. publication on 8 October 2014. The British Computer Society. Section D:

- Security in Computer Systems and Networks. *The Computer Journal*, v. 58, n. 10, 2015, pp 2297-2392. Disponível em < <https://doi.org/10.1093/comjnl/bxu101> >. Acesso em Abr. 2016.
- LISI, M. Security in Large, Strategic and Complex Systems. Università degli Studi CampusBio-Medico di Roma. 2013. Disponível em < <https://www.slideshare.net/MarcoLisi/homeland-security2013-lisivo3>>. Acesso em Nov. 17.
- MARTINS, A. B.; SANTOS, C. A. S. A Methodology to Implement an Information Security Management System. *Journal of Information Systems and Technology Management*, v. 2, n. 2, 2005, pp. 121-136. Disponível em < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752005000200002>. Acesso em Set. 2016.
- MEAD, NANCY. The Common Criteria. Carnegie Mellon University. 2013. Disponível em < <https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria>>. Acesso em Nov. 2017.
- MORAES, A. F. de. Segurança em Redes: Fundamentos. 1. ed. São Paulo: Érica, 2010.
- NETO, B.B.; SCARMINIO, I. S.; BRUNS, R. E. Como fazer experimentos: Pesquisa e desenvolvimento na ciência e na indústria. 4.ed. Porto Alegre/RS: Bookman, 2010.
- OHTOSHI, P. H. Análise Comparativa de Metodologias de Gestão e de Análise de Riscos Sobre a Ótica da Norma ABNT NBR ISO/IEC 27005. Brasília: Universidade de Brasília – UnB – Instituto de Ciências Exatas – Departamento de Ciência da Computação, 2008.
- PADILHA, L. Defesa cibernética. Notícias EPEX. Disponível em: <<http://www.epex.eb.mil.br/index.php/projetos/defesacibernetica.html>>. Acesso em 13 Dez. 2015.
- REIS, M. M. Conceitos Elementares de Estatística. Universidade Federal de Santa Catarina. Disponível em: < <http://www.inf.ufsc.br/~marcelo.menezes.reis/intro.html>>. Acesso em 04 Jul. 2017.

- SILVA, M. J. C. F. T. Avaliação da Segurança de Sistemas de Informação usando uma abordagem multicritério. Lisboa, Portugal: Técnico Lisboa – Engenharia Informática e de Computadores, 2014.
- SIPONEN, M; WILLISON, R. Information Security Management Standards: Problems and Solutions. Journal Information and Management, Elsevier, v. 46, n. 5, pp 267-270, 2009. Disponível em: < doi>10.1016/j.im.2008.12.007 >. Acesso em Set. 2016.
- STALLINGS, W. Network Security Essentials: Applications and Standards. 2. ed. New Jersey: Prentice Hall, 2003.
- TANENBAUM, A. S.; WETHERALL, D. Redes de computadores.5. ed. São Paulo/SP: Pearson Prentice Hall, 2011.
- TASHI, I. ; OUTI-HÉLIE, S. G. Efficient Security Measurements and Metrics for Risk Assessment. Internet Monitoring and Protection, International Conference on, Computer & Society, IEEE, v. 0, n. , pp 131-138, 2008. Disponível em < http://doi.ieeecomputersociety.org/10.1109/ICIMP.2008.34>. Acesso em Set. 2016.
- TRČEK, D. An Integral Framework for Information Systems Security Management. Computers & Security, Elsevier, v. 22, n. 4, pp 337-360, 2003. Disponível em: < http://www.isy.vcu.edu/~gdhillon/Old2/teaching/Spring07-VCU-790-GlobalConseq/temp/An%20integral%20framework%20for%20information%20systems%20security%20management.pdf>. Acesso em Set. 2016.
- VIALI, L. Testes de hipóteses não paramétricos. Apostila. Instituto de Matemática. Departamento de Estatística. UFRGS – Universidade Federal do Rio Grande do Sul. Porto Alegre/RS: 2008.
- WHEELER, D. A. Secure Programming HOWTO – Versão 3.72, 2015-09-19. Disponível em: <http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/requirements.html>. Acesso em 26 Jul. 2016.
- WORLD ECONOMIC FORUM - WEF, News Release. Disponível em: <http://www3.weforum.org/docs/Media/PT_GITR15_Final.pdf>. Acesso em 03 Ago. 2015.

YU, YC.; HOU, TW. Utilize Common Criteria Methodology for Secure Ubiquitous Healthcare Environment. *Journal of Medical Systems*, Springer US, v. 36, n. 3, pp 1689-1696, 2012. Disponível em: < <https://doi.org/10.1007/s10916-010-9629-2>>. Acesso em Set. 2016.

APÊNDICES

APÊNDICE A

Seguem abaixo as telas das evidências coletadas no TOE, quando da realização da validação do perfil ora levantado.



Figura 16 – Vista frontal do TOE



Figura 17 – Instalação básica do TOE



Figura 18 – Login no console administrativo remoto



Figura 19 – Resposta de retorno ao inserir credenciais erradas de login no TOE

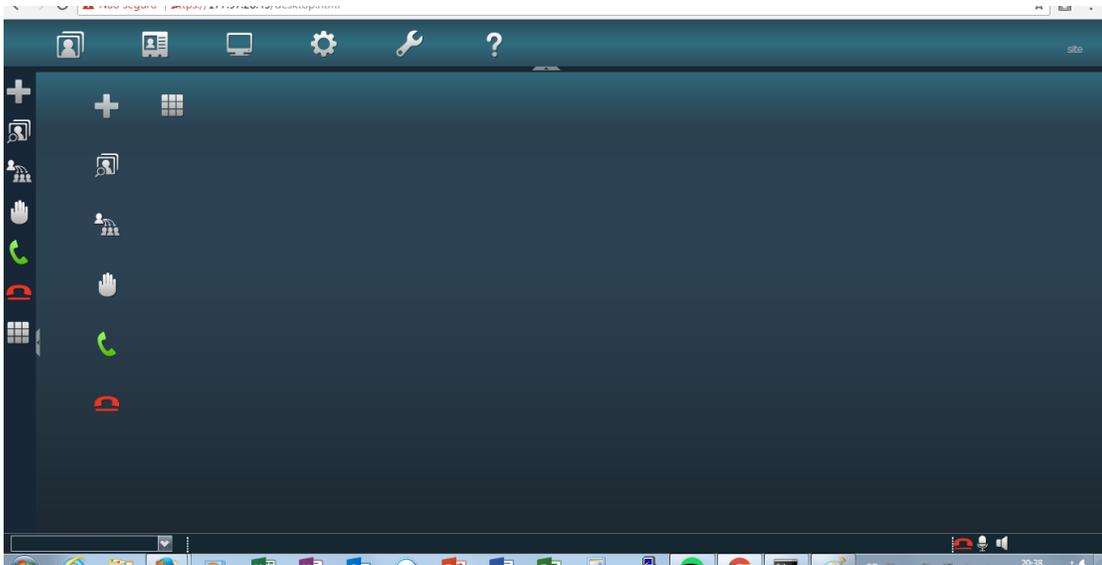


Figura 20 – Tela do console administrativo remoto após efetuar login com credenciais corretas no TOE

```

log (1) - Bloco de notas
Arquivo  Editar  Formatar  Exibir  Ajuda
<?xml version="1.0" encoding="UTF-8"?><LogModule>[System][Info] 2017-06-21 17:24:41 LOG_MOD_BSP 1 web string:system trig event: key
[System][Info] 2017-06-21 17:24:42 LOG_MOD_BSP 2 web string:system trig event: key
[System][Info] 2017-06-21 17:24:43 LOG_MOD_BSP 4 web string:system trig event: key
[System][Info] 2017-06-21 17:25:16 LOG_MOD_MC 6 web string:ipv4 static access succ.
[System][Info] 2017-06-21 17:25:17 LOG_MOD_BSP 101 web string:Create a type of IP message to LCD buffer. The first: IP, the second: 192.168.1.1
[System][Info] 2017-06-21 17:25:19 LOG_MOD_BSP 111 web string:Power on the terminal successful
[System][Info] 2017-06-21 17:25:30 LOG_MOD_MC 143 web string:license: parse succ.
[System][Info] 2017-06-21 17:25:33 LOG_MOD_BSP 162 web string:system exit event: aux_video_in
[System][Info] 2017-06-21 17:27:37 LOG_MOD_AUDIO 168 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 17:28:50 LOG_MOD_AUDIO 169 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 17:29:30 LOG_MOD_AUDIO 170 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 17:29:32 LOG_MOD_AUDIO 171 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 17:32:24 LOG_MOD_AUDIO 172 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 17:33:57 LOG_MOD_MC 204 web string:ipv4 dynamic access succ.
[System][Info] 2017-06-21 17:36:51 LOG_MOD_BSP 240 web string:Create a type of IP message to LCD buffer. The first: IP, the second: 192.168.15.8
[System][Info] 2017-06-21 17:36:51 LOG_MOD_MC 242 web string:ipv4 static access succ.
[System][Info] 2017-06-21 17:40:52 LOG_MOD_AUDIO 267 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 17:41:39 LOG_MOD_AUDIO 268 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 17:44:43 LOG_MOD_AUDIO 269 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 17:47:03 LOG_MOD_AUDIO 303 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 17:47:03 LOG_MOD_AUDIO 304 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 17:47:26 LOG_MOD_AUDIO 306 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 17:48:09 LOG_MOD_BSP 392 web string:system trig event: web
[System][Info] 2017-06-21 17:48:15 LOG_MOD_BSP 394 web string:system enter event: web
[System][Info] 2017-06-21 17:51:12 LOG_MOD_AUDIO 398 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 17:52:48 LOG_MOD_AUDIO 399 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 17:55:28 LOG_MOD_AUDIO 400 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 18:09:21 LOG_MOD_BSP 458 web string:system exit event: web
[System][Info] 2017-06-21 18:13:40 LOG_MOD_BSP 460 web string:system trig event: web
[System][Info] 2017-06-21 18:13:49 LOG_MOD_BSP 462 web string:system enter event: web
[System][Info] 2017-06-21 18:16:20 LOG_MOD_AUDIO 463 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 18:18:25 LOG_MOD_BSP 467 web string:system exit event: web
[System][Info] 2017-06-21 18:18:37 LOG_MOD_AUDIO 468 web string:mic array disconnected. Device ID[1].
[System][Info] 2017-06-21 18:28:25 LOG_MOD_BSP 515 web string:terminal enter sleep mode success
[System][Info] 2017-06-21 18:46:54 LOG_MOD_BSP 538 web string:system trig event: web
[System][Info] 2017-06-21 18:46:54 LOG_MOD_BSP 539 web string:terminal exit sleep mode success
[System][Info] 2017-06-21 18:46:58 LOG_MOD_BSP 542 web string:system enter event: web
[System][Info] 2017-06-21 18:55:33 LOG_MOD_AUDIO 556 web string:mic array disconnected. Device ID[0].
[System][Info] 2017-06-21 18:55:33 LOG_MOD_AUDIO 557 web string:mic array disconnected. Device ID[1].
  
```

Figura 21 – Log contendo registros de ligar o TOE (linha 6), configuração de informações de segurança (endereço IP - linhas 4, 5, 14 à 17), login e logout no console administrativo (linhas 24, 25, 29 a 31)

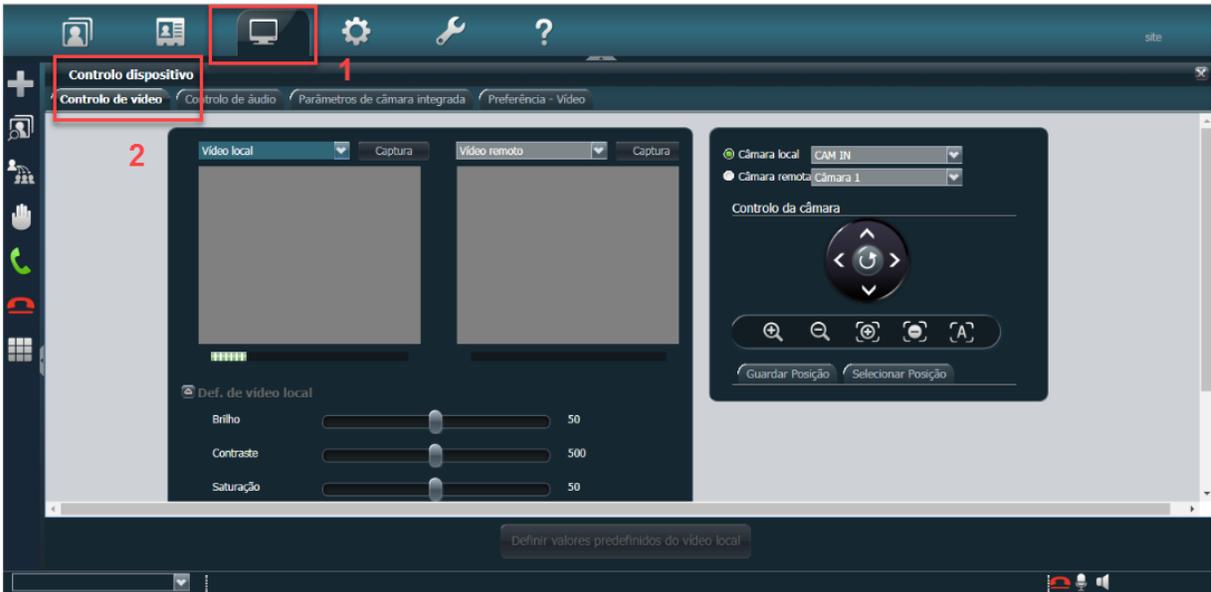


Figura 22 – Controle de vídeo console administrativo do TOE



Figura 23 – Alterações das configurações de segurança: criptografia e alteração da palavra-passe.

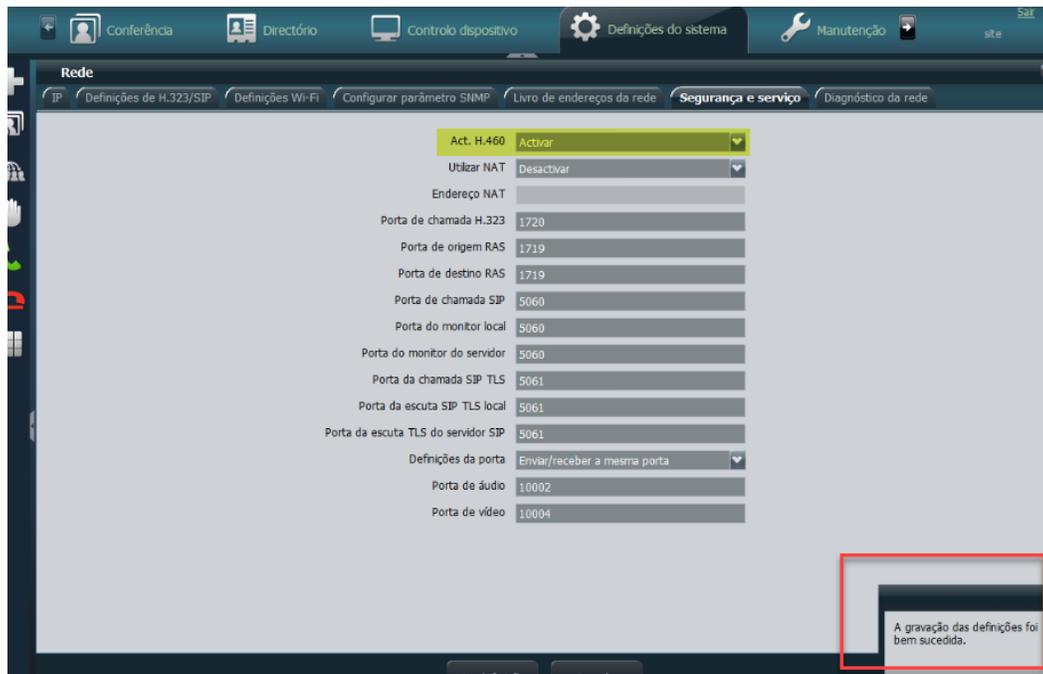


Figura 24 – Alterações da configuração de segurança uso do protocolo H.460.

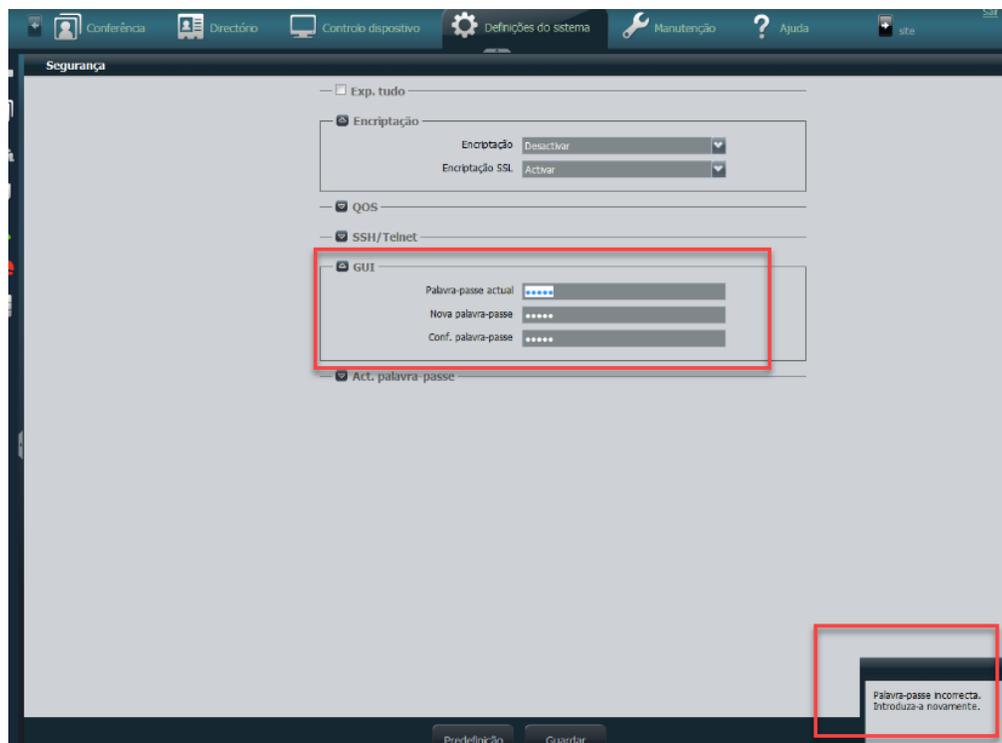


Figura 25 – Tentativa de alteração de palavra-passe com senha atual incorreta.

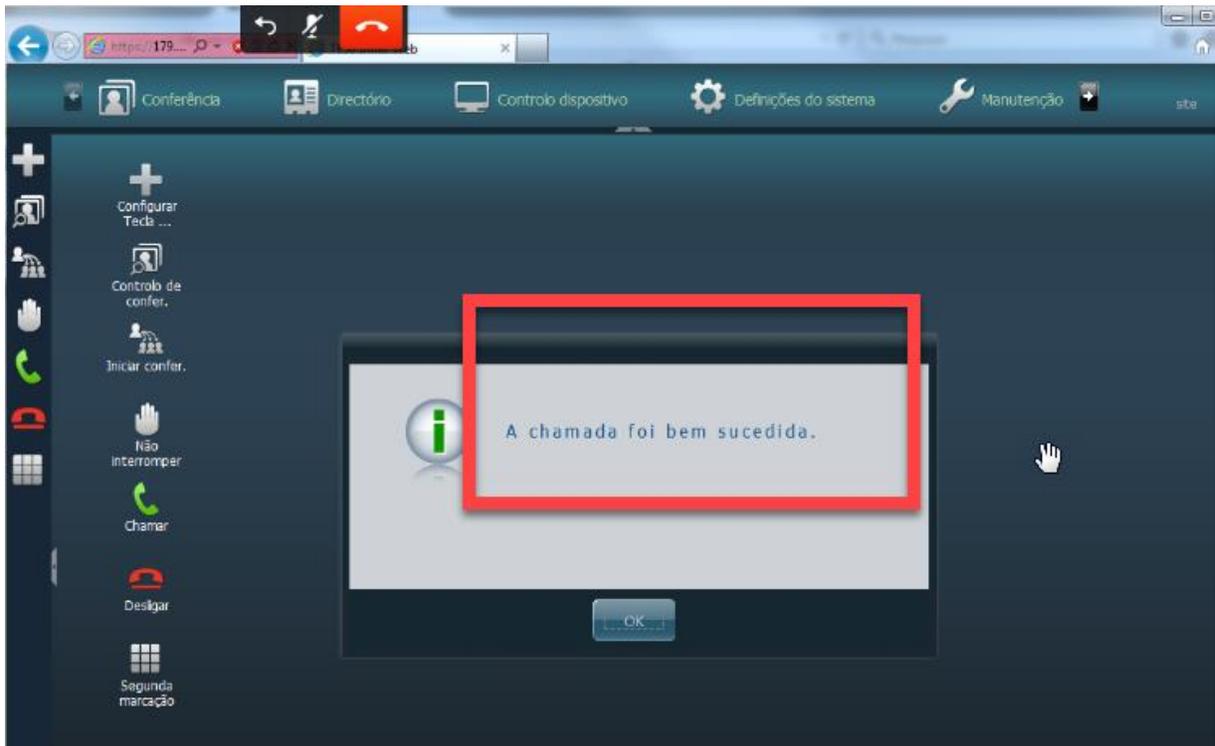


Figura 26 – Registro de chamada com criptografia ativa no TOE.

The image displays a call log interface for a conference titled '391302 Teste roteiro'. It includes a 'Time Left: 106 min' indicator and a 'Connect requested: 179.95.24.109' status. Below this, there are fields for 'Start Time', 'End Time', 'Owner', and 'Locked'. A small video thumbnail shows a participant in a striped shirt. The main part of the interface is a table with columns for 'Participants', 'Event Log', and 'Graphical View'. The table lists participants with their names, status, video and audio settings, and connection details. A red rectangular box highlights the 'Details' column for the participant '179.95.24.109', which shows 'Auto' for video and '4096 kbps' for audio. A mouse cursor is visible over the table.

Name	Status	Video	Audio	Details	Connection	Number	Remote
179.95.24.109	Calling			Auto	IP	179.95.24.109	videoconfmcu1b15
511195775@172.24.11.28	Connected	H264	G722	4096 kbps	H.323	43021	videoconfmcu1b15
IP Video Dial In	Idle			Auto	H.323	43021	videoconfmcu1b15

Figura 27 – Registro de chamada com criptografia ativa.

	Enviado	Recabido
Largura banda chamada	3,840k	3,840k
Protocolo de vídeo	H264 BP CIF	H264 BP 4CIF
Largura banda vídeo [vel. fotografamas]	2,000.00k[30]	1,952.00k[30]
Protocolo de áudio	G.7221c	G.7221c
Largura banda áudio	32.00k	48.00k
Protocolo da apresentação	--	--
Largura banda apresentação [vel. Fotografamas]	--	--
Número remoto	170.66.3.21	
Encriptação H.235	Encriptado	Encriptado

Figura 28 – Registro da criptografia ativa no TOE

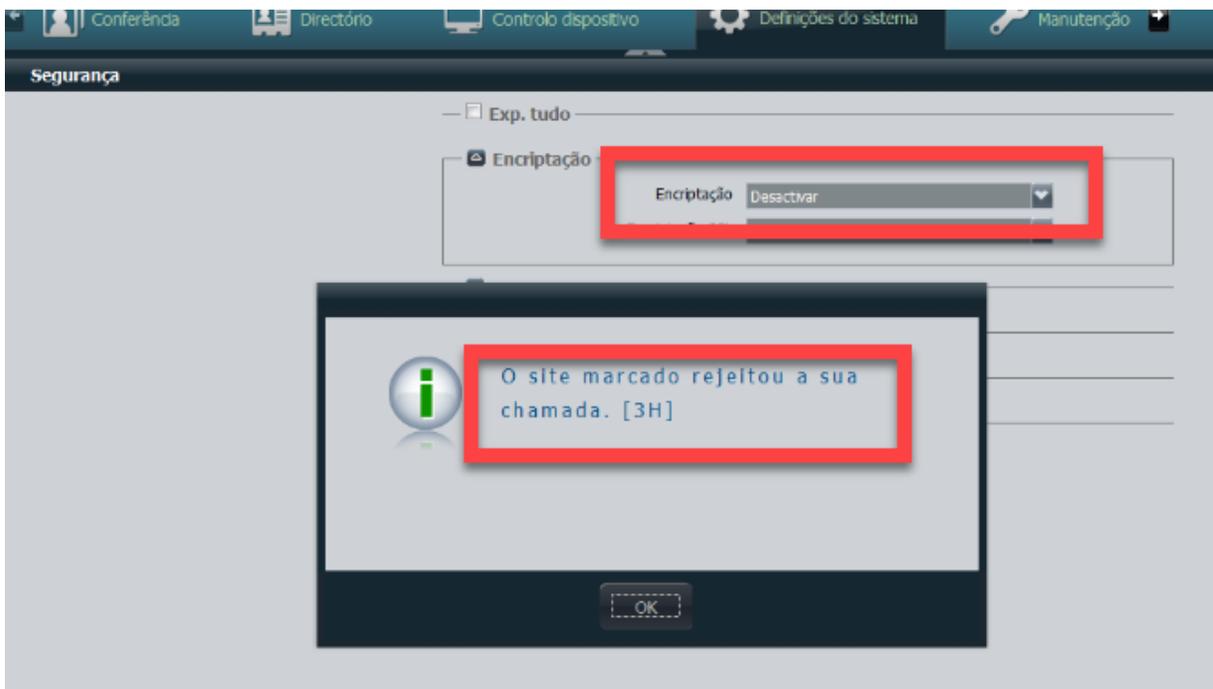


Figura 29 – Recusa da chamada sem criptografia ativa no TOE

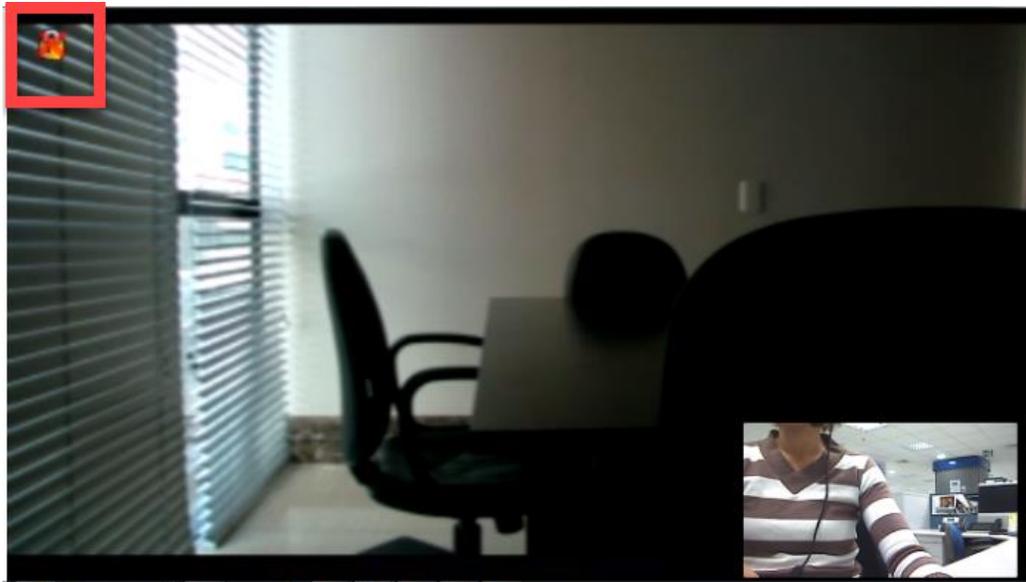


Figura 30 – Chamada concluída com sucesso com a criptografia desativada no destino (TOE) e na origem da chamada (*Jabber*)

Estado do sistema

Estado da linha Estado da chamada **Parâmetros da confer.** Est. interferência entrada

	Enviado	Recebido
Largura banda chamada	3,840k	3,840k
Protocolo de vídeo	H264 BP CIF	H264 BP 4CIF
Largura banda vídeo [vel. fotogramas]	2,000.00k[30]	1,952.00k[30]
Protocolo de áudio	G.7221c	G.7221c
Largura banda áudio	32.00k	48.00k
Protocolo da apresentação	--	--
Largura banda apresentação [vel. Fotogramas]	--	--
Número remoto	170.66.3.21	
Encriptação H.235	Desencriptado	Desencriptado
Número de conferência p/ acesso de vídeo	--	
Número de conferência p/ acesso de áudio	--	
Número de relé RDIS	--	
Número de conferência p/ acesso RDIS	--	
Palavra-passe para autenticação de conferência	--	

Figura 31 – Informações no TOE da chamada concluída com sucesso com a criptografia desativada no destino (TOE) e na origem da chamada (*Jabber*)

APÊNDICE B

Segue parte do registro dos eventos no log, capturado no TOE. Foi suprimida a exibição de grande parte de seus registros, considerando que o log possui mais de 1000 linhas de informações.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<LogModule>
```

```
[System][Info] 2017-06-21 17:24:41 LOG_MOD_BSP 1 Web string:System trig event: key
```

```
[System][Info] 2017-06-21 17:24:42 LOG_MOD_BSP 2 Web string:System trig event: key
```

```
[System][Info] 2017-06-21 17:24:43 LOG_MOD_BSP 4 Web string:System trig event: key
```

```
[System][Info] 2017-06-21 17:25:16 LOG_MOD_MC 6 Web string:Ipv4 static access succ.
```

```
[System][Info] 2017-06-21 17:25:17 LOG_MOD_BSP 101 Web string:Create a type of IP message to LCD buffer. The first: IP, the second: 192.168.1.1
```

```
[System][Info] 2017-06-21 17:25:19 LOG_MOD_BSP 111 Web string:Power on the terminal successful
```

```
[System][Info] 2017-06-21 17:25:30 LOG_MOD_MC 143 Web string:License: parse succ.
```

```
[System][Info] 2017-06-21 17:25:33 LOG_MOD_BSP 163 Web string:System exit event: aux_video_in
```

```
[System][Info] 2017-06-21 17:27:37 LOG_MOD_AUDIO 168 Web string:Mic array disconnected. Device ID[0].
```

```
[System][Info] 2017-06-21 17:28:50 LOG_MOD_AUDIO 169 Web string:Mic array disconnected. Device ID[0].
```

```
[System][Info] 2017-06-21 17:29:30 LOG_MOD_AUDIO 170 Web string:Mic array disconnected. Device ID[1].
```

```
[System][Info] 2017-06-21 17:29:32 LOG_MOD_AUDIO 171 Web string:Mic array disconnected. Device ID[1].
```

```
[System][Info] 2017-06-21 17:32:24 LOG_MOD_AUDIO 172 Web string:Mic array disconnected. Device ID[0].
```

```
[System][Info] 2017-06-21 17:33:57 LOG_MOD_MC 204 Web string:Ipv4 dynamic access succ.
```

[System][Info] 2017-06-21 17:33:57 LOG_MOD_BSP 206 Web string:Create a type of IP message to LCD buffer. The first: IP, the second: 192.168.15.8

[System][Info] 2017-06-21 17:36:51 LOG_MOD_BSP 240 Web string:Create a type of IP message to LCD buffer. The first: IP, the second: 192.168.15.3

[System][Info] 2017-06-21 17:36:51 LOG_MOD_MC 242 Web string:Ipv4 static access succ.

[System][Info] 2017-06-21 17:40:52 LOG_MOD_AUDIO 267 Web string:Mic array disconnected. Device ID[1].

[System][Info] 2017-06-21 17:41:39 LOG_MOD_AUDIO 268 Web string:Mic array disconnected. Device ID[0].

[System][Info] 2017-06-21 17:44:43 LOG_MOD_AUDIO 269 Web string:Mic array disconnected. Device ID[1].

[System][Info] 2017-06-21 17:47:03 LOG_MOD_AUDIO 303 Web string:Mic array disconnected. Device ID[0].

[System][Info] 2017-06-21 17:47:03 LOG_MOD_AUDIO 304 Web string:Mic array disconnected. Device ID[1].

[System][Info] 2017-06-21 17:47:26 LOG_MOD_AUDIO 306 Web string:Mic array disconnected. Device ID[0].

[System][Info] 2017-06-21 17:48:09 LOG_MOD_BSP 392 Web string:System trig event: web

[System][Info] 2017-06-21 17:48:15 LOG_MOD_BSP 394 Web string:System enter event: web

[System][Info] 2017-06-21 17:51:12 LOG_MOD_AUDIO 398 Web string:Mic array disconnected. Device ID[1].

[System][Info] 2017-06-21 17:52:48 LOG_MOD_AUDIO 399 Web string:Mic array disconnected. Device ID[0].

[System][Info] 2017-06-21 17:55:28 LOG_MOD_AUDIO 400 Web string:Mic array disconnected. Device ID[0].

[System][Info] 2017-06-21 18:09:21 LOG_MOD_BSP 458 Web string:System exit event: web

[System][Info] 2017-06-21 18:13:40 LOG_MOD_BSP 460 Web string:System trig event: web

[System][Info] 2017-06-21 18:13:49 LOG_MOD_BSP 462 Web string:System enter event: web

(...)

[Debug][Info] 2017-06-26 15:45:17 LOG_MOD_PRTCL 20509 Upnp string:H323 Ras send 2 timeout [H323cHandleRasTimeout:8130] FILE:h323c_ras.c LINE:8130

[Debug][Info] 2017-06-26 15:45:17 LOG_MOD_PRTCL 20510 Upnp string:H323 Recv self message 7 FILE:h323c_callfunc.c LINE:451

[Debug][Info] 2017-06-26 15:45:17 LOG_MOD_PRTCL 20511 Upnp string:ProtType[H323] Regist result[CC_RESULT_ERR], reason[CC_REGISTER_TRANSPORTNOTSUPPORTED]. FILE:cc_pro_interface.c LINE:209

[Debug][Info] 2017-06-26 15:45:17 LOG_MOD_PRTCL 20512 Upnp string:Ccm send message to MC.msgId[1018], para1[1], para2[f] FILE:cc_ctrl.c LINE:1455

[Debug][Info] 2017-06-26 15:45:17 LOG_MOD_MC 20513 Upnp string:McCallCtrlSubMsgCCRegRet:CC Result: uwProtocol=1 ucRegResult=15 FILE:mc_conf_callctrl.c LINE:4829

[Debug][Info] 2017-06-26 15:45:17 LOG_MOD_MC 20514 Upnp string:McCallCtrlDoCCRegGkRet: ucRegGkOK = 0 FILE:mc_conf_callctrl.c LINE:18544

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_PRTCL 20520 Upnp string:Ccm send message 2007 From 0 To 3, MsgLen:8 [CC_SetDisableSNP 2842] FILE:cc_mc_interface.c LINE:2842

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_PRTCL 20521 Upnp string:Ccm UnRegister protocol[H323]. FILE:cc_mc_interface.c LINE:116

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_PRTCL 20522 Upnp string:Ccm send message 2033 From 0 To 3, MsgLen:4 [CC_UnRegister 128] FILE:cc_mc_interface.c LINE:128

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_PRTCL 20523 Upnp string:H323 Recv CCm message 2007 FILE:h323c_ccmcall.c LINE:60

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_PRTCL 20524 Upnp string:H323 Recv CCm message 2033 FILE:h323c_ccmcall.c LINE:60

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_PRTCL 20525 Upnp string:ProtType[H323] unregist result[CC_RESULT_OK],reason[CC_UNREGISTER_SUCCESS]. FILE:cc_pro_interface.c LINE:263

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_PRTCL 20526 Upnp string:Ccm send message to MC.msgId[1019], para1[1], para2[0] FILE:cc_ctrl.c LINE:1455

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_MC 20527 Upnp string:McCallCtrlSubMsgCCUnRegRet:UnReg Result: uwProtocol=1, udwResult=0 FILE:mc_conf_callctrl.c LINE:4894

[Debug][Info] 2017-06-26 15:45:23 LOG_MOD_MC 20528 Upnp string:McCallCtrlSubMsgCCUnRegRet: ucRegGkOK = 0, unreg success FILE:mc_conf_callctrl.c LINE:4910

[Debug][Error] 2017-06-26 15:45:31 LOG_MOD_MC 20529 Upnp string:UI_GetIPVersion: IP is domain address! FILE:mc_uiif_comm.c LINE:2542

[Debug][Error] 2017-06-26 15:45:31 LOG_MOD_MC 20530 Upnp string:UI_GetIPVersion: pIpStr len is 0 FILE:mc_uiif_comm.c LINE:2533

[Debug][Error] 2017-06-26 15:45:31 LOG_MOD_MC 20531 Upnp string:UI_GetIPVersion: pIpStr len is 0 FILE:mc_uiif_comm.c LINE:2533

</LogModule>

APÊNDICE C

Registro dos logs das chamadas no TOE.

RowID	StartTime	EndTime	RemotesSystemName	CallNumber	TransportType	CallRate	CallDirection	Ip	AudioProtocol_Tx	AudioProtocol_Rx	VideoProtocol_Tx	VideoProtocol_Rx
1	2017/06/27 00:02:03	2017/06/27 00:02:03	1994403	1994403	H.323	1024 kbps	out					
2	2017/06/27 00:01:41	2017/06/27 00:01:41	43021@bb.com.br	43021@bb.com.br	H.323	1920 kbps	out					
3	2017/06/26 23:45:31	2017/06/26 23:45:31	43021@bb.com.br	43021@bb.com.br	H.323	1920 kbps	out					
4	2017/06/26 23:44:41	2017/06/26 23:44:41	43021@bb.com.br	43021@bb.com.br	H.323	1920 kbps	out					
5	2017/06/26 23:44:26	2017/06/26 23:44:26	511195775@bb.com.br	511195775@bb.com.br	H.323	1920 kbps	out					
6	2017/06/26 23:44:12	2017/06/26 23:44:12	511195775@bb.com.br	511195775@bb.com.br	SIP	1920 kbps	out					
7	2017/06/26 23:43:53	2017/06/26 23:43:53	bb.com.br#43021	bb.com.br#43021	SIP	1920 kbps	out					
8	2017/06/26 23:43:43	2017/06/26 23:43:43	bb.com.br#43021	bb.com.br#43021	SIP	1920 kbps	out					
9	2017/06/26 23:43:30	2017/06/26 23:43:30	43021@bb.com.br	43021@bb.com.br	SIP	1920 kbps	out					
10	2017/06/26 23:43:19	2017/06/26 23:43:19	43021@bb.com.br	43021@bb.com.br	SIP	1920 kbps	out					
11	2017/06/26 12:01:59	2017/06/26 12:01:59	170.66.3.21@43021	170.66.3.21@43021	SIP	3840 kbps	out					
12	2017/06/26 12:01:41	2017/06/26 12:01:41	43021@170.66.3.21	43021@170.66.3.21	SIP	3840 kbps	out					
13	2017/06/26 12:01:24	2017/06/26 12:01:24	43021@bb.com.br	43021@bb.com.br	SIP	1024 kbps	in	172.24.11.2	G.7221c	G.7221c	H.264	H.264
14	2017/06/26 23:41:35	2017/06/26 23:42:35	1994403	1994403	H.323	1024 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
15	2017/06/26 23:36:19	2017/06/26 23:36:22	1994403	1994403	H.323	1024 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
16	2017/06/26 23:31:50	2017/06/26 23:35:33	1994403	1994403	H.323	1024 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
17	2017/06/26 23:30:28	2017/06/26 23:30:30	1999985	1999985	H.323	1024 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
18	2017/06/26 23:29:59	2017/06/26 23:30:17	1999985	1999985	H.323	1024 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
19	2017/06/26 12:17:16	2017/06/26 12:19:19	43021	43021	H.323	3840 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
20	2017/06/26 12:10:31	2017/06/26 12:13:48	43021	43021	H.323	3840 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
21	2017/06/26 12:04:18	2017/06/26 12:09:32	43021	43021	H.323	3840 kbps	in	170.66.3.21	G.7221c	G.7221c	H.264	H.264
22	2017/06/26 23:31:14	2017/06/26 23:31:25	1999985	1999985	H.323	1024 kbps	miss	170.66.3.21	G.7221c	G.7221c	H.264	H.264
23	2017/06/26 12:09:49	2017/06/26 12:09:55	43021	43021	H.323	3840 kbps	miss	170.66.3.21	G.7221c	G.7221c	H.264	H.264
24	2017/06/25 09:15:18	2017/06/25 09:17:16	101	101	SIP	3840 kbps	miss					
25	2017/06/25 09:15:46	2017/06/25 09:15:46	101	101	SIP	3840 kbps	miss					
26	2017/06/25 08:14:49	2017/06/25 08:16:47	101	101	SIP	3840 kbps	miss					
27	2017/06/25 08:15:21	2017/06/25 08:15:21	101	101	SIP	3840 kbps	miss					
28	2017/06/25 07:14:25	2017/06/25 07:16:23	101	101	SIP	3840 kbps	miss					
29	2017/06/25 07:14:59	2017/06/25 07:14:59	101	101	SIP	3840 kbps	miss					
30	2017/06/25 06:14:11	2017/06/25 06:16:09	101	101	SIP	3840 kbps	miss					
31	2017/06/25 06:14:47	2017/06/25 06:14:47	101	101	SIP	3840 kbps	miss					
32	2017/06/25 05:13:38	2017/06/25 05:15:36	101	101	SIP	3840 kbps	miss					
33	2017/06/25 05:14:19	2017/06/25 05:14:19	101	101	SIP	3840 kbps	miss					
34	2017/06/25 04:13:09	2017/06/25 04:15:07	101	101	SIP	3840 kbps	miss					
35	2017/06/25 04:13:47	2017/06/25 04:13:47	101	101	SIP	3840 kbps	miss					
36	2017/06/25 03:08:39	2017/06/25 03:10:37	101	101	SIP	3840 kbps	miss					

ANEXOS

ANEXO A

Datasheet Quick Start Guide do TOE Sistema de videoconferência TE 30 Huawei

DATASHEET

HUAWEI TE30

All-in-One HD Videoconferencing System



HUAWEI TE30 is an all-in-one HD videoconferencing system with unique voice dialing and Wi-Fi access, and enables more people to join a multipoint conference. Its compact appearance and simplified installation make it an ideal choice for small and medium-sized conference rooms.

Elegant all-in-one design, easy to deploy and install

TE30 is a compact system with built-in HD codec, camera, and microphone array.

It takes just 1 cable and 5 minutes from unpacking to joining a video conference.

Smart design enables TE30 to be wall-mounted, placed on a TV set, or ceiling-mounted with inverted installation.

Voice Dialing, P2P to multipoint

TE30 recognizes multiple languages. You can call or join a conference by saying the name of the scheduled conference or the site name.

The third-party can be added in a P2P call or called to connect to other multipoint conferences. No need to hang up the conference. This simplifies operation and improves efficiency.

Wi-Fi Access

Built-in Wi-Fi enables TE30 to support wireless network, wireless microphone, air content sharing.

User-Friendly Interface and Remote-Control Design

Innovative 3D GUI, convenient to use and maintain.

Wizard for first-time installation.

LCD display for real-time local site information.

Wireless touch panel (Optional) for visualized control.

Next-Generation Technology for Superior HD Experience at Lower Bandwidth

Supports Video Motion Enhancement (VME) and H.264 HP; saves 50% of bandwidth.

Proprietary VME combined with intelligent face recognition and video image processing helps TE30 adapt to different lighting conditions, reduce bandwidth consumption, and enhance video quality. Built-in microphone with sound pickup radius up to 6 m.

Outstanding Network Adaptability and Security Mechanism

Patented Super Error Concealment (SEC) ensures high-quality video experience even with packet loss of 20 percent.

Supports H.264 SVC to adapt to different bandwidths, device capabilities, and network requirements.

Standard H.460 and proprietary SNP technology guarantee secure firewall traversal.

H.235 media stream and signaling encryption; SRTP, TLS, and HTTPS encryption.

Extensive System Integration

Inter-operable with standard endpoints and infrastructures.

Integration with Microsoft Lync 2010™/Lync 2013™ and OCS 2007R2.

Seamless integration with IMS.

Plentiful third-party APIs for system integration and customization.



QUICK START GUIDE

■ Overview



The HUAWEI TE30 videoconferencing endpoint (TE30 for short) delivers the 1080p HD video performance in a sleek design.

Key features:

- All-in-one design, simple installation
- Voice dialing, English & Chinese.
- Wi-Fi supported

■ Getting Started

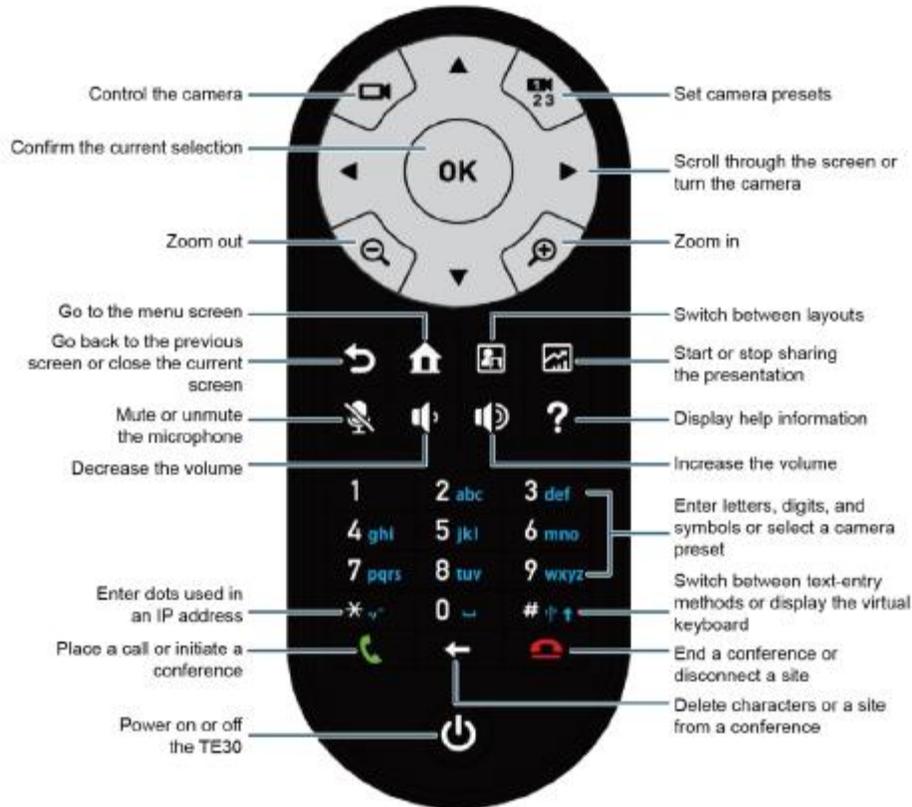


No.	Component	Description
①	Lens	12x optical zoom lens.
②	Built-in microphone	Provides 180-degree sound pickup and an optimal pick-up range of six meters.
③	MODE button	<ul style="list-style-type: none">● Restores the TE30 to its default settings if you press and hold this button for 10 seconds or more when

No.	Component	Description
		<p>the TE30 is operating properly.</p> <ul style="list-style-type: none"> Enters the boot ROM system if you press and hold this button for 3 seconds or more when the TE30 is being started. Switches the VGA IN port between VGA and YPbPr modes if you press this button when the TE30 is operating properly.
4	Infrared receiver module	Receives infrared signals from the remote control provided with the TE30.
5	OLED display	Displays the IP address, site number, and indications for the startup, upgrade, sleep mode, and malfunction.
6	Status indicator	Indicates the TE30 status, including operating, sleeping, malfunctioning, and upgrading.
7	SELECT button	<ul style="list-style-type: none"> Mutes or unmutes local microphones if you press this button when the TE30 is operating properly. Restores the TE30 to the settings of the last startup if you press and hold this button for 10 seconds or more when the TE30 is operating properly.
8	USB port	Connects to a USB flash drive.
9	LINE IN port	Connects to an audio input source such as a computer and mobile phone.
10	MIC/TV/LAN/POWER port	Functions as an HDMI, Ethernet, microphone, or power port using the accessorial integration cable.

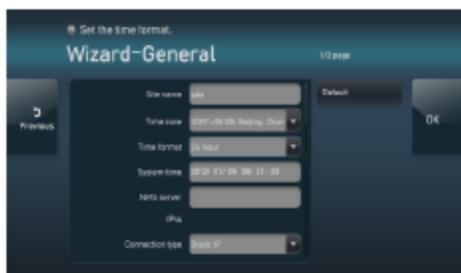
No.	Component	Description
⑪	LINE OUT port	Connects to an audio output device such as an external speaker or the input port in a monitor.
⑫	VGA IN port	Connects to a VGA input source such as a computer and DVD player.
⑬	VGA OUT port	Connects to a VGA display device such as a projector.

■ Using the Remote Control



- The maximum operating distance of the remote control is 15 meters.
- The remote control performance may be affected under bright light.

■ Configuring the TE30



When powered on for the first time, your TE30 prompts you to select a language. After you select a language, the screen to the left is displayed for you to set the general parameters.

Q If you set **NMS server**, **Connection type**, **Local IP address**, **Subnet mask**, and **Gateway address**, the TE30 automatically attempts to obtain the configuration of the network management system (NMS) server. After the TE30 obtains the configuration, it displays the conferencing screen.

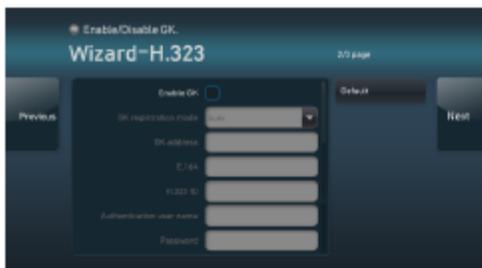
Parameter	Description	Setting
NMS server	IP address of the HUAWEI SMC 2.0.	Contact the local reseller or operator.
Connection type	<p>Mode for obtaining an IP address.</p> <ul style="list-style-type: none"> Static IP: The network administrator assigns an IP address to your TE30. If you select this option, you must also set Local IP address, Subnet mask, and Gateway address. Dynamic IP: When a DHCP server is available on the network, your TE30 automatically obtains an IP address using the Dynamic Host Configuration Protocol (DHCP). 	<p>The default value is Static IP.</p> <p>If you have set NMS server, select Static IP for this parameter.</p>

Parameter	Description	Setting
Local IP address Subnet mask	IP address and subnet mask of your TE30.	Contact the network administrator. Examples: <ul style="list-style-type: none"> • IPv4 address: 192.168.1.10 • IPv6 address: 2000:0:0:0:200:55:26:1
Gateway address	Gateway address that corresponds to the TE30 IP address. This parameter is mandatory when Connection type is set to Static IP .	Contact the network administrator. Examples: <ul style="list-style-type: none"> • IPv4 address: 192.168.1.1 • IPv6 address: 2000:0:0:0:200:55:0:1

Click **OK** to save the settings. Then proceed based on your settings:

- If you have set **NMS server**, **Local IP address**, **Subnet mask**, and **Gateway address**, a dialog box is displayed. If you click **Yes**, the TE30 automatically attempts to obtain the NMS server configuration. After the TE30 obtains the configuration, it displays the conferencing screen.
- If you have not configured the NMS server or if the attempt to obtain the NMS server configuration times out, you must manually set H.323 and SIP parameters.

Setting H.323 Parameters



On the screen shown to the left, set H.323 parameters.

Parameter	Description	Setting
Enable GK	<p>Whether to register your TE30 with the network gatekeeper (GK).</p> <ul style="list-style-type: none"> If you select this option, the TE30 will register with the GK after being started. After the TE30 successfully registers with the GK, it can call endpoints defined in the address book by their IP addresses, numbers, and names. If you do not select this option, the TE30 will not register with the GK and can call other endpoints by their IP addresses only. 	<p>By default, this option is deselected.</p> 
Site number	<p>Site number for the TE30. If the TE30 is registered with the GK, other endpoints can call it by this number.</p>	<p>The site number can contain only digits. Example: 12345</p>
H.323 ID	<p>Name by which the GK identifies the TE30 after it registers with the GK.</p>	<p>The name consists of digits, letters, and special characters, such as @#%. Example: ab3@Joe</p>
Authentication user name	<p>User name used for H.323 authentication.</p>	<p>Obtain the user name from your network service provider. Ensure that this user name is the same as that predefined on the GK.</p>

Parameter	Description	Setting
Password	Password used by the TE30 to register with the GK. The GK uses the password to authenticate your TE30.	Obtain the password from your network service provider. Ensure that this password is the same as that predefined on the GK.
Huawei GK	Whether to enable the Huawei GK. If the Huawei GK is disabled, some functions, such as Conference Control , are unavailable on the TE30.	By default, this option is deselected. Deselect this option if your TE30 is interoperating with endpoints of other suppliers.

Setting SIP Parameters



Click **Next**. On the screen shown to the left, set SIP parameters.

Parameter	Description	Setting
Register with server	Whether to register with the SIP server. <ul style="list-style-type: none"> If you select this option, the TE30 will register with the SIP server. After the TE30 successfully registers with the SIP server, it can call endpoints defined in the address book by their IP addresses, numbers, and 	By default, this option is deselected.

Parameter	Description	Setting
	<p>names.</p> <ul style="list-style-type: none"> If you do not select this option, the TE30 will not register with the SIP server and can call other endpoints by their IP addresses only. 	
Site number	Site number for the TE30. If the TE30 is registered with the SIP server, other endpoints can call it by this number.	Example: 12345
User name Password	User name and password used by the TE30 to register with the SIP server.	<p>The values can consist of numbers, letters, and special symbols, such as @ # %.</p> <p>Example: ab3@Joe</p>

Click **Finish**.

■ Getting to Know the User Interface

Conferencing Screen



To access the conferencing screen, press  on the remote control.

To move section 1, 2, or 3 to the middle, press the left and right arrow keys on the remote control.

- | | |
|-------------------------------|--------------------|
| 1 Conference schedules screen | 2 Call screen |
| 3 Conference history screen | 4 System time |
| 5 Status icon | 6 Local IP address |

Menu Screen



To access the menu screen, press  on the remote control.

- You can find the menu bar on the left of the menu screen. This menu bar is your interface to all functions except conferencing
- To hide the menu bar, press the left arrow key, , or  on the remote control.
- To show the menu bar again, press  on the remote control.

■ Initiating a Conference

From the conferencing screen, you can initiate a conference using one of the following methods:



Select **Call**. On the screen shown to the left, perform any of the following

- In the text box, enter the name, IP address, or number of the site you wish to call. Then press **OK** or  on the remote control.
- From the displayed list, select the site or group you wish to call. Then press **OK** or  on the remote control.
- Click  or press and hold  on the remote control. Then speak out the name of the site you wish to call.



Select **Conference History**. On the screen shown to the left:

- Select a multipoint conference entry and press **OK** on the remote control twice.
- Select a point-to-point conference entry and press **OK** on the remote control.



Select **Conference Schedules**. On the screen shown to the left, select a favorite or ongoing conference and press **OK** on the remote control to initiate or join the conference.

- : indicates that the conference is ongoing
- : indicates that the conference has not yet started and you cannot call into it.
- : indicates that the conference is a favorite conference.

■ Sharing a Presentation

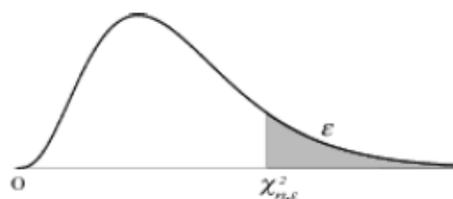
Use a VGA cable to connect the video output of the presentation source to the VGA IN port in the TE30. Then press the  key on the remote control to share the presentation.

The presentation contents can be static pictures, such as a computer desktop, or motion video played on a Digital Video Disc (DVD) or Video Compact Disc (VCD) player.

ANEXO B

Distribuição do Qui-Quadrado (CONTI, 2011)

$$\chi^2_{n,\varepsilon} : P(X > \chi^2_{n,\varepsilon}) = \varepsilon$$



ε	995	990	975	950	900	.750	.500	250	.100	.050	.025	.010	.005	.001
1	.000	.000	.001	.004	.016	.102	.455	1.323	2.706	3.841	5.024	6.635	7.879	10.827
2	.010	.020	.051	.103	.211	.575	1.386	2.773	4.605	5.991	7.378	9.210	10.597	13.815
3	.072	.115	.216	.352	.584	1.213	2.366	4.108	6.251	7.815	9.348	11.345	12.838	16.266
4	.207	.297	.484	.711	1.064	1.923	3.357	5.385	7.779	9.488	11.143	13.277	14.860	18.466
5	.412	.554	.831	1.145	1.610	2.675	4.351	6.626	9.236	11.070	12.832	15.086	16.750	20.515
6	.676	.872	1.237	1.635	2.204	3.455	5.348	7.841	10.645	12.592	14.449	16.812	18.548	22.457
7	.989	1.239	1.690	2.167	2.833	4.255	6.346	9.037	12.017	14.067	16.013	18.475	20.278	24.321
8	1.344	1.647	2.180	2.733	3.490	5.071	7.344	10.219	13.362	15.507	17.535	20.090	21.955	26.124
9	1.735	2.088	2.700	3.325	4.168	5.899	8.343	11.389	14.684	16.919	19.023	21.666	23.589	27.877
10	2.156	2.558	3.247	3.940	4.865	6.737	9.342	12.549	15.987	18.307	20.483	23.209	25.188	29.588
11	2.603	3.053	3.816	4.575	5.578	7.584	10.341	13.701	17.275	19.675	21.920	24.725	26.757	31.264
12	3.074	3.571	4.404	5.226	6.304	8.438	11.340	14.845	18.549	21.026	23.337	26.217	28.300	32.909
13	3.565	4.107	5.009	5.892	7.041	9.299	12.340	15.984	19.812	22.362	24.736	27.688	29.819	34.527
14	4.075	4.660	5.629	6.571	7.790	10.165	13.339	17.117	21.064	23.685	26.119	29.141	31.319	36.124
15	4.601	5.229	6.262	7.261	8.547	11.037	14.339	18.245	22.307	24.996	27.488	30.578	32.801	37.698
16	5.142	5.812	6.908	7.962	9.312	11.912	15.338	19.369	23.542	26.296	28.845	32.000	34.267	39.252
17	5.697	6.408	7.564	8.672	10.085	12.792	16.338	20.489	24.769	27.587	30.191	33.409	35.718	40.791
18	6.265	7.015	8.231	9.390	10.865	13.675	17.338	21.605	25.989	28.869	31.526	34.805	37.156	42.312
19	6.844	7.633	8.907	10.117	11.651	14.562	18.338	22.718	27.204	30.144	32.852	36.191	38.582	43.819
20	7.434	8.260	9.591	10.851	12.443	15.452	19.337	23.828	28.412	31.410	34.170	37.566	39.997	45.314
21	8.034	8.897	10.283	11.591	13.240	16.344	20.337	24.935	29.615	32.671	35.479	38.932	41.401	46.796
22	8.643	9.542	10.982	12.338	14.041	17.240	21.337	26.039	30.813	33.924	36.781	40.289	42.796	48.268
23	9.260	10.196	11.689	13.091	14.848	18.137	22.337	27.141	32.007	35.172	38.076	41.638	44.181	49.728
24	9.886	10.856	12.401	13.848	15.659	19.037	23.337	28.241	33.196	36.415	39.364	42.980	45.558	51.179
25	10.520	11.524	13.120	14.611	16.473	19.939	24.337	29.339	34.382	37.652	40.646	44.314	46.928	52.619
26	11.160	12.198	13.844	15.379	17.292	20.843	25.336	30.435	35.563	38.885	41.923	45.642	48.290	54.051
27	11.808	12.878	14.573	16.151	18.114	21.749	26.336	31.528	36.741	40.113	43.195	46.963	49.645	55.475
28	12.461	13.565	15.308	16.928	18.939	22.657	27.336	32.620	37.916	41.337	44.461	48.278	50.994	56.892
29	13.121	14.256	16.047	17.708	19.768	23.567	28.336	33.711	39.087	42.557	45.722	49.588	52.335	58.301
30	13.787	14.953	16.791	18.493	20.599	24.478	29.336	34.800	40.256	43.773	46.979	50.892	53.672	59.702
40	20.707	22.164	24.433	26.509	29.051	33.660	39.335	45.616	51.805	55.758	59.342	63.691	66.766	73.403
50	27.991	29.707	32.357	34.764	37.689	42.942	49.335	56.334	63.167	67.505	71.420	76.154	79.490	86.660
60	35.534	37.485	40.482	43.188	46.459	52.294	59.335	66.981	74.397	79.082	83.298	88.379	91.952	99.608
70	43.275	45.442	48.758	51.739	55.329	61.698	69.334	77.577	85.527	90.531	95.023	100.425	104.215	112.317
80	51.172	53.540	57.153	60.391	64.278	71.145	79.334	88.130	96.578	101.879	106.629	112.329	116.321	124.839
90	59.196	61.754	65.647	69.126	73.291	80.625	89.334	98.650	107.565	113.145	118.136	124.116	128.299	137.208
100	67.328	70.065	74.222	77.929	82.358	90.133	99.334	109.141	118.498	124.342	129.561	135.807	140.170	149.449

Como usar a tabela

Ao se consultar uma tabela de χ^2 deve-se lembrar que:

$$G.L. = \text{número de classes} - 1$$

A tabela de Qui Quadrado mostra o número de *Graus de liberdade* nas linhas e o valor da *Probabilidade* nas colunas.

Na coluna referente a 5% de probabilidade encontra-se o *valor crítico* de qui quadrado (χ_c^2), com o qual deve ser comparado o valor calculado de χ^2 .

GL \ P	0,99	0,95	0,90	0,80	...	χ_c^2	0,02	0,01	0,001
						0,05			
1	0,0002	0,004	0,016	0,064	...	3,841	5,412	6,635	10,827
2	0,020	0,103	0,211	0,446	...	5,991	7,824	9,210	13,815
3	0,115	0,352	0,584	1,005	...	7,815	9,837	11,345	16,266
4	0,297	0,711	1,064	1,649	...	9,488	11,668	13,277	18,467
5	0,554	1,145	1,610	2,343	...	11,070	13,388	15,080	20,515
...									
Conclusão	Aceita-se a hipótese de igualdade estatística entre os números de observados e de esperados (H_0). Os desvios <i>não são</i> significativos.					Rejeita-se H_0 e aceita-se H_1 . Os números de obs e esp são estatisticamente diferentes. Os desvios <i>são</i> significativos.			

ANEXO C

Correção de Yates (ou Correção de continuidade) (CONTI, 2011)

Ao aplicar o teste de χ^2 supõe-se que o tamanho das amostras seja "grande".

Mas em situações práticas, o valor de χ^2 calculado é *aproximado*, pois

- utiliza-se amostras de tamanho finito,
- o valor da frequência observada só assumir os valores de números inteiros, ou seja nunca haverá por exemplo 2,73 indivíduos observados.

Quando se obtém um valor de χ^2 *significativo* mas nota-se que *a amostra é pequena* e/ou que a *frequência esperada em uma das classes é pequena* (tipicamente, quando for menor que 5) a fórmula de obtenção de χ^2 poderá produzir um valor maior que o real.

Alguns autores, entre eles *Ronald Fisher*, recomendam que se observe a seguinte restrição:

O teste de χ^2 pode ser usado se o número de observações em cada casela da tabela for *maior ou igual a 5* e a menor *frequência esperada* for maior ou igual a 5.

Em caso contrário, em cada classe deve ser utilizada a correção de Yates:

$$\chi^2 = \sum [(|o - e| - 0,5)^2 / e]$$

Evidentemente, não é preciso usar a correção de Yates se o valor de χ^2 obtido for *menor* que χ^2_c , pois o novo valor será menor que o primeiro, continuando a não ser significativo.

Apesar do assunto ser *controverso*, de modo geral, usa-se a correção de Yates quando:

- o valor de Qui Quadrado obtido é maior que o crítico e
- o valor de *N* é menor que 40 ou
- há pelo menos uma classe com número de esperados menor que 5.

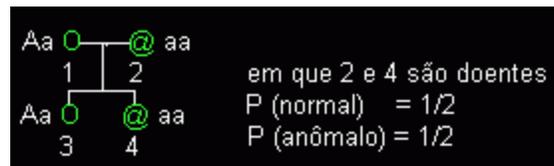
Exemplo 1

Supondo uma coleção de irmandades, com *N = 16*, filhos de casais com um cônjuge afetado por uma anomalia endógena.

4 dentre os filhos também apresentam a doença.

A característica obedece ao padrão de transmissão autossômico, dominante e monogênico?

A *genealogia* seria:



Em 16 filhos espera-se 8 normais e 8 anormais. Mas foram observados 12 normais e 4 anormais.

Obtém-se o valor de Qui quadrado:

$$\chi^2 = [(12 - 8)^2 / 8 + (4 - 8)^2 / 8] = 2 + 2 = 4$$

Simplesmente analisando o valor de χ^2 concluiria-se que como é maior que χ^2_c (3,841) os desvios não são devidos ao acaso. Portanto, conclui-se que a doença não obedece o padrão de transmissão autossômico, dominante e monogênico.

Entretanto, deve-se reparar que:

- N é menor que 40 e
- o valor de Qui Quadrado obtido é maior que o crítico

Portanto, deve-se aplicar a correção de Yates:

$$\chi^2 = [(|o_1 - e_1| - 0,5)^2 / e_1 + (|o_2 - e_2| - 0,5)^2 / e_2]$$

$$\chi^2 = [(|12 - 8| - 0,5)^2 / 8 + (|4 - 8| - 0,5)^2 / 8] = 1,51313 + 1,51313 = 3,026$$

É importante notar que agora, *após* ter sido aplicada a correção, $\chi^2 < \chi^2_c$, ou seja, será alterada a decisão a que o teste permite chegar.

Portanto, aceita-se que os desvios são devidos ao acaso. Assim, conclui-se que a doença obedece ao padrão de transmissão autossômico, dominante e monogênico.