NORMA TÉCNICA – B 04

SEGURANÇA ELETRÓNICA DE INFRAESTRUTURAS E DE PRODUTOS UTILIZADOS NO PROCESSAMENTO E DISSEMINAÇÃO DE INFORMAÇÃO CLASSIFICADA

"MODELO DE ZONA"

Lisboa, 15 de dezembro de 2023

A Autoridade Nacional de Segurança

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2023.12.20 10:52:05 Z

(António Gameiro Marques)

(ESTA PÁGINA FOI DEIXADA EM BRANCO INTENCIONALMENTE)

1. REFERÊNCIAS

a. Nacionais:

1) Lei Orgânica do GNS, Decreto-Lei nº3/2012, de 16 de janeiro, na sua atual redação;
2) Resolução do Conselho de Ministros nº 50/88, de 3 de dezembro (SEGNAC 1);
3) Resolução do Conselho de Ministros nº 37/89, de 24 de outubro (SEGNAC 2);
4) Resolução do Conselho de Ministros nº 16/94, de 22 de março (SEGNAC 3);
5) Resolução do Conselho de Ministros nº 05/90, de 28 de fevereiro (SEGNAC 4).

b. Organização do Tratado do Atlântico Norte (OTAN/NATO):

1) C-M(2002)49 *NATO Security Policy*;
2) AC/35-D/2004 – *Primary Directive on CIS Security*;
3) AC/35-D/2005 – *Management Directive on CIS Security*;
4) AC/322-D/0048-REV3 (INV) – *Technical and Implementation Directive on CIS Security*;
5) AC/322-D(2019)0021 (INV) - *Directive on Emission Security*.

c. União Europeia (EU/EU):

1) DECISÃO DO CONSELHO de 23 de setembro de 2013 relativa às regras de segurança aplicáveis à proteção das Informações Classificadas da UE (2013/488/UE);
2) DECISÃO (UE, EURATOM) 2015/444 DA COMISSÃO de 13 de março de 2015 relativa às regras de segurança aplicáveis à proteção das Informações Classificadas da UE;
3) *IA Security Policy on TEMPEST* – IASP 7;
4) *IA Security Guidelines on Selection and Installation of TEMPEST Equipment* – IASG 7-01:
5) *IA Security Guidelines on TEMPEST Zoning Procedures* – IASG 7-02;
6) *IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures* – IASG 7-03.

d. Outras:

1) SDIP 27 – *NATO TEMPEST Requirements and Evaluation Procedures*;
2) SDIP 28 – *NATO Zoning Procedures*;
3) SDIP 29 - *Facility Design Criteria and Installation of Electrical Equipment for Processing Classified Information*;
4) *NATO STANDARD AECTP-250 Electrical and Electromagnetic Environmental Conditions, Edition C Version1, December 2014;*
5) *NATO STANDARD AECTP-500 Electromagnetic Environmental Effects tests and Verification, Edition E Version1, December 2016;*

6) *ITU-T K.84 – Test methods and guide against information leaks through unintentional electromagnetic emissions;*
7) *ITU-T K.87 – Guide for the application of electromagnetic security requirements – Overview;*
8) ITU-T K.115 - *Mitigation methods against electromagnetic security threats;*
9) CISPR 17 - *Methods of measurement of the suppression characteristics of passive radio interference filters and suppression components*;
10) *MIL-STD-220B - Departement of Defense, Test Method Standard, Method of Insertion Loss Measurement;*
11) *BSI TR-03209 – 1* e *BSI TR-03209 – 2 - Federal Office for Information Security*, Blindagem eletromagnética de edifícios*;*
12) *BSI TR-03305 - Federal Office for Information Security, Hardware* testado em termos de emissões e aprovado para Informações Classificadas do governo *(VS);*
13) Portaria n.º 949-A/2006 de 11 de setembro - Regras técnicas das instalações elétricas de baixa tensão.

2. DEFINIÇÕES

a. Atenuação:[1] Diminuição do nível de um sinal atribuído à absorção, reflexão, espalhamento, filtragem e dispersão.

b. Emanação:[2] Sinal (eletromagnético, acústico ou outro meio) que é emitido por um sistema (por meio de radiação ou condutância) como consequência (ou seja, por produto) da sua operação, e que pode conter informação sensível ou classificada.

c. Emanações comprometedoras:[3] Sinais não intencionais que, se intercetados e analisados, poderão revelar informação classificada transmitida, recebida, tratada ou de outra forma processada por sistemas de informação eletrónicos.

d. Espaço Inspecionável: Espaço tridimensional ao redor do equipamento ou sala onde se processa informação classificada, dentro das quais a exploração *TEMPEST* pode ser desconsiderada por existir autoridade legal para identificar e remover uma potencial ameaça *TEMPEST*.

[1] Tradução livre do documento: *IA Security Policy on TEMPEST – IASP 7.*
[2] Idem.
[3] Tradução livre do documento: *IA Security Policy on TEMPEST – IASP 7.*

e. **Interferência eletromagnética intencional (IEMI):**[4] Termo aplicado a um ambiente eletromagnético criado intencionalmente para produzir interferência em equipamentos e Tecnologias de Informação (TIC). A ameaça IEMI é dividida em dois tipos principais: ameaças eletromagnéticas de alta potência (HPEM) e por pulso eletromagnético de alta altitude (HEMP).

f. **Interferência eletromagnética não-intencional (EMI):**[5] Termo aplicado a um ambiente onde as ondas rádio emitidas involuntariamente pela exploração de equipamentos e TIC são passiveis de ser capturadas e reproduzidas num outro ambiente.

g. ***Facility Zoning*:**[6] Caracterização da atenuação de um local em função do nível de radiação eletromagnética não intencional observado através da realização de testes de medição com radiofrequência (RF).

h. **Perímetro Controlado**: Perímetro que rodeia uma infraestrutura, separado do restante espaço por uma barreira, vedação ou muro e que se encontra sob monitorização continua por parte de uma entidade de segurança.

i. **Segurança de Emanações Eletromagnéticas (*EMSEC*):**[7] Disciplina que estuda a emanação de sinais eletromagnéticos intencionais e não intencionais, conduzidos ou radiados, através da imposição de restrições físicas e eletrónicas por forma a evitar a emanação de informações comprometedoras.

j. **Sistemas de Informação (SI):** Conjunto de componentes (Hardware e Software) inter-relacionados que trabalham em conjunto para recolher, processar, armazenar e distribuir informação para suporte da tomada de decisão, coordenação, controlo, análise e visualização na organização[8].

---

[4] Idem.
[5] Tradução livre do documento: ITU-T K.84 – *Test methods and guide against information leaks through unintentional electromagnetic emissions*.
[6] Tradução livre do documento: *IA Security Policy on TEMPEST* – IASP 7.
[7] Idem.
[8] Tradução livre de *LAUDON*, K. e *LAUDON*, J., *Essentials of Management Information Systems, Organization and Technology, 2nd edition, Prentice-Hall*, 1996.

k. **Sistemas de Informação e de Comunicação (SIC)**[9]**:** Sistemas que permitem o tratamento de informação em formato eletrónico, que compreendem todos os ativos necessários para o seu funcionamento, incluindo a infraestrutura, a organização, o pessoal e os sistemas de informação (SI).

l. **Tecnologias de Informação e de Comunicação (TIC):** Conjunto diversificado de ferramentas e recursos tecnológicos utilizados para transmitir, armazenar, criar, compartilhar ou trocar informação. Essas ferramentas e recursos tecnológicos incluem computadores, a Internet, tecnologias de transmissão, tecnologias de gravação e de telecomunicação (fixa ou móvel, satélite, etc.).[10]

m. ***Telecommunications Electronics Material Protected From Emanating Spurious Transmissions (TEMPEST):***[11] Conjunto de especificações e padrões tecnológicos usados para limitar a força das emanações eletromagnéticas produzidas por equipamentos elétricos e eletrónicos e, assim, reduzir a vulnerabilidade à escuta e exfiltração de informação comprometedora.

3. SITUAÇÃO

a. As ondas eletromagnéticas são normalmente descritas coletivamente pelo termo radiofrequência (RF), podendo a emanação de RF ser discutida em termos de "energia", "radiação" ou "campos".

b. Todo o dispositivo eletrónico emana interferência eletromagnética durante a sua operação, propagando-se como ondas eletromagnéticas, sem qualquer meio físico de transporte ao longo de condutores metálicos.

c. Os dispositivos que processam Informação Classificada (IC) não só radiam ou conduzem energia, podendo esta energia transportar a informação que está a ser processada, ser exfiltrada ou sofrer perturbações ou ataques de variada ordem.

---

[9] Tradução livre de *COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information* (2013/488/EU), disponível em: https://eur-lex.europa.eu/legal-content/EN/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=ENTXT/PDF/?uri=CELEX:32013D0488&from=EN, consultada em 17/08/2020.

[10] Tradução livre de: http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict , consultada em 17/08/2020.

[11] Tradução livre do documento: ITU-T K.87 – *Guide for the Application of Electromagnetic Security requirements – Overview.*

d. Dado que a intensidade das emissões de interferência diminui com o aumento da distância da fonte da interferência, a medida de proteção mais fiável contra um ataque de espionagem é implementar a maior área de segurança possível em torno dos dispositivos a proteger.

e. Sendo outro fator de proteção, o reforço da estrutura do edifício ou do espaço por forma a enfraquecer as emissões eletromagnéticas, de forma a que a intensidade da radiação fora do edifício seja menor do que seria esperado com base apenas na distância.

f. Estes dois fatores de proteção – distância e atenuação – são utilizados para a criação de um modelo, designado por "**Modelo de Zona**".

g. Quer a OTAN, quer a UE possuem Modelos de Zona com intuito de fazer face a ataques de espionagem.

h. Recentemente a UE, atualizou o seu referencial, *Information Assurance Security Guidelines on Selection and Installation of TEMPEST equipment* (IASG 7-01) [EU-R], introduzindo uma nova zona, designada por *Facility Zoning* 3, motivando a necessidade de criar um Modelo de Zona a aplicar pelas entidades nacionais.

4. OBJETO/FINALIDADE

O presente documento visa definir o Modelo de Zona e as medidas de proteção segurança eletrónica a serem observadas pelas entidades nacionais publicas e privadas no âmbito do processamento de Informação Classificada na marca Nacional de grau igual ou superior a CONFIDENCIAL.

5. ÂMBITO

A presente norma destina-se a ser implementada por:

a. Entidades e organismos públicos e privados que processam Informação Classificada de qualquer marca ou grau;

b. Projetistas, engenheiros de projeto e construtores que edifiquem salas ou edifícios com requisitos de segurança eletrónica;

c. Chefes de Sub-Registo e Postos de Controlo, Responsáveis pela Segurança dos Serviços, Órgãos ou Organismos públicos, quer dentro, quer fora do país que necessitem planear, desenhar, implementar e explorar SIC para manuseio de informação classificada, independentemente do regime normativo ao qual a Informação Classificada está subjacente.

6. O MODELO DE ZONA

a. Tomando por base os anexos A, B, C e D, nos quais são explicitadas as noções elementares que servem de base ao estudo da exploração do espectro eletromagnético, é concebido o **Modelo de Zona**, cujo objetivo é garantir que nenhuma emanação comprometedora possa ser detetada nas áreas de domínio público, ou seja passível de ser usada para a condução de escutas clandestinas e a exfiltração de Informação Classificada.

b. O pré-requisito para a utilização do Modelo de Zona assenta na definição do limite da área segura, perímetro controlado, na qual um qualquer atacante possui liberdade suficiente ou não representa uma ameaça direta para a exploração de dispositivos eletrónicos, nomeadamente para o processamento de Informação Classificada (IC).

c. A avaliação do nível de atenuação da infraestrutura, é medido entre a localização do dispositivo eletrónico que processa IC e o limite da área segura ou perímetro controlado, permitindo atribuir um "Nível de Zona" à infraestrutura, doravante designado por ZONA, que pode variar entre a ZONA 0 e a ZONA 3.

d. Neste sentido, o Modelo de Zona permite à organização projetar a sua infraestrutura tecnológica tirando partido do nível de atenuação que a sua infraestrutura física oferece.

e. Resumidamente a medição do nível de atenuação de uma infraestrutura física inicia-se com a medição do valor de referência em campo livre a uma distância de 20 (vinte) metros, através de um gerador que transmite diferentes frequências com potência definida.

f. Posteriormente no interior das instalações é realizado novo teste em cada espaço de interesse, registando-se o valor lido. O nível de atenuação da estrutura física varia com a frequência e será dado pela diferença entre as duas leituras feitas sobre a intensidade de campo em decibéis [dB].

g. Assim, uma infraestrutura física pode oferecer condições de segurança eletrónica de diferentes níveis, designadamente:

1) **ZONA 0**: para um perímetro controlado inferior a 20 metros;
2) **ZONA 1**: para um perímetro controlado entre 20 e 100 metros;
3) **ZONA 2**: para um perímetro controlado entre 100 e 1000 metros;
4) **ZONA 3**: para um perímetro controlado superior a 1000 metros.

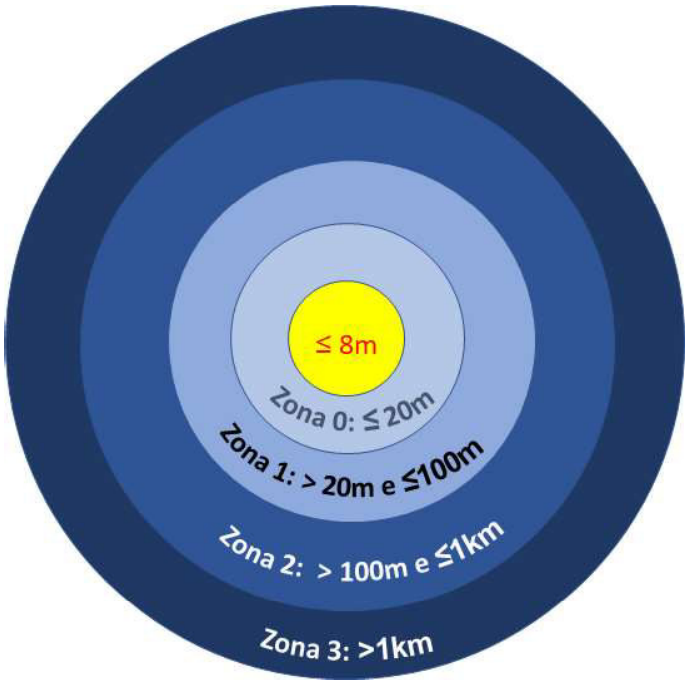

Figura 1 – Modelo de Zona

h. A determinação do tipo de zona permite à organização mapear os diferentes espaços interiores e projetar com maior rigor o grau de proteção em termos de segurança eletrónica que é necessário.

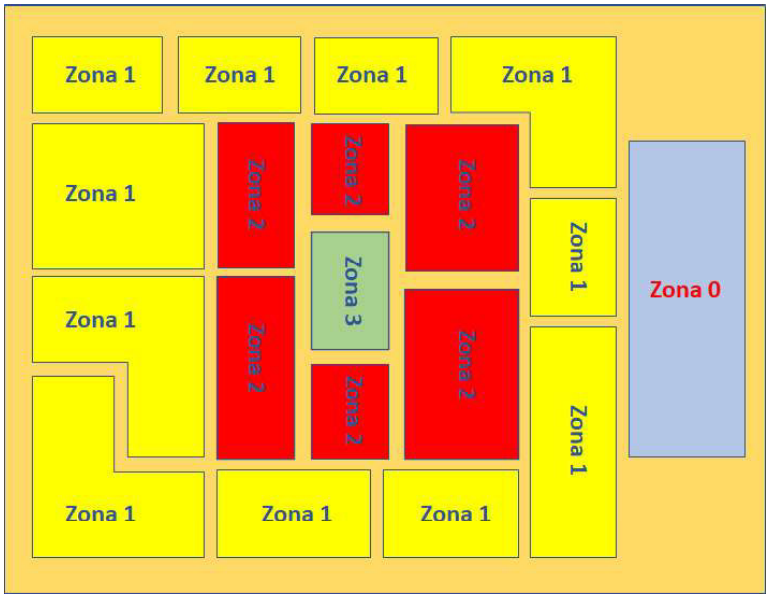

Figura 2 – Modelo de Zona aplicado a uma organização

i. A determinação do tipo de zona poder ser feito por avaliação da distância em relação ao perímetro controlado ou por avaliação do nível de atenuação equivalente na estrutura física ou espaço da organização, presente no Anexo G.

j. Semelhantemente, também pode ser determinado o nível de ruido que cada dispositivo eletrónico emite, fazendo-o corresponder um tipo de zona, designadamente:

1) **Equipamento Zona (EZ) 0**: para dispositivos com emanação residual, ou avaliados como nível A de acordo com o referencial SDIP27/2 ou o referencial *IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures* IASG 7-03;
2) **Equipamento Zona (EZ) 1**: para dispositivos com fraca emanação, ou avaliados como nível B de acordo com o referencial SDIP27/2 ou o *referencial IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures* IASG 7-03;
3) **Equipamento Zona (EZ) 2**: para dispositivos com moderada emanação, ou avaliados como nível C de acordo com o referencial SDIP27/2 ou o referencial *IA Security Guidelines on EU TEMPEST Requirements and Evaluation Procedures* IASG 7-03;
4) **Equipamento Zona (EZ) 3**: para dispositivos caracterizados pela Diretiva Europeia 214/30/EU, vulgarmente designados por commercial-of-the-shelf (COTS), desde que sem antenas ou módulos transmissores de RF na sua composição.

k. A avaliação de dispositivos eletrónicos, como sejam produtos comerciais, mas também produtos fabricados com elevados requisitos de proteção eletromagnética designados como produtos de Baixa Radiação (*TEMPEST*), é feita no âmbito do Esquema de Avaliação e Certificação em Segurança Tecnológica de produtos e serviços habilitados para tratamento de Informação Classificada.

l. Neste sentido, fazendo corresponder nível de zona da infraestrutura física ao nível de ruido de cada dispositivo eletrónico, é possível obter um nível de proteção de segurança eletrónica maior, de forma eficiente e com claras vantagens para a organização e para a segurança da informação classificada por esta manuseada.

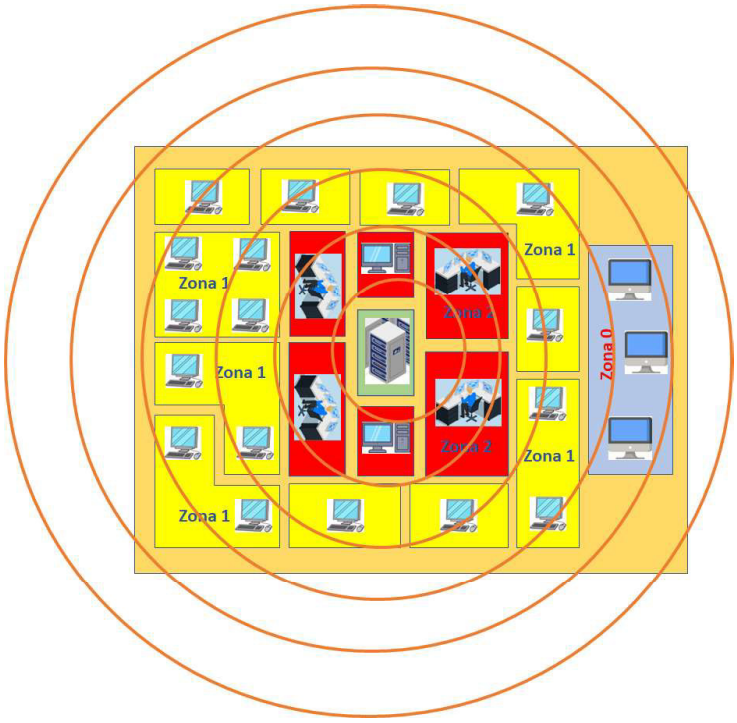

Figura 3 – Exemplificação do Modelo de Zona aplicado à seleção de equipamentos

m. Quando o nível de proteção de segurança eletrónica obtido através do Modelo de Zona, não é suficiente, devem ser tomadas medidas de proteção adicionais ao nível da infraestrutura física ou ao nível da seleção de dispositivos eletrónicos de Baixa Radiação (*TEMPEST*).

n. Sempre que o espaço inspecionável for igual ou inferior a 8 metros, deve ser consultada a Autoridade TEMPEST (AT) por forma a definir que medidas devem ser tomadas ao nível da proteção da infraestrutura física ou ao nível da seleção de dispositivos eletrónicos de Baixa Radiação (*TEMPEST*).

7. MEDIDAS GERAIS DE PROTEÇÃO SEGURANÇA ELETRÓNICA

a. Os requisitos de Segurança Eletrónica assentam em exigências de blindagem, filtragem, separação, proteção e controlo.

b. No anexo E, são identificadas medidas adicionais de mitigação de fuga de informação em computadores. Sendo, no anexo F, apresentada uma relação do custo-benefício explicitada pelo congénere alemão do *Federal Office for Information Security* (BSI).

7.1. REQUISITOS DE BLINDAGEM

a. Dependendo do grau, o processamento de Informação Classificada (IC), apenas é possível utilizar espaços avaliados segundo o Modelo de Zona, que combinem o nível de atenuação da infraestrutura com o nível de emanação dos dispositivos eletrónicos utilizados.

b. Os requisitos de blindagem atuam sobre a infraestrutura física, sobre a redução da radiação eletromagnética emitida por um dispositivo eletrónico, ou sobre ambos os fatores.

c. O processamento de IC de grau igual ou superior a NACIONAL CONFIDENCIAL, requer a avaliação das infraestruturas físicas através do Modelo de Zona por parte do GNS.

d. O anexo G proporciona os requisitos gerais de blindagem que uma infraestrutura deve possuir por forma a processar IC.

e. Com base na avaliação o GNS pode estabelecer a necessidade de medidas adicionais de blindagem em função do grau de classificação da IC que é necessário manusear.

f. A avaliação de dispositivos eletrónicos de acordo com o Modelo de Zona é realizada em Laboratórios devidamente acreditados e de acordo com o Esquema de Avaliação e Certificação em Segurança Tecnológica de produtos e serviços habilitados para tratamento de IC.

g. O processamento de IC de grau igual ou superior a NACIONAL CONFIDENCIAL, requer a avaliação de dispositivos eletrónicos de acordo com o Modelo de Zona, ou a utilização de dispositivos de Baixa Radiação (*TEMPEST*).

7.2. REQUISITOS DE FILTRAGEM

a. A impedância da corrente elétrica deve estar normalizada para 50 ohms, devendo o sistema elétrico ser filtrado por um "*power TEMPEST filter*" que introduza uma atenuação de 60dB sobre o espectro de frequência entre 100kHz e os 1GHz, se abastecido por uma potência inferior a 100 kVA (kVA = Watts / (1.000 x fator de potencia).

b. Semelhantemente, todas as demais linhas condutoras que saiam de uma área controlada e sejam passiveis de ser fonte de fuga de informação, devem ser filtradas através da inserção de uma atenuação de 60dB.

c. Para garantir uma impedância diferente entre *RED/BLACK*, os equipamentos *RED* instalados em Áreas de Segurança de CLASSE 1 usadas para manusear Informação Classificada (IC), devem ser dotadas com um quadro elétrico próprio devidamente dimensionado.

d. Filtrar o nível de sinal das redes wireless não controladas, por forma a inserir uma atenuação suficiente para que o nível de sinal wireless seja inferior a -90dB.

e. Utilizar filtros de ferrite externos na ponta de cabos elétricos condutores que ligam os diferentes equipamentos, com uma impedância de 300 ohm a 100MHz.

f. Os elementos metálicos, tais como tubos de água, tubos de aquecimento, condutas de ar condicionado, etc., são propícios à propagação de sinais comprometedores. A sua continuidade elétrica deve, portanto, ser interrompida pela inserção de uma manga isolante colocada fora de qualquer zona de acoplamento e no interior do espaço inspecionável. O espaço de isolamento deve ter um comprimento mínimo de 10 centímetros.

g. Semelhantemente as condutas de ventilação que entram em áreas de segurança, devem estar protegidas por favos em ambas as extremidades, possuírem defletores de metal ou ductos em Z e filtros acústicos.

h. Deve ser garantido uma filtragem acústica igual ou superior a:

1) 56dB para Áreas de Segurança de CLASSE 1;
2) 53dB para Áreas de Segurança de CLASSE 2.

i. Deve ser garantida uma filtragem visual através da aplicação de peliculas opacas ou translucidas em janelas de forma a impossibilitar que do exterior se consiga ver para o interior, devendo as Áreas de Segurança de CLASSE 1 e de CLASSE 2 possuir as janelas protegidas por filme composto por multicamadas nanoabsorvente laminado para fazer face a possíveis tentativas de escuta por tecnologia baseada em laser.

7.3. REQUISITOS DE SEPARAÇÃO

a. As calhas técnicas devem segregar cabos de dados e cabos condutores elétricos conforme definido pela publicação SDIP 29/2 e *IA Security Guidelines on Selection and Installation of TEMPEST Equipment* – IASG 7-01.

b. As calhas técnicas ou condutas de cabos de energia devem distar em pelo menos 10cm de todas as outras condutas ou calhas técnicas de dados, conforme definido pela publicação SDIP 29/2 e *IA Security Guidelines on Selection and Installation of TEMPEST Equipment* – IASG 7-01.

c. Quando necessário for, as calhas técnicas/esteiras podem cruzar em ângulos retos, com uma separação de 15 cm em altura em relação aos cabos de energia.

d. Se a distância física entre condutores não for possível, deve ser demonstrado um nível de isolamento entre condutores equivalente a 60dB, a partir de 10kHz.

e. O nível de isolamento de um condutor pode ser aferido através de uma avaliação do cabo, ou através da inclusão de plano metálico entre os dois condutores.

f. Circuitos óticos devem assegurar que o cabo de fibra ótica não é blindado ou protegido por membrana metálica, funcionando como um condutor elétrico fortuito.

g. Um cabo de fibra ótica não pode ser utilizado para transportar informação *RED* e *BLACK*.

h. Dentro de um edifício os cabos que transportam informação RED entre diferentes pisos devem ser entubados em tubo semi-rígido de policloreto de vinilo (PVC) ou equivalente.

i. Se um cabo que transporta informação *RED* necessitar interligar diferentes edifícios dentro de um mesmo perímetro controlado, deve fazê-lo em tubo de policloreto de vinilo (PVC) ou equivalente, enterrado e através de caleira devidamente sinalizada.

j. Todos os cabos que necessitem sair perímetro controlado transportando informação RED ou que estejam acessíveis dentro do perímetro controlado a qualquer pessoa, devem estar entubados em tubo ou calha técnica metálica.

k. Deve existir um meio de acesso para inspeção elétrica de todos os caminhos de transmissão que saem de uma Área de Segurança.

l. Qualquer equipamento rádio (transmissor) deve distar pelo menos 200cm de qualquer equipamento não protegido que processe Informação Classificada (IC), conforme definido pela publicação SDIP 29/2 e *IA Security Guidelines on Selection and Installation of TEMPEST Equipment* – IASG 7-01.

m. Os equipamentos ativos que manuseiam diferentes marcas de segurança devem distar pelo menos 100cm, devendo observar-se uma distância de pelo menos 50cm entre equipamentos que processem diferentes Graus de IC, conforme definido pela publicação SDIP 29/2 e IA *Security Guidelines on Selection and Installation of TEMPEST Equipment* – IASG 7-01.

n. As ligações externas de operadores devem ser segregadas através da instalação de um conjunto de quadros *(frames)*, dispositivos ou bastidores, de acordo com:

1) um primeiro quadro (*frame*) ou bastidor para instalar os equipamentos externos de cada operador;
2) um segundo quadro (*frame*) ou bastidor para interligar o primeiro bastidor com a os sistemas internos;
3) um terceiro quadro (*frame)* ou bastidor para distribuir a cablagem interna de modo vertical/horizontal.

o. Não devem ser utilizadas ligações cruzadas entre quadros (*frame*) ou bastidores internos e externos, devendo ser utilizados apenas quadros (*frame*) ou bastidores internos para distribuir ligações a equipamentos terminais.

p. A utilização de redes *wireless* deve segregar entre redes controladas e redes não controladas.

q. A utilização de redes *wireless* controladas deve segregar utilizadores corporativos dos demais utilizadores e desinibir a propagação do identificador do conjunto de serviços (*service set identifier* (*SSID*)).

r. Não se utilizam redes wireless para manuseamento de Informação Classificada.

s. Devem ser separadas as diferentes redes de controlo e manutenção ambiental, composta por sensores de presença, de incêndio/fumos e outros equipamentos congéneres, das restantes redes de dados classificados.

t. As redes que processam IC devem ser segregadas e completar a instrução de um processo de acreditação de segurança.

7.4. REQUISITOS DE PROTEÇÃO

a. A Terra de Proteção é um condutor que serve como proteção contra emanações comprometedoras, descargas elétricas e como potencial de referência (0V) para circuitos elétricos e eletrónicos e não deve conduzir corrente elétrica.

b. O elétrodo de Terra deve ser instalado dentro do perímetro controlado e espaço inspecionável.

c. Os dispositivos eletrónicos que processam informação *BLACK* devem ser ligados à Terra de Proteção fornecida pelo distribuidor comercial.

d. Os dispositivos eletrónicos que processam Informação Classificada (RED) devem ser ligados a um plano de Terra, diferenciado, dentro do perímetro controlado.

e. O plano de Terra deve ter pelo menos 1m para cada lado em relação à área plana usada por dispositivos eletrónicos RED.

f. Todos os artefactos metálicos, dispositivos e bastidores RED devem ser ligados ao plano de Terra RED.

g. A resistência entre o equipamento RED e o plano de Terra deve ser inferior a 2 ohms.

h. Os equipamentos RED usados para manusear IC devem ser protegidos por interruptores e disjuntores diferenciais sensíveis a uma corrente residual de 30mA.

i. Todos os condutores fortuitos que entram numa área de segurança (condutas de água, condutas de ar, equipamentos de ar condicionado, cabos de energia elétrica, telecomunicações, etc.), devem estar devidamente isolados.

1) Condutores metálicos: através da instalação de uma união dielétrica adjacente à penetração do tubo através da parede perimetral (parede interna), ou através da ligação do condutor metálico ao sistema de proteção de terra do edifício.
2) Tubos metálicos com aspersores (*sprinklers*) (supressão de incêndio): devem estar ligados ao sistema de proteção de Terra do edifício.
3) Linhas de refrigeração de um sistema mecânico: devem estar ligados ao sistema de proteção de Terra do edifício.

j. Devem ser seguidas as Regras Técnicas das Instalações Elétricas de Baixa Tensão (RTIEBT) (conforme legislado na Portaria n.º 949-A/2006 de 11 de setembro).

7.5. REQUISITOS DE CONTROLO

a. Deve existir um inventário/cadastro de todos os equipamentos existentes num dado espaço, identificados pelo menos por modelo, número de série e quantidade;

b. Deve existir um cadastro de toda a cablagem elétrica e de dados em função de pelo menos: o tipo de cabo, origem-destino, função e classificação;

c. Deve existir um cadastro das frequências usadas para quaisquer comunicações eletrónicas, incluindo os serviços de *broadcast* de televisão e as comunicações móveis;

d. Deve ser restringido o acesso de equipamentos pessoais de computação e de comunicações moveis a Áreas de Segurança;

e. Devem ser disponibilizados armários de cacifos para depósitos de aparelhos eletrónicos com chave individual;

f. Devem ser seguidas as Prescrições e Especificações Técnicas das Infraestruturas de Telecomunicações em Edifícios do *MANUAL ITED* v.4;

g. Deve ser implementado um plano de monitorização e avaliação de segurança anual, devendo o relatório ser arquivado de acordo com o seu grau de classificação.

8. REVISÃO DA PRESENTE NORMA

A manutenção da presente norma é da responsabilidade da Equipa Multidisciplinar de Segurança Digital, Tecnológica e de Infraestruturas, a quem cabe sempre que se tornar exigível ou a cada período de 3 anos proceder à sua revisão e atualização.

9. ACRÓNIMOS

ANS – Autoridade Nacional de Segurança

BSI – *Federal Office for Information Security*

CISPR – *International Special Committee on Radio Interference*

EMI – Interferência eletromagnética não-intencional (EMI)

EMSEC – Segurança de Emanações Eletromagnéticas (EMSEC)

EU/EU – União Europeia / *European Union*

GNS – Gabinete Nacional de Segurança

IC – Informação Classificada

IEMI – Interferência Eletromagnética Intencional

ITU – *International Telecommunication Union*

OTAN/NATO – Organização do Tratado do Atlântico Norte / *North Atlantic Treaty Organization*

NT – Norma Técnica

SDIP – *SECAN Doctrine and Information Publication*

SE – *Shielding Effectiveness*

SI – Sistemas de Informação

SIC – Sistemas de Informação e de Comunicação

TEMPEST – *Telecommunications Electronics Material Protected from Emanating Spurious Transmissions*

TIC – Tecnologias de Informação e Comunicação

10. ANEXOS

Anexo A – Noções elementares de propagação e influência das ondas eletromagnéticas;

Anexo B – Noções elementares de blindagem (*Shielding*)

Anexo C – Noções elementares de filtragem (*Filtering*)

Anexo D – Noções elementares de separação (*Crosstalk*)

Anexo E – Métodos de mitigação de fuga de informação em computadores

Anexo F – Relação custo-benefício do *Federal Office* for *Information Security* alemão (BSI)

Anexo G – Valores mínimos e máximos de atenuação a observar em infraestruturas e equipamentos [RESERVADO]

11. LISTA DE DISTRIBUIÇÃO

Geral

ANEXO A – NOÇÕES ELEMENTARES DE PROPAGAÇÃO E INFLUÊNCIA DAS ONDAS ELETROMAGNÉTICAS

a. Do ponto de vista físico, as ondas eletromagnéticas propagam oscilações no campo eletromagnético, caracterizando-se como ondas de rádio, radiação infravermelha, luz visível, radiação UV, raios X e raios gama. No contexto desta norma, apenas as ondas radio são relevantes.

b. O surgimento das ondas eletromagnéticas é explicado pelas equações de *Maxwell*. Afirmam estas que cada mudança temporal no campo elétrico está sempre ligada a uma mudança espacial no campo magnético. Da mesma forma, cada mudança no campo magnético ao longo do tempo está, por sua vez, ligada a uma mudança espacial no campo elétrico. Para campos que mudam periodicamente (em particular sinusoidalmente), esses efeitos juntos resultam em uma onda eletromagnética que se propaga no espaço.

c. Além de uma frequência característica, todo o campo eletromagnético possui um comprimento de onda, sendo a relação entre a frequência (f) e o comprimento de onda (λ) dada pela velocidade da luz (c)

$$c = \lambda \cdot f$$

d. As ondas eletromagnéticas surgem quando um campo elétrico ou magnético muda ao longo do tempo.

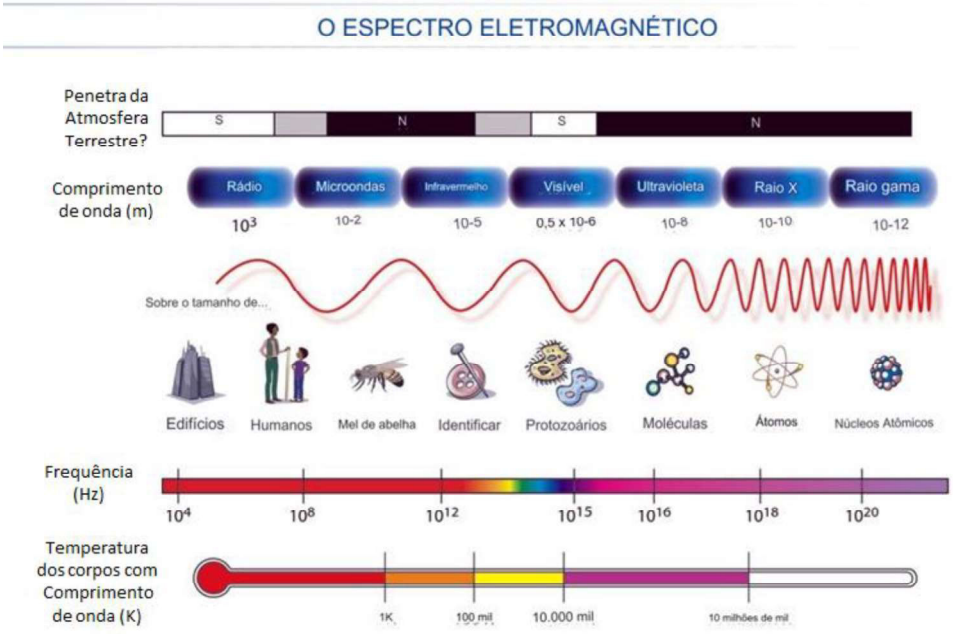

Figura A1 – Tipos de ondas eletromagnéticas

e. A polarização descreve a direção do vetor do campo elétrico de uma onda eletromagnética. Existem diferenças entre um campo polarizado linearmente e um campo polarizado circularmente. Com a polarização linear, o vetor do campo elétrico oscila em uma direção espacial fixa. O vetor de campo magnético resultante é sempre gerado 90° em comparação com o vetor elétrico conforme Figura A2.

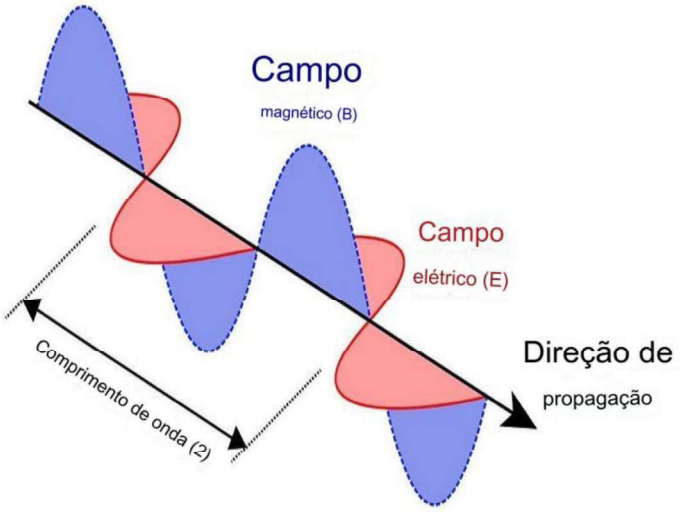

Figura A2 – Polarização de ondas eletromagnéticas

f. No caso de uma onda eletromagnética polarizada circularmente, o campo é gerado por dois ou mais vetores de campo elétrico que são desfasados um em relação ao outro e que fazem com que o vetor de campo resultante corra sobre uma elipse. Um círculo é formado se os vetores do campo elétrico tiverem a mesma magnitude e houver um deslocamento de fase de 90°.

g. A polarização é fundamental para a medição de campos elétricos, pois a máxima potência de transmissão (sem atenuação) só é alcançada se a antena recetora for polarizada da mesma forma que o campo eletromagnético. Em contraste, do ponto de vista teórico nenhuma potência pode ser transmitida (atenuação infinita) no caso da polarização oposta.

h. O caminho ao longo do qual uma onda eletromagnética se propaga é chamado de caminho de acoplamento. Apesar de uma onda eletromagnética não necessitar de um meio material, a sua propagação é, no entanto, fortemente influenciada pelo seu ambiente.

i. Materiais com elevadas propriedades elétricas ou magnéticas afetam a propagação de ondas eletromagnéticas, observando-se que na faixa de frequências de 30 MHz a 10 GHz a boa condutividade de todos os metais tem um efeito particularmente forte.

j. Dependendo da frequência e da condutividade, se o metal for suficientemente espesso, a onda pode ser completamente refletida pela profundidade de penetração.

k. A existência de ondas estacionárias com direção oposta de propagação, amplifica ou reduz a intensidade do campo resultante, dando origem a uma interferência. De forma geral a interferência de objetos puramente metálicos no campo eletromagnético promove a retenção de energia por via da reflexão.

l. Todas as ondas eletromagnéticas de qualquer faixa de frequência influenciam os dispositivos eletrónicos, assim como, os sistemas biológicos.

m. As ondas eletromagnéticas emitidas por dispositivos eletrónicos são geralmente indesejáveis (com exceção para os dispositivos transmissores criados com o intuito de emanar) e dependendo da faixa de frequência e intensidade podem influenciar outros dispositivos eletrónicos, prejudicando o seu funcionamento e dando origem a interferência.

n. O Decreto-Lei n.º 31/2017 de 22 de março, transpõe para a ordem jurídica nacional, a Diretiva n.º 2014/30/UE, do Parlamento Europeu e do Conselho, de 26 de fevereiro 2014, estabelecendo as regras aplicáveis à compatibilidade eletromagnética dos "dispositivos que podem causar interferência eletromagnética ou cujo funcionamento pode ser afetado por interferência" e regulando os requisitos de "compatibilidade eletromagnética" de dispositivos.

o. De acordo com esta lei, os dispositivos devem ser concebidos de tal forma que "a geração de interferência eletromagnética seja limitada a tal ponto que os dispositivos de rádio e telecomunicações e outros dispositivos possam funcionar conforme pretendido". Os valores-limite para a radiação de interferência eletromagnética permitida de dispositivos eletrónicos são especificados na norma europeia de produtos EN 55022.

p. Os valores limite para produtos certificados como *TEMPEST* são significativamente inferiores aos valores limite dos padrões de produtos EMC, de modo que um dispositivo compatível com EMC geralmente não é protegido automaticamente contra emissões comprometedoras.

q. Por questões de segurança eletrónica, todos os dispositivos, utilizados para processamento de informação classificada, devem cumprir com os limites de emanação definidos.

ANEXO B – NOÇÕES ELEMENTARES DE BLINDAGEM (SHIELDING)

a. O objetivo da blindagem eletromagnética é eliminar os caminhos de acoplamento das ondas eletromagnéticas.

b. O efeito da blindagem é recíproco, ou seja, a proteção contra a entrada de campos fornece simultaneamente proteção contra campos emergentes, permitindo que um dispositivo eletrónico seja protegido contra interferência externa, mas também contra a emanação do próprio dispositivo para o exterior.

c. Quando uma onda eletromagnética atinge uma parede, a onda é refletida em maior ou menor extensão, dependendo das propriedades eletromagnéticas do material. A porção da onda que não é refletida penetra no material (transmissão), sendo ali parcialmente absorvida. (ver Figura B1).

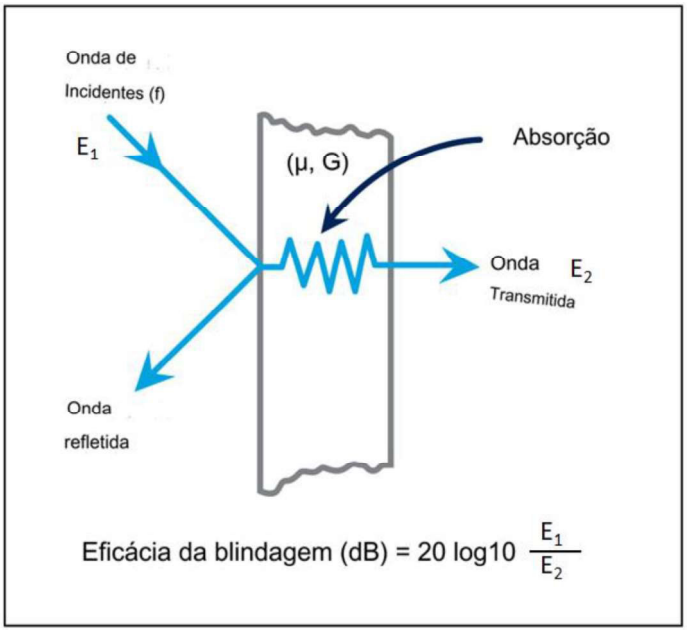

Figura B1 – Ilustração dos princípios de blindagem

d. Uma blindagem eficaz pode ser alcançada através da capacidade de reflexão ou da qualidade de absorção do material de construção.

e. As qualidades de reflexão e absorção de materiais ou estruturas dependem fortemente da frequência e das propriedades elétricas ou magnéticas do material.

f. Para proteger um campo eletromagnético, a escolha do material de blindagem ideal depende da componente magnética ou elétrica que seja predominante no campo a ser blindado. Esta propriedade do campo é descrita pela chamada resistência da onda de campo.

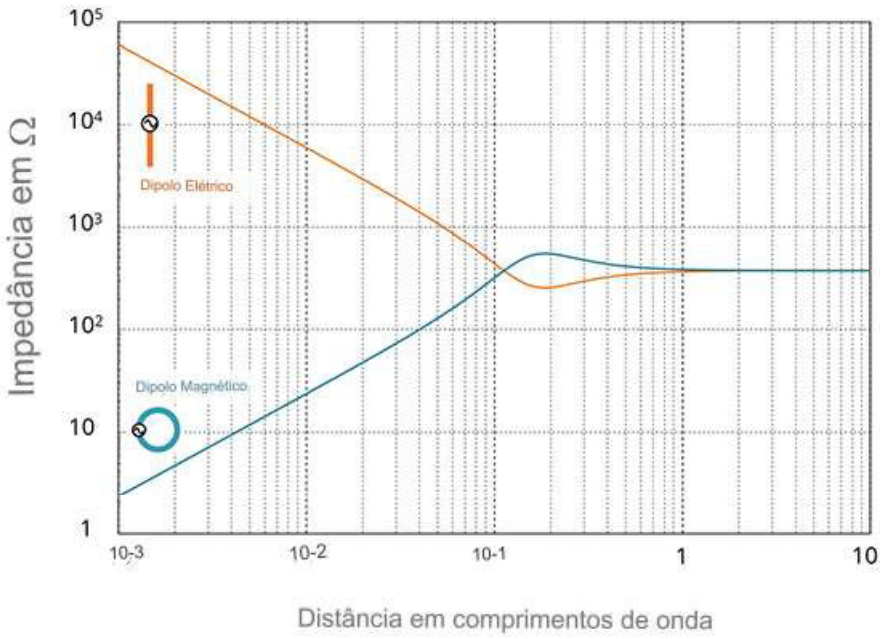

Figura B2 – Ilustração dos princípios de blindagem

g. Com um dipolo elétrico, a resistência da onda do campo é muito alta no campo próximo (campo de alta impedância), com um dipolo magnético é muito baixa (campo de baixa impedância). No campo distante aproxima-se do valor constante de aproximadamente 377 ohms para ambos os tipos de dipolo.

h. No caso de campos de baixa impedância, o efeito de blindagem de um material é determinado pela sua condutividade magnética (permeabilidade), sendo exemplos os materiais de ferro ou ferrite que possuem uma elevada permeabilidade.

i. Por outro lado, materiais com elevada condutividade elétrica (principalmente metais) são necessários para uma blindagem eficaz de campos de alta impedância

j. Para frequência acima de 30MHz (correspondente a um comprimento de onda de 10 m), o campo distante possui uma impedância de campo de 377 ohms, a uma distância de 1,6 m, independentemente da fonte da radiação ser de natureza elétrica ou magnética. Nesta faixa de frequência, a alta condutividade é mais eficaz do que a alta permeabilidade

k. O fator de blindagem (S) de uma estrutura é definido como a razão entre a potência do campo penetrante com blindagem e a potência da radiação penetrante sem blindagem, utilizando-se normalmente uma representação logarítmica. A eficácia da blindagem (SE) é medida em decibéis [dB].

Atenuação blindagem SE em dB	Proporção de potência de campo penetrante	Grau de blindagem em %
0	1/1	0
3	1/2	50
6	1/4	75
7	1/5	80
10	1/10	90
13	1/20	95
16	1/40	97,5
20	1/100	99
30	1/1.000	99,9
40	1/10.000	99,99
50	1/100.000	99.999
60	1/1.000.000	99.9999
70	1/10.000.000	99,99999
80	1/100.000.000	99,999999

Figura B3 – Relação entre atenuação da blindagem e grau de blindagem

l. A eficácia da blindagem é normalmente determinada por:

$$\mathbf{SE_{(dB)} = {}_{20}log\ E1\ /E2\ (dB)}$$

1) E1 é o valor do Campo Elétrico (μV/m) sem blindagem

2) E2 é o valor Campo Elétrico (μV/m) com blindagem

m. A qualidade da reflexão é alcançada através de:

1) Blindagem feita de materiais com alta condutividade (cobre, alumínio, aço)

2) Estrutura superficial ou entrelaçada, feita de materiais condutores em malha pequena.

$(m<\lambda/2)$

n. A qualidade de absorção é alcançada por:

1) Alto número de interfaces no meio (poros, agregados, paredes)

2) Baixa condutividade

3) Elevadas permeabilidade e permissividade

o. Neste sentido a eficácia da blindagem também pode ser determinada por:

$$\mathbf{SE_{(dB)} = R + A + M\ (dB)}$$

1) **R** é o valor da atenuação devido à reflexão

$$\mathbf{R(dB) = 168 + 10log(@/\mu * f)\ (dB)}$$

a) @ é o valor da condutividade

b) **μ** é o valor da permeabilidade

c) f é o valor da frequência

2) **A** é o valor da atenuação devido à absorção

$$R_{(dB)} = 131{,}4 * t + \sqrt{(f * @ * \mu)}\ (dB)$$

a) **t** é o valor para a espessura

b) **@** é o valor da condutividade

c) **μ** é o valor da permeabilidade

d) f é o valor da frequência

3) **M** é o valor do termo de correção de reflexão múltipla (na maioria das situações práticas o valor de M é negligenciável)

p. Em resumo, a eficácia da blindagem, depende altamente de:

1) material fino para blindar o campo elétrico;

2) material espesso para blindar o campo magnético;

3) a polarização do campo eletromagnético;

4) as propriedades elétricas, magnéticas e dielétricas dos materiais;

5) especialmente o conteúdo de água no material;

6) o número, tamanho, orientação e posição de aberturas e atravessamentos no material.

ANEXO C – NOÇÕES ELEMENTARES DE FILTRAGEM (FILTERING)

a. As entidades reguladoras asseguram que os valores-limite para a radiação de interferência eletromagnética permitida por cada dispositivos eletrónicos é mantida em conformidade com a norma europeia EN 55022, garantindo desta forma que os dispositivos eletrónicos funcionam corretamente sob um determinado nível de ruído limite, que por sua vez atesta um nível de proteção de segurança eletrónica adequada.

b. Para controlar o nível de ruido a quase totalidade dos dispositivos eletrónicos encontram-se incorporados com filtros de proteção contra a interferência eletromagnética não-intencional (EMI).

c. O filtro EMI é um componente eletrónico que suprime o ruído eletromagnético produzido por uma fonte de energia, normalmente usado em conjunto outros tipos de proteção, como é o caso da blindagem.

d. Os filtros EMI podem ser classificados como passa-baixa, passa-alta, passa-banda ou de rejeição de banda.

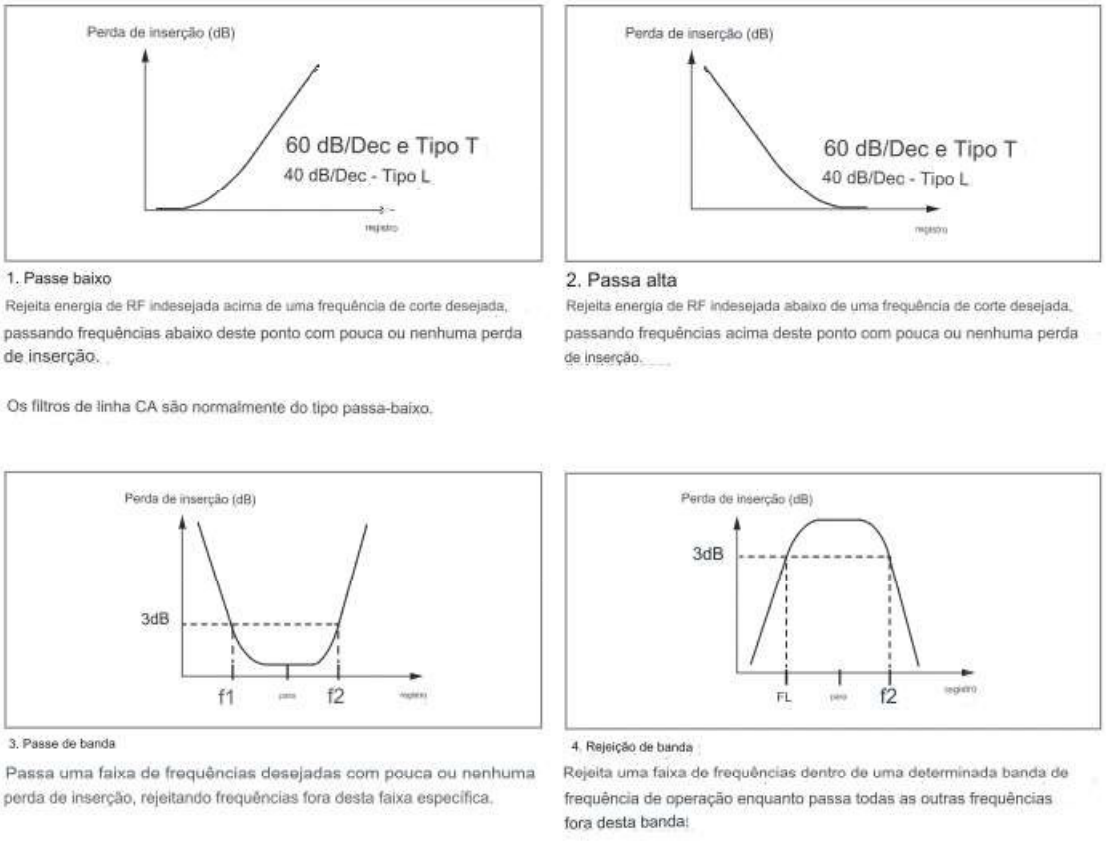

Figura C1 – Tipo de filtros

e. A filtragem de circuitos elétricos assenta na incompatibilidade de impedâncias, aferida pelo nível de atenuação inserido num dado circuito, pelo que os filtros EMI assentam geralmente em componentes passivos como condensadores e indutores.

f. Os indutores, em um filtro EMI, permitem a passagem de sinais de baixa frequência, mas bloquearão componentes indesejados de alta frequência. Os condensadores direcionarão o ruído de alta frequência através de um caminho de baixa impedância de volta para a terra de proteção da fonte de alimentação ou do sistema.

g. Semelhantemente aos dispositivos eletrónicos, as linhas de alimentação possuem diferentes problemas para os quais requerem filtragem, como sejam a existência de elementos parasitas, perdas de correntes, saturação, desalinhamento de impedâncias, que podem provocar interferência por via da condução elétrica.

h. Para uma filtragem eficaz é necessário proceder a um leitura e avaliação de todas as frequências existentes num dado espaço ou equipamento.

i. Como procedimento para avaliar o desempenho de um filtro, aconselha-se a utilização da norma CISPR 17 "*Methods of measurement of the suppression characteristics of passive radio interference filters and suppression components*", ou a norma *MIL-STD-220B "Method of insertion loss measurement"*.

ANEXO D – NOÇÕES ELEMENTARES DE SEPARAÇÃO (CROSSTALK)

a. O objetivo da separação é reduzir o risco de transferência indesejada de sinais entre diferentes canais de comunicação (CROSSTALK).

b. A suscetibilidade do cobre a interferências e ruídos tem sido um fator importante que limita a sua utilização, podendo ter um grande impacto na fiabilidade de qualquer ligação, no rendimento dos serviços implementados e na capilaridade que pode ser disseminada.

c. Interferência eletromagnética (EMI) é uma das fontes comuns de ruído em ambiente com elevada densidade de cablagem em cobre, potenciando a ocorrência de efeitos de *side-channel* que permitem a coletar informação ou a influencia sobre a operação de um sistema.

d. Os efeitos de *side-channel* ocorrem quando um sinal transmitido por um par trançado de cobre irradia e interfere ou degrada a transmissão em outro par, existindo diferentes efeitos conforme imagem em baixo.

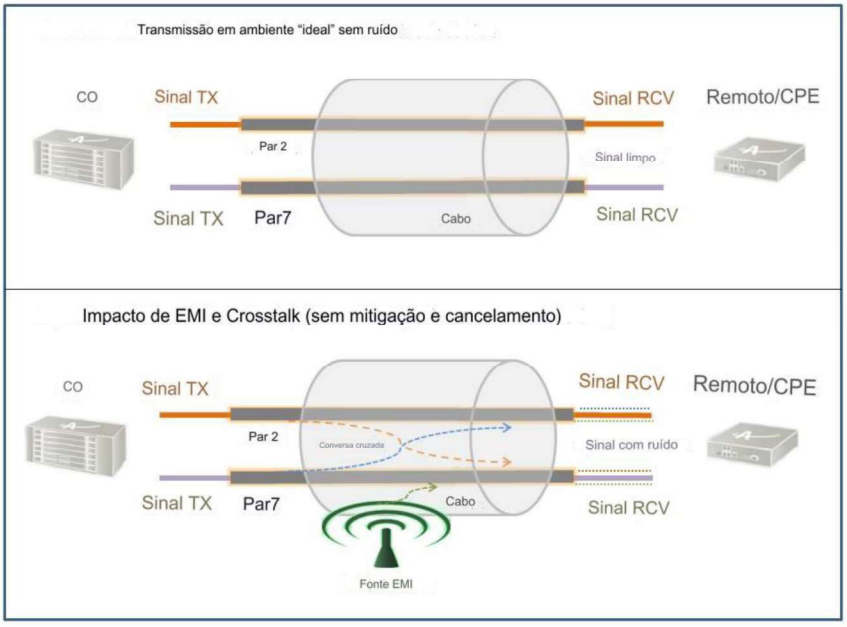

Figura D1 – Efeitos *Side-Channel*

e. A separação depende das propriedades resistivas, indutivas, capacitivas e condutoras de cada componente de um circuito elétrico, sendo necessário por exemplo o distanciar os diferentes condutores RED e BLACK.

f. Embora não exista uma implementação completamente livre de canais laterais, devem ser tomadas medidas adequadas para garantir que um eventual ataque seja praticamente inviável.

ANEXO E – MÉTODOS DE MITIGAÇÃO DE FUGA DE INFORMAÇÃO EM COMPUTADORES

a. A publicação ITU-T K.115 - *Mitigation methods against electromagnetic security threats*, dá conta de um conjunto de contramedidas que podem ser aplicadas a um computador para evitar a fuga de informação por ação de emanações comprometedoras.

b. Conforme anteriormente descrito no ponto 15., as contramedidas ora assentam na redução de sinal e ou na geração de ruído, procurando alterar a relação sinal-ruído (SNR) do recetor.

c. A utilização de computadores gera campos elétricos, magnéticos e eletromagnéticos que dependem fortemente da tecnologia utilizada. Por exemplo: uma unidade de disco rígido (HDD) utiliza campos magnéticos para armazenar dados e, portanto, emite campos magnéticos de baixa frequência; as unidades de estado sólido (SSD), ao contrário, não emitem esses campos porque a tecnologia de armazenamento é baseada em semicondutores. A fonte de alimentação, o monitor ou módulos de rede para comunicação sem fio, como WLAN ou Bluetooth geram igualmente campos.

d. A figura A dá conta das contramedidas aplicadas a equipamentos computacionais:

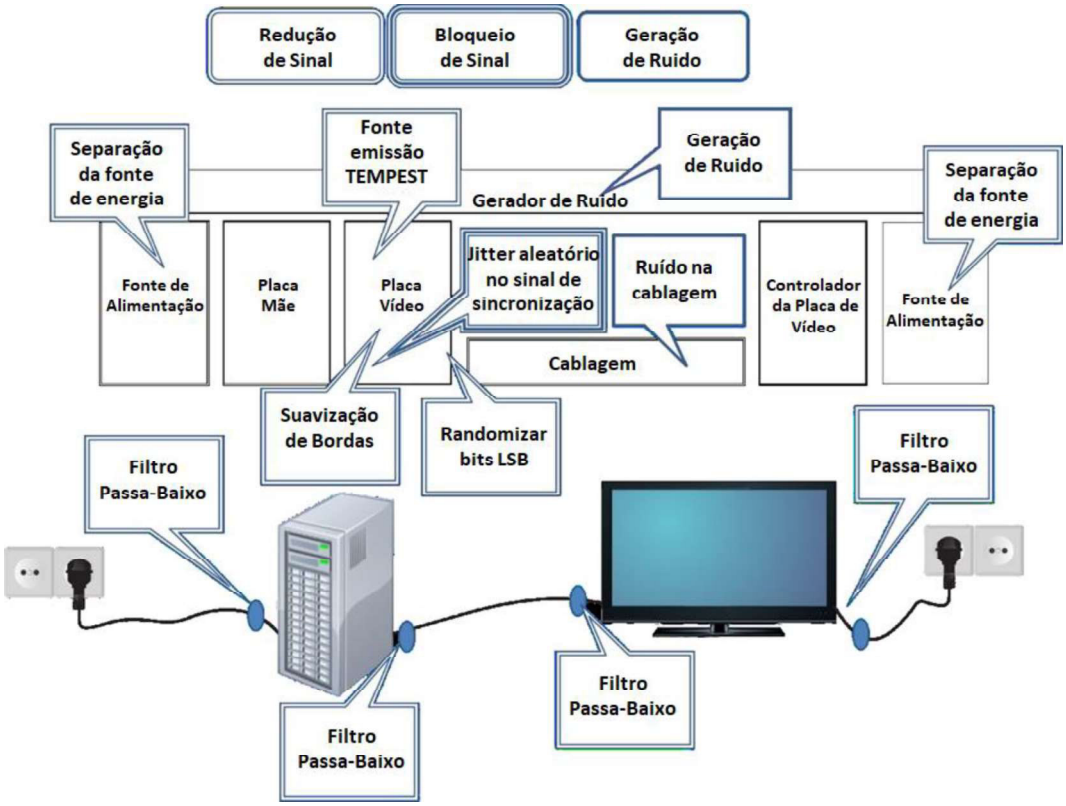

Figura E1 – Medidas de mitigação para um sistema computacional fixo

e. Semelhantemente um *laptop* é uma versão portátil de um PC e combina o computador com monitor, rato e teclado num único dispositivo. A fonte de alimentação é normalmente combinada com um cabo de carregamento encontrando-se, portanto fora do *laptop*, pelo que as principais contramedidas dizem respeito ao controlo dos interfaces externos disponibilizados pelo dispositivo.

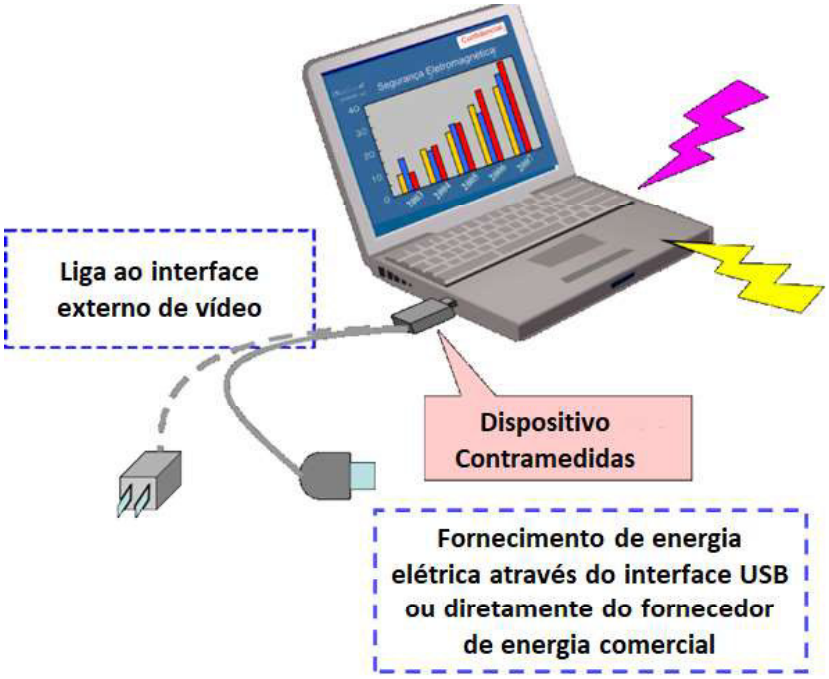

Figura E2 – Medidas de mitigação para um sistema computacional portátil

ANEXO F – RELAÇÃO CUSTO-BENEFÍCIO DO FEDERAL OFFICE FOR INFORMATION SECURITY ALEMÃO (BSI)

a. Segundo um estudo do *Federal Office for Information Security* alemão (BSI) 12, os custos da aplicação de medidas de blindagem num espaço de 20m2 acrescem cerca de 24.300,00€[13] ao projeto, sendo até três vezes mais caras se aplicadas posteriormente;

b. Por seu turno, a criação de uma câmara blindada (*Faraday*), com um nível de proteção contra campos eletromagnéticos igual ou superior a 80dB, representa um investimento superior a 30.400,00€[14].

c. Semelhantemente, um dispositivo eletrónico *TEMPEST* requer 100% de esforço adicional em relação ao preço de compra, observando-se que os dispositivos eletrónicos projetados de acordo com o Modelo de Zona representam apenas um acréscimo de 20% de custos relacionados com a reparação ou atualização dos dispositivos, a cada três ou quatro anos.

d. Neste sentido, observa-se que por um lado o investimento em blindagem oferece uma vida útil relativamente mais longa, apesar de um nível de investimento inicial mais elevado. Por outro lado, o investimento em dispositivos eletrónicos, apesar do menor investimento inicial e maior flexibilidade, apresenta custos de manutenção adicionais maiores.

e. Como linha orientadora, o BSI, definiu uma medida de custo-benefício assente em:[15]

1) Se a estimativa de custos com a aquisição de um sistema de informação e de comunicação (SIC) for superior a 4.900€[16], é preferível a implementação de medidas estruturais em função do Modelo de Zona, em vez da aplicação de dispositivos eletrónicos de baixa radiação (*TEMPEST*);
2) Se o custo do sistema de informação e de comunicação (SIC) for superior a 8.500€[17], o planeamento de medidas de blindagem é preferível.

---

[12] BSI TR-03209 – 2 - Blindagem eletromagnética de edifícios, acedido através de http://www.bsi.bund.de, em 05/09/2023.
[13] Valor de 20.000€ em 2008, atualizado em termos de inflação, de acordo com o Portal PORDATA cujo linke é: https://www.pordata.pt/simulador-inflacao-quanto-vale-hoje-o-dinheiro-do-passado.
[14] Valor de 25.000€ em 2008, atualizado em termos de inflação, de acordo com o Portal PORDATA cujo linke é: https://www.pordata.pt/simulador-inflacao-quanto-vale-hoje-o-dinheiro-do-passado.
[15] idem
[16] Valor de 4000€ em 2008, atualizado em termos de inflação, de acordo com o Portal PORDATA cujo linke é: https://www.pordata.pt/simulador-inflacao-quanto-vale-hoje-o-dinheiro-do-passado.
[17] Valor de 7000€ em 2008, atualizado em termos de inflação, de acordo com o Portal PORDATA cujo linke é: https://www.pordata.pt/simulador-inflacao-quanto-vale-hoje-o-dinheiro-do-passado.