A
PREFEITURA MUNICIPAL DE GUARAPAI
(Secretária Municipal de Educação – SEMED)
ESTADO DO ESPÍRITO SANTO

COMISSÃO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 003/2024
PROCESSO ADMINISTRATIVO Nº 5.372/2024

A empresa SPEED TECNOLOGIA EIRELI, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº. 34.289.656/0001-98, sediada na rua Santiago Dantas, nº 49 (térreo), bairro Nossa Senhora da Penha, cidade de Vila Velha, estado do Espírito Santo, CEP 29.110-230, participante do certame referido certame, na data de 13 (treze) do mês de maio deste ano corrente (2024 – dois mil e vinte e quatro), na modalidade de pregão eletrônico, sendo o mesmo disputado na plataforma www.portaldecompraspublicas.com.br. Sob condução da pregoeira Rosiani Emilia Cansi.

Razão Social: SPEED TECNOLOGIA EIRELI
CNPJ: 34.289.656/0001-98
Endereço: Rua Santiago Dantas, nº 49
Bairro: Nossa Senhora da Penha
Cidade: Vila Velha - ES
CEP: 29.110-230 **Telefone: (**27**)** 3020-1802
E-mail: speed.operacional03@gmail.com

Identificação do Representante Legal:
Nome do representante legal para assinatura da Ata: Jorge Vasconcelos Correa
CPF: 998.049.377-06 / **Identidade:** 831.904-SPTC/ES
Residência: Rua 299, nº 36, Vila Nova, Vila Velha – ES – CEP: 29.105-161
Cargo na Empresa: Sócio Proprietário.
Dados Bancários: Banco: SICOOB - Agência: 3008 - Conta Corrente: 118.144-0

RAZÃO

Após declaração do fornecedor licitante "3D PROJETOS E ASSESSORIA EM INFORMÁTICA LTDA" como VENCEDORA/ARREMATANTE, cuja a mesma propôs como solução de atendimento as exigências descritas no termo de referência "ANEXO I – páginas 25 à 34), a solução LENOVO THINKCENTRE NEO 50S GEN 4, como computador desktop.

Acontece que no descritivo do termo de referência está sendo exigido que a solução proposta deve possuir TPM 2.0 (páginas 26,34, 34 e 58).
O TPM (Trusted Platform Module) é um microcontrolador que armazena chaves, senhas e certificados digitais. Ou seja, um recurso essencial para questões de segurança do equipamento e dados armazenados nele (https://learn.microsoft.com/pt-br/windows/security/hardware-security/tpm/tpm-fundamentals).

As versões do TPM através de Firmware e ou discreto, tem recursos limitados ao serem comparados com o CHIP INTEGRADO a placa do equipamento, se tornando então o recurso de TPM discreto e firmware inferiores ao chip integrado.

E quando o edital solicita em seus termos que a solução proposta "DEVERÁ POSSUIR TPM 2.0 OU SUPERIOR" é entendido que a instituição esta visando que o equipamento a ser proposto deverá possuir recursos de segurança nativo, ou seja, o CHIP nativo/integrado ao equipamento contemplado todos os recursos e suas funcionalidades.

DO FATO

FATO 01 – Conforme as documentações apresentadas pelo fornecedor licitante declarado como arrematante, sendo possível identificar nos arquivos "ThinkCentre_neo_50s_Gen_4_DataSheet e ThinkCentre_neo_50s_Gen_4_Spec". A solução proposta possui a funcionalidade TPM na versão DISCRETA. Que ao ser comparada com o chip integrado não possui todos os recursos e funcionalidades, conforme as literaturas anexas a este pedido.
Entendendo que a segurança é algo de extrema importância, e devido a falta de dos recursos e funcionalidades, o equipamento proposto (ThinkCentre NEO 50s Gen 4) não atende as exigências solicitadas.

FATO 02 – A diferença entre os meios/versões do TPM aplicadas ao equipamento, impactam diretamente o valor do equipamento proposto, onde os equipamentos com versões inferiores aos equipamentos que possui o CHIP nativo/integrado com todas as suas funcionalidades.

FATO 03 – O laudo de avaliação de amostra emitido pela comissão técnica designada para analise deste processo, pode não ter observado a exigência que esta sendo questionada, confrontando os recursos e funcionalidades. Por este motivo foi considerado como APROVADO o equipamento.

DO PEDIDO

Por meio deste solicitamos que seja refeita a avaliação do equipamento proposto/ofertado pelo fornecedor licitante arrematante, permitindo que esta avaliação seja acompanhada por um representante de nossa empresa, para que seja validado todos os procedimentos de avaliação física e técnica do equipamento e todos os seus recursos e funcionalidades.
Dando ênfase as funções de seguranças referente aos recursos do TPM na versão 2.0.

Diante da possibilidade real de não atendimento do equipamento conforme as literaturas descritas sobre o TPM, seja refeito o laudo do equipamento, atestando que o mesmo não atende as exigências editalícias descritas no termo de referência.

Em seguida, solicitamos a desclassificação da solução proposta e que seja convocado o próximo classificado para que apresente as suas soluções, documentações e equipamento para a devida avaliação.

Certo de que todos os pontos e questões aqui apresentados serão criteriosamente analisados. Ficamos no aguardo do parecer desta comissão de julgamento.

Sem mais para o momento.

JORGE VASCONCELOS CORREA:99804930706

Assinado digitalmente por JORGE VASCONCELOS CORREA:99804930706
DN: C=BR, O=ICP-Brasil, OU=50214482000150, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A1, OU=(EM BRANCO), OU=videoconferencia, CN=JORGE VASCONCELOS CORREA:99804930706
Razão: Eu sou o autor deste documento
Localização: 2022
Data: 2024.07.18 14:19:25-03'00'
Foxit PDF Reader Versão: 11.2.2

Vila Velha/ES, 18 de julho de 2024.

SPEED TECNOLOGIA EIRELI
34.289.656/0001-98
Jorge Vasconcelos Correa
Sócio Proprietário
RG nº 831.904-SPTC
CPF: 998.049.307-06

34.289.656/0001-98
SPEED TECNOLOGIA EIRELI
Rua Santiago Dantas, 49 - N. Sra. da Penha
CEP 29.110-230 - VILA VELHA - ES

3º ALTERAÇÃO CONTRATUAL
SPEED TECNOLOGIA EIRELI

Pelo presente instrumento particular, o abaixo assinado:

JORGE VASCONCELOS CORREA, brasileiro, natural de Cariacica/ES, solteiro, empresário, nascido em 03/06/1970, inscrito no CPF sob o n°. 998.049.307-06 e no RG n°. 831.904 SPTC/ES, residente e domiciliado na Rua Vinte e Nove, nº 36, Bairro Vila Nova, Vila Velha, Estado do Espírito Santo, CEP 29.105-161, na condição de titular da empresa.

A empresa gira sob o nome empresarial de **SPEED TECNOLOGIA EIRELI**, registrada na JUCEES sob o NIRE Nº 32600264935, inscrita no CNPJ/MF n°. 34.289.656/0001-98 **(artigo 997, II, CC/2002),** com sede localizada na Rua Regente Feijó, nº 434, anexo 1, Bairro Nossa Senhora da Penha, Vila Velha, Estado do Espírito Santo, CEP: 29.110-160 **(artigo 997, II, CC/2002)**, Resolve alterar o seu Ato Constitutivo de Eireli, mediante as cláusulas e condições a seguir:

Cláusula Primeira:

O endereço da sede da empresa passa a ser**: Rua Santiago Dantas, Nº 49, Térreo, Bairro Nossa Senhora da Penha, Vila Velha/ES, CEP: 29.110-230.**

Em face das modificações ora ajustadas, **CONSOLIDA-SE** o Ato Constitutivo:

3º ALTERAÇÃO CONTRATUAL – CONSOLIDADA
SPEED TECNOLOGIA EIRELI

Pelo presente instrumento particular, o abaixo assinado:

JORGE VASCONCELOS CORREA, brasileiro, natural de Cariacica/ES, solteiro, empresário, nascido em 03/06/1970, inscrito no CPF sob o n°. 998.049.307-06 e no RG n°. 831.904 SPTC/ES, residente e domiciliado na Rua Vinte e Nove, nº 36, Bairro Vila Nova, Vila Velha, Estado do Espírito Santo, CEP 29.105-161, na condição de titular da empresa.

A empresa gira sob o nome empresarial de **SPEED TECNOLOGIA EIRELI**, registrada na JUCEES sob o NIRE Nº 32600264935, inscrita no CNPJ/MF n°. 34.289.656/0001-98 **(artigo 997, II, CC/2002),** com sede localizada na Rua Santiago Dantas, Nº 49, Térreo, Bairro Nossa Senhora da Penha, Vila Velha, Estado do Espírito Santo, CEP: 29.110-230 **(artigo 997, II, CC/2002)**, e será regida pelas seguintes condições e cláusulas:

Cláusula Primeira: A empresa poderá, a qualquer tempo, abrir ou fechar filial ou outra dependência, mediante alteração do ato constitutivo.

Cláusula Segunda: A empresa terá por objeto as seguintes atividades econômicas:

80.20-0-01 - Atividades de monitoramento de sistemas de segurança eletrônico;
26.21-3-00 - Fabricação de equipamentos de informática;
35.30-1-00 - Produção e distribuição de vapor, água quente e ar condicionado;

42.21-9-03 - Manutenção de redes de distribuição de energia elétrica;
42.21-9-04 - Construção de estações e redes de telecomunicações;
42.21-9-05 - Manutenção de estações e redes de telecomunicações;
43.21-5-00 - Instalação e manutenção elétrica;
43.22-3-02 - Instalação e manutenção de sistemas centrais de ar condicionado, de ventilação e refrigeração;
43.30-4-05 - Aplicação de revestimentos e de resinas em interiores e exteriores;
45.11-1-01 - Comércio a varejo de automóveis, camionetas e utilitários novos;
45.30-7-03 - Comércio a varejo de peças e acessórios novos para veículos automotores;
45.30-7-04 - Comércio a varejo de peças e acessórios usados para veículos automotores;
45.30-7-05 - Comércio a varejo de pneumáticos e câmaras-de-ar;
45.41-2-03 - Comércio a varejo de motocicletas e motonetas novas;
45.41-2-04 - Comércio a varejo de motocicletas e motonetas usadas;
45.41-2-06 - Comércio a varejo de peças e acessórios novos para motocicletas e motonetas;
46.19-2-00 - Representantes comerciais e agentes do comércio de mercadorias em geral não especializado;
47.13-0-02 - Lojas de variedades, exceto lojas de departamentos ou magazines;
47.23-7-00 - Comércio varejista de bebidas;
47.29-6-99 - Comércio varejista de produtos alimentícios em geral ou especializado em produtos alimentícios não especificados anteriormente;
47.41-5-00 - Comércio varejista de tintas e materiais para pintura;
47.42-3-00 - Comércio varejista de material elétrico;
47.43-1-00 - Comércio varejista de vidros;
47.44-0-01 - Comércio varejista de ferragens e ferramentas;
47.44-0-03 - Comércio varejista de materiais hidráulicos;
47.44-0-99 - Comércio varejista de materiais de construção em geral;
47.51-2-01 - Comércio varejista especializado de equipamentos e suprimentos de informática;
47.51-2-02 - Recarga de cartuchos para equipamentos de informática;
47.52-1-00 - Comércio varejista especializado de equipamentos de telefonia e comunicação;
47.53-9-00 - Comércio varejista especializado de eletrodomésticos e equipamentos de áudio e vídeo;
47.54-7-01 - Comércio varejista de móveis;
47.54-7-03 - Comércio varejista de artigos de iluminação;
47.55-5-01 - Comércio varejista de tecidos;
47.55-5-02 - Comercio varejista de artigos de armarinho;
47.55-5-03 - Comercio varejista de artigos de cama, mesa e banho;
47.56-3-00 - Comércio varejista especializado de instrumentos musicais e acessórios;
47.57-1-00 - Comércio varejista especializado de peças e acessórios para aparelhos eletroeletrônicos para uso doméstico, exceto informática e comunicação;
47.59-8-99 - Comércio varejista de outros artigos de uso pessoal e doméstico não especificados anteriormente;
47.61-0-03 - Comércio varejista de artigos de papelaria;
47.63-6-01 - Comércio varejista de brinquedos e artigos recreativos;
47.71-7-01 - Comércio varejista de produtos farmacêuticos, sem manipulação de fórmulas;
47.72-5-00 - Comércio varejista de cosméticos, produtos de perfumaria e de higiene pessoal;
47.73-3-00 - Comércio varejista de artigos médicos e ortopédicos;
47.81-4-00 - Comércio varejista de artigos do vestuário e acessórios;
47.82-2-01 - Comércio varejista de calçados;
47.82-2-02 - Comércio varejista de artigos de viagem;
47.83-1-02 - Comércio varejista de artigos de relojoaria;

47.89-0-05 - Comércio varejista de produtos saneantes domissanitários;
47.89-0-07 - Comércio varejista de equipamentos para escritório;
47.89-0-08 - Comércio varejista de artigos fotográficos e para filmagem;
47.89-0-99 - Comércio varejista de outros produtos não especificados anteriormente;
61.90-6-01 - Provedores de acesso às redes de comunicações;
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis;
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação;
63.11-9-00 - Tratamento de dados, provedores de serviços de aplicação e serviços de hospedagem na internet;
63.19-4-00 - Portais, provedores de conteúdo e outros serviços de informação na internet;
73.19-0-02 - Promoção de vendas;
77.11-0-00 - Locação de automóveis sem condutor;
77.31-4-00 - Aluguel de máquinas e equipamentos agrícolas sem operador;
77.32-2-01 - Aluguel de máquinas e equipamentos para construção sem operador, exceto andaimes;
77.32-2-02 - Aluguel de andaimes;
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios;
77.39-0-03 - Aluguel de palcos, coberturas e outras estruturas de uso temporário, exceto andaimes;
77.39-0-99 - Aluguel de outras máquinas e equipamentos comerciais e industriais não especificados anteriormente, sem operador;
82.99-7-99 - Outras atividades de serviços prestados principalmente às empresas não especificadas anteriormente;
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos;
95.12-6-00 - Reparação e manutenção de equipamentos de comunicação;
95.21-5-00 - Reparação e manutenção de equipamentos eletroeletrônicos de uso pessoal e doméstico.

Cláusula Terceira: A empresa iniciou suas atividades no dia 23/07/2019 e seu prazo de duração é indeterminado.

Cláusula Quarta: A empresa tem o capital de R$ 200.000,00 (Duzentos Mil Reais), totalmente subscrito e integralizado, em moeda corrente nacional, de responsabilidade do titular.

Cláusula Quinta: A responsabilidade do titular é restrita ao valor do capital integralizado.

Cláusula Sexta: A administração da empresa cabe, **isoladamente,** a JORGE VASCONCELOS CORREA, com os poderes e atribuições de representação ativa e passiva, judicial e extrajudicialmente, podendo praticar todos os atos compreendidos no objeto, sempre de interesse da empresa, autorizado o uso do nome empresarial.

Cláusula Sétima: Ao término de cada exercício da empresa, em 31 de dezembro, proceder-se-á a elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo ao titular os lucros ou perdas apurados.

Cláusula Oitava: Falecendo ou interditado o titular, a empresa continuará suas atividades com os herdeiros ou sucessores. Não sendo possível ou inexistindo interesse destes, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da empresa, à data da resolução, verificada em balanço especialmente levantado.

3º ALTERAÇÃO CONTRATUAL – CONSOLIDADA
SPEED TECNOLOGIA EIRELI

Cláusula Nona: O Administrador declara, sob as penas da lei, que não está impedido de exercer a administração da empresa, por lei especial ou em virtude de condenação criminal, ou por se encontrar sob efeito dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos, ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública ou propriedade.

Cláusula Décima: O titular da empresa declara, sob as penas da lei, que não participa de outra empresa da mesma modalidade, estando desimpedido para constituir a presente EIRELI.

Cláusula Décima Primeira: Fica eleito o **foro de Vila Velha/ES,** para o exercício e cumprimento dos direitos e obrigações resultantes deste ato constitutivo.

E, por estar justo e contratado, assina o presente instrumento em 01 via**.**

Vila Velha/ES, 05 de Maio de 2021**.**

_____
JORGE VASCONCELOS CORREA

ASSINATURA ELETRÔNICA

Certificamos que o ato da empresa SPEED TECNOLOGIA EIRELI consta assinado digitalmente por:

IDENTIFICAÇÃO DO(S) ASSINANTE(S)	
CPF	Nome
99804930706	JORGE VASCONCELOS CORREA

CERTIFICO O REGISTRO EM 10/05/2021 13:11 SOB Nº 20210447745.
PROTOCOLO: 210447745 DE 09/05/2021.
CÓDIGO DE VERIFICAÇÃO: 12103238407. CNPJ DA SEDE: 34289656000198.
NIRE: 32600264935. COM EFEITOS DO REGISTRO EM: 10/05/2021.
SPEED TECNOLOGIA EIRELI

PAULO CEZAR JUFFO
SECRETÁRIO-GERAL
www.simplifica.es.gov.br

JORGE VASCONCELOS CORREA: 99804930706

Assinado digitalmente por JORGE VASCONCELOS CORREA:99804930706
DN: C=BR, O=ICP-Brasil, OU=50214482000150, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A1, OU=(EM BRANCO), OU=videoconferencia, CN=JORGE VASCONCELOS CORREA:99804930706
Razão: Eu sou o autor deste documento
Localização: 2022
Data: 2024.04.08 08:47:29-03'00'
Foxit PDF Reader Versão: 11.2.2

ESTADO DO ESPIRITO SANTO
PREFEITURA MUNICIPAL DE GUARAPARI
SECRETARIA MUNICIPAL DA EDUCAÇÃO

LAUDO DE AVALIAÇÃO DE AMOSTRA

Referente: Pregão Eletrônico nº. 003/2024

Processo: Nº 5.372/2024

Objeto: Aquisição de Computadores do tipo Desktop com Garantia Onsite

Atestamos que o ***Computador Lenovo ThinkCentre Neo 50S Gen 4***, apresentado pela empresa ***3D PROJETOS E ASSESSORIA EM INFORMATICA LTDA, CNPJ nº 7.766.048/0002-35,*** atendem às especificações mínimas exigidas no Termo de Referência, resultando na aprovação desta comissão.

LOTE 01

ITEM	QUANT.	DESCRIÇÃO	MARCA / MODELO	RESULTADO
01	40	NOTEBOOK	LENOVO / THINKCENTRE NEO 50S GEN 4	APROVADO

Responsáveis pela aprovação das amostras:

gov.br Documento assinado digitalmente
BRUNO DOS SANTOS MAIA
Data: 09/07/2024 09:16:33-0300
Verifique em https://validar.iti.gov.br

Bruno dos Santos Maia
Matrícula 14172

gov.br Documento assinado digitalmente
DIEGO DA SILVA MENDES
Data: 09/07/2024 09:09:01-0300
Verifique em https://validar.iti.gov.br

Diego da Silva Mendes
Matrícula 2229684

gov.br Documento assinado digitalmente
JOSE ELTON PEREIRA NETO
Data: 09/07/2024 09:17:28-0300
Verifique em https://validar.iti.gov.br

Jose Elton Pereira Neto
Matrícula 165317

Guarapari, 09 de julho de 2024.

ESTADO DO ESPIRITO SANTO
PREFEITURA MUNICIPAL DE GUARAPARI
SECRETARIA MUNICIPAL DA EDUCAÇÃO

LAUDO TÉCNICO DE AVALIAÇÃO DE AMOSTRA

Referente: Pregão Eletrônico nº. 003/2024
Processo: Nº 5.372/2024
Objeto: Aquisição de Computadores do tipo Desktop com Garantia Onsite

Introdução

O presente laudo tem como objetivo avaliar a proposta da empresa **JOÃO BRAULIO COMERCIO DE EQUIPAMENTOS ELETRONICOS LTDA CNPJ Nº 27.845.560/00001-01** referente ao Pregão Eletrônico nº 003/2024, que visa a aquisição de computadores desktop com garantia onsite.

Análise das Especificações

Após meticulosa análise da proposta e documentação apresentada pela empresa, verificamos que a mesma **não atende** às especificações mínimas exigidas no Termo de Referência, conforme detalhado a seguir:

1. Processador (Item 3.1.1):

3.1.1. Atinge índice de 13505 pontos para o desempenho, tendo como referência a base de dados CPU Mark disponível no site https://www.cpubenchmark.net/;

- **Exigência do Edital:** O processador ofertado deve alcançar uma pontuação mínima no CPU BENCHMARK, de acordo com a base de dados CPU Mark disponível no site https://www.cpubenchmark.net/.
- **Não Conformidade:** A proposta não apresenta comprovações de desempenho do processador, conforme solicitado. Adicionalmente, o modelo do processador ofertado não foi especificado. Sem a identificação do modelo, torna-se impossível verificar se o mesmo atende à exigência.

2. Memória RAM e Unidade de Disco (Itens 3.2.2 e 3.5.1):

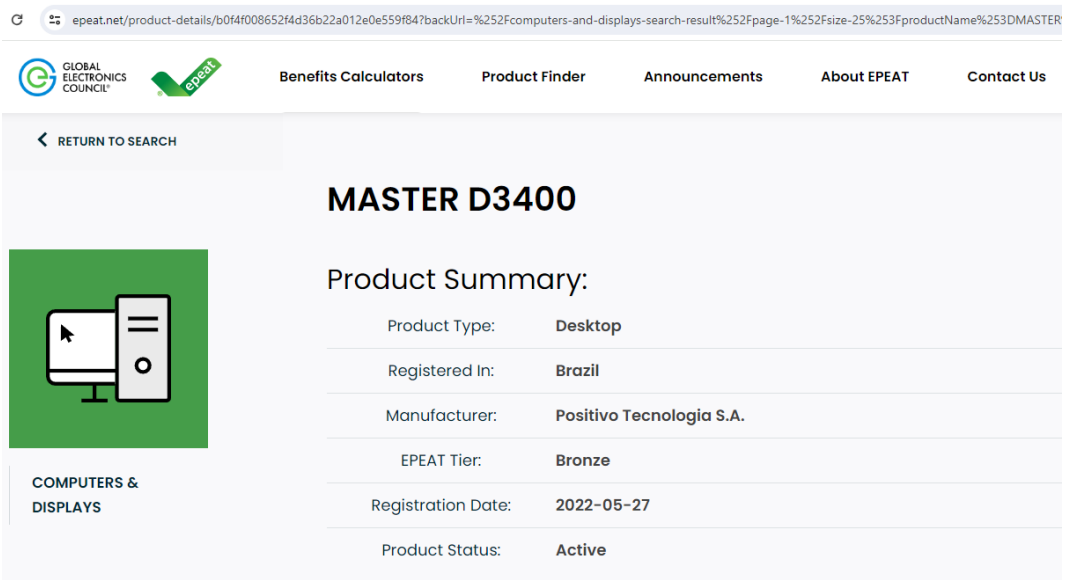
3.2.2. Possui 08 (Oito) GB de memória instalada;
3.5.1. Possui um SSD de 256GB M.2 2280PCIe NVMe;

- **Exigência do Edital:** O equipamento deve possuir 8 GB de memória RAM instalada e um SSD de 256 GB M.2 2280PCIe NVMe.
- **Não Conformidade:** A proposta não especifica a quantidade de memória RAM e armazenamento a serem fornecidos, impossibilitando a verificação se atendem ao Termo de Referência.

3. Comprovações Técnicas (Item 3.16.2):

3.16.2. Os equipamentos ofertados devem possuir no mínimo EPEAT Silver, sendo que a comprovação se fará por intermédio do site da https://www.epeat.net/;

- **Exigência do Edital:** Os equipamentos devem possuir no mínimo certificação EPEAT Silver, comprovada através do site https://www.epeat.net/.
- **Não Conformidade:** O modelo de equipamento ofertado não possui a certificação mínima exigida, conforme verificado no site https://www.epeat.net/. O modelo apresentado possui apenas certificação EPEAT na categoria Bronze.



Conclusão

Diante das análises realizadas, **conclui-se que a proposta da empresa JOÃO BRAULIO COMERCIO DE EQUIPAMENTOS ELETRONICOS LTDA não atende às**

ESTADO DO ESPIRITO SANTO
PREFEITURA MUNICIPAL DE GUARAPARI
SECRETARIA MUNICIPAL DA EDUCAÇÃO

especificações mínimas exigidas no Termo de Referência do Pregão Eletrônico nº 003/2024.

ITEM	QUANT.	DESCRIÇÃO	MARCA / MODELO	RESULTADO
01	40	DESKTOP, COM GARANTIA ONSITE DE 36 MESES.	POSITIVO / MASTER D3400	REPROVADO

Responsáveis pela aprovação das amostras:

gov.br Documento assinado digitalmente
BRUNO DOS SANTOS MAIA
Data: 19/06/2024 14:16:43-0300
Verifique em https://validar.iti.gov.br

Bruno dos Santos Maia
Matrícula 14172

gov.br Documento assinado digitalmente
DIEGO DA SILVA MENDES
Data: 19/06/2024 14:10:20-0300
Verifique em https://validar.iti.gov.br

Diego da Silva Mendes
Matrícula 2229684

gov.br Documento assinado digitalmente
JOSE ELTON PEREIRA NETO
Data: 19/06/2024 14:19:03-0300
Verifique em https://validar.iti.gov.br

Jose Elton Pereira Neto
Matrícula 165317

Guarapari, 19 de junho de 2024.

LAUDO TÉCNICO DE AVALIAÇÃO DE AMOSTRA

Referente: Pregão Eletrônico nº. 003/2024

Processo: Nº 5.372/2024

Objeto: Aquisição de Computadores do tipo Desktop com Garantia Onsite

Introdução

O presente laudo tem como objetivo avaliar a proposta da empresa INFINITY STORE COMERCIO E SERVICOS DE INFORMATICA LTDA CNPJ Nº 37.007.414/0001-52 referente ao Pregão Eletrônico nº 003/2024, que visa a aquisição de computadores desktop com garantia onsite.

Análise das Especificações

Após análise criteriosa da proposta e documentação apresentada pela empresa, constatamos que a mesma **não atende às especificações mínimas exigidas no Termo de Referência**, conforme detalhado a seguir:

Especificações não atendidas:

a) BIOS (Item 3.3.3):

3.3.3. Possibilita que a senha de acesso ao BIOS seja ativada e desativada via SETUP; BIOS português ou inglês, desenvolvida pelo fabricante em conformidade com a especificação UEFI 2.1 (http://www.uefi.org), e capturáveis pela aplicação de inventário SCCM (System Center Configuration Manager); O fabricante possui compatibilidade com o padrão UEFI comprovada através do site http://www.uefi.org/members, na categoria membros;

- **Exigência:** A senha de acesso ao BIOS deve ser ativada e desativada via SETUP; BIOS em português ou inglês, desenvolvida pelo fabricante em conformidade com a especificação UEFI 2.1, capturável pelo SCCM; compatibilidade UEFI comprovada no site http://www.uefi.org/members.
- **Não Conformidade:** A empresa não apresentou documentação comprovando a conformidade do equipamento com o padrão UEFI conforme exigido. Pesquisa no site http://www.uefi.org/members não encontrou o fabricante listado.

b) Diagnóstico Pré-Boot (Item 3.3.4):

3.3.4. Possui diagnóstico pré-boot para no mínimo disco, memória e fonte;

- **Exigência:** Diagnóstico pré-boot para disco, memória e fonte.
- **Não Conformidade:** A documentação apresentada (folder) não comprova esta funcionalidade.

c) Portas USB e TPM (Itens 3.4.3 e 3.4.4):

3.4.3. Possui 07 portas USB, sendo pelo menos 02x USB:3.2 e 01x USB-C na parte frontal do gabinete e 2x USB2.0, 2x USB 3.2 na parte traseira (sem utilização de hubs, placas ou adaptadores);
3.4.4. Deve possuir TPM 2.0 ou superior;

- **Exigências:**
  - 07 portas USB (02x USB 3.2 e 01x USB-C na frente; 2x USB 2.0 e 2x USB 3.2 atrás).
  - TPM 2.0 ou superior.
- **Não Conformidade:** A documentação apresentada não comprova a existência das portas USB e do módulo TPM, conforme exigido.

d) Controladora de Rede e Conectividade (Item 3.6):

3.6. CONTROLADORA DE REDE GIGABITETHERNET, COM AS SEGUINTES CARACTERÍSTICAS:
3.6.1. Opera a 100/1000 Mbps, com reconhecimento automático da velocidade da rede;
3.6.2. Capacidade de operar no modo full-duplex;
3.6.3. Suporte ao protocolo SNMP;
3.6.4. Conector RJ-45 fêmea;
3.6.5. Possui placa de Rede Wi-fi 802.11AX (2x2);
3.6.6. Bluetooth 5.1.

- **Exigências:**
  - Operação a 100/1000 Mbps com reconhecimento automático de velocidade.
  - Capacidade de operar em modo full-duplex.
  - Suporte ao protocolo SNMP.
  - Conector RJ-45.
  - Placa de Rede Wi-fi 802.11AX (2x2) e Bluetooth 5.1.
- **Não Conformidade:** A documentação apresentada não comprova essas características.

e) Garantia (Item 3.13.4):

3.13.4. Os equipamentos devem possuir garantia do fabricante por um período de 36 (trinta e seis) meses na modalidade on-site. Caso a garantia padrão do equipamento não seja a solicitada, deve ser informado o part-number do serviço correspondente a esta garantia ou deverá ser apresentada nos documentos de habilitação, declaração do fabricante para este certame que a garantia do produto corresponde a solicitada, sob pena de desclassificação.

- **Exigência:** Garantia de 36 meses na modalidade on-site, com documentação comprobatória ou declaração do fabricante.
- **Não Conformidade:** A proposta não comprova a garantia de 36 meses on-site conforme solicitado.

f) Certificações Técnicas (Item 3.16):

3.16. COMPROVAÇÕES TÉCNICAS:

3.16.1. O fabricante do equipamento deverá possuir certificação DMTF como board member ou leadershipmember, sendo que a comprovação se fará por intermédio do site da DMTF: http://www.dmtf.org/about/list.

3.16.2. Os equipamentos ofertados devem possuir no mínimo EPEAT Silver, sendo que a comprovação se fará por intermédio do site da https://www.epeat.net/;

3.16.3. Os equipamentos deverão possuir certificado IEC60950;

3.16.4. Os equipamentos deverão possuir certificado IEC61000;

3.16.5. Os equipamentos devem possuir certificação Rohs;

3.16.6. Os equipamentos devem possuir certificado Energy star 8.0 ou superior;

- **Exigências:**
  - Certificação DMTF (board member ou leadership member).
  - Certificação EPEAT Silver.
  - Certificados IEC60950, IEC61000, Rohs, e Energy Star 8.0 ou superior.
- **Não Conformidade:** A empresa não apresentou documentação comprovando a conformidade com as certificações exigidas.

Conclusão:

A proposta apresentada pela empresa INFINITY STORE COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA não atende às especificações mínimas exigidas no Termo de Referência do Pregão Eletrônico nº 003/2024, conforme detalhado acima.

ITEM	QUANT.	DESCRIÇÃO	MARCA / MODELO	RESULTADO
01	40	DESKTOP, COM GARANTIA ONSITE DE 36 MESES.	BRAZIL PC	REPROVADO

Responsáveis pela aprovação das amostras:

gov.br Documento assinado digitalmente
BRUNO DOS SANTOS MAIA
Data: 24/05/2024 15:23:37-0300
Verifique em https://validar.iti.gov.br

Bruno dos Santos Maia
Matrícula 14172

gov.br Documento assinado digitalmente
DIEGO DA SILVA MENDES
Data: 24/05/2024 13:33:33-0300
Verifique em https://validar.iti.gov.br

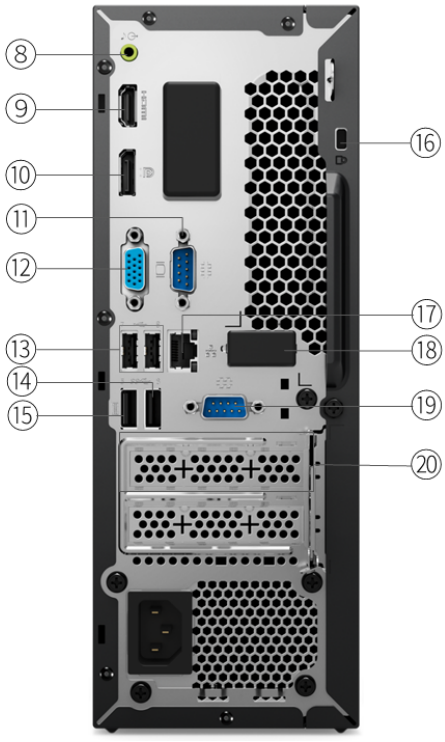
Diego da Silva Mendes
Matrícula 2229684

gov.br Documento assinado digitalmente
JOSE ELTON PEREIRA NETO
Data: 24/05/2024 13:35:58-0300
Verifique em https://validar.iti.gov.br

Jose Elton Pereira Neto
Matrícula 165317

Guarapari, 24 de maio de 2024.

OVERVIEW



1. Power button	11. Serial *
2. Card reader *	12. VGA
3. Microphone (3.5mm)	13. 2x USB 2.0
4. Headphone / microphone combo jack (3.5mm)	14. 1x USB 3.2 Gen 1
5. USB-C 3.2 Gen 1 (data transfer, 15W charging)	15. 1x USB 3.2 Gen 1 (smart power on)
6. 2x USB 3.2 Gen 1	16. Kensington Security Slot
7. Optical drive *	17. Ethernet (RJ-45)
8. Audio line-out (3.5mm)	18. Smart cable clip slots *
9. HDMI 2.1 TMDS	19. Serial *
10. DP 1.4	20. Optional ports *

Notes:

- Items with * are only available on selected models

PERFORMANCE

Processor

Processor Family

Intel® Celeron®, Intel® Pentium®, or 12th / 13th Generation Intel® Core™ i3 / i5 / i7 Processor

Processor**

Processor Name	Cores	Threads	Base Frequency	Max Frequency	Cache	Processor Graphics
Celeron® G6900	2	2	3.4GHz	-	4MB	Intel® UHD Graphics 710
Pentium® Gold G7400	2	4	3.7GHz	-	6MB	Intel® UHD Graphics 710
Core™ i3-12100	4 (4 P-core + 0 E-core)	8	P-core 3.3GHz	P-core 4.3GHz[1]	12MB	Intel® UHD Graphics 730
Core™ i3-12300	4 (4 P-core + 0 E-core)	8	P-core 3.5GHz	P-core 4.4GHz[2]	12MB	Intel® UHD Graphics 730
Core™ i5-12400	6 (6 P-core + 0 E-core)	12	P-core 2.5GHz	P-core 4.4GHz[3]	18MB	Intel® UHD Graphics 730
Core™ i5-12500	6 (6 P-core + 0 E-core)	12	P-core 3.0GHz	P-core 4.6GHz[4]	18MB	Intel® UHD Graphics 770
Core™ i5-12600	6 (6 P-core + 0 E-core)	12	P-core 3.3GHz	P-core 4.8GHz[5]	18MB	Intel® UHD Graphics 770
Core™ i7-12700	12 (8 P-core + 4 E-core)	20	P-core 2.1GHz / E-core 1.6GHz	Max Turbo up to 4.9GHz / P-core 4.8GHz / E-core 3.6GHz[6]	25MB	Intel® UHD Graphics 770
Core™ i3-13100	4 (4 P-core + 0 E-core)	8	P-core 3.4GHz	P-core 4.5GHz[7]	12MB	Intel® UHD Graphics 730
Core™ i5-13400	10 (6 P-core + 4 E-core)	16	P-core 2.5GHz / E-core 1.8GHz	P-core 4.6GHz / E-core 3.3GHz[8]	20MB	Intel® UHD Graphics 730
Core™ i5-13500	14 (6 P-core + 8 E-core)	20	P-core 2.5GHz / E-core 1.8GHz	P-core 4.8GHz / E-core 3.5GHz[9]	24MB	Intel® UHD Graphics 770
Core™ i5-13600	14 (6 P-core + 8 E-core)	20	P-core 2.7GHz / E-core 2.0GHz	P-core 5.0GHz / E-core 3.7GHz[10]	24MB	Intel® UHD Graphics 770
Core™ i7-13700	16 (8 P-core + 8 E-core)	24	P-core 2.1GHz / E-core 1.5GHz	Max Turbo up to 5.2GHz / P-core 5.1GHz / E-core 4.1GHz[11]	30MB	Intel® UHD Graphics 770

Notes:

[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11] Intel® Max Turbo frequency will vary depending on application workload and the hardware and software configurations, see http://www.intel.com/technology/turboboost/ for more information.

Operating System

Operating System**

- Windows® 11 Pro
- Windows® 11 Home
- Windows® 11 Home Single Language
- Windows® 11 DG Windows® 10 Pro 64
- Ubuntu Linux[1]
- No preload operating system

Notes:

[1] Some features may not be supported on the system with Linux preload, including but not limited to Intel® RST RAID, Human Presence Detection, etc.

Graphics

Graphics

**[1]

Graphics	Type	Memory	Connector	Max Resolution	Key Features
Intel® UHD graphics 710	Integrated	Shared	1x HDMI® 2.1 TMDS, 1x VGA, 1x DP 1.4 HBR2	3840×2160@60Hz(HDMI®), 1920x1200@60Hz(VGA), 4096x2304@60Hz(DP)	DirectX® 12
Intel® UHD graphics 730	Integrated	Shared	1x HDMI® 2.1 TMDS, 1x VGA, 1x DP 1.4 HBR2	3840×2160@60Hz(HDMI®), 1920x1200@60Hz(VGA), 4096x2304@60Hz(DP)	DirectX® 12
Intel® UHD graphics 770	Integrated	Shared	1x HDMI® 2.1 TMDS, 1x VGA, 1x DP 1.4 HBR2	3840×2160@60Hz(HDMI®), 1920x1200@60Hz(VGA), 4096x2304@60Hz(DP)	DirectX® 12

Notes:

[1] The information of integrated graphics are not applicable for the models with processor which has no integrated graphics inside (for the details, please refer to processor section).

Monitor Support

Monitor Support

Supports up to 3 independent displays via (HDMI®, DP and VGA)

Chipset

Chipset

Intel® B660 chipset

Memory

Max Memory[1]

Up to 64GB DDR4-3200

Memory Slots

Two DDR4 UDIMM slots, dual-channel capable

Memory Type

DDR4-3200

Notes:

[1] The max memory is based on the test results with current Lenovo® memory offerings.

Storage

Storage Support[1]

Up to two drives, 1x 3.5" HDD + 1x M.2 SSD
• 3.5" HDD up to 2TB
• M.2 SSD up to 1TB

Storage Type***

Disk Type	Interface	RPM	Security
3.5" SATA HDD	SATA 6Gb/s	7.2K	-
M.2 2280 SSD	PCIe® NVMe®, PCIe® 4.0 x4	-	Opal
M.2 2280 SSD	PCIe® NVMe®, PCIe® 4.0 x4	-	Opal 2.0

Notes:

[1] The max capacity of each disk type is based on the test results with current Lenovo® storage offerings.

Removable Storage

Optical**

- DVD-ROM, SATA 1.5Gb/s, slim (9.0mm)
- DVD burner (DVD±RW), SATA connector, slim (9.0mm)

- None

Card Reader

- 7-in-1 card reader (SD, SDHC, SDXC, MMC, MS, MS-Pro, XD)
- No card reader

Multi-Media

Audio Chip

High Definition (HD) Audio, Realtek® ALC623-CG codec

Speakers

- No speakers
- Single speaker, 1W x1

Power Supply

Power Supply**

Power	Type	Efficiency	Key Features
260W	Fixed	90%	Autosensing, 80 PLUS Gold qualified
180W	Fixed	85%	Autosensing

DESIGN

Input Device

Keyboard**

- Lenovo® Calliope Keyboard (USB connector), black
- Lenovo® Traditional Keyboard (USB connector), black
- No keyboard

Mouse

- Lenovo® Calliope Mouse (USB connector), black
- No mouse

Mechanical

Form Factor

SFF (7.4L)

Dimensions (WxDxH)[1]

100 x 308 x 274.8 mm (3.9 x 12.1 x 10.8 inches)

Packaging Dimensions (WxDxH)

195 x 390 x 500 mm (7.7 x 15.4 x 19.7 inches)

Weight[2]

Around 4.5 kg (9.9 lbs)

Packaging Weight

Around 6.35 kg (14 lbs)

Case Color

Raven black

Bays

- 1x 2.5"/3.5" disk bay
- 1x slim ODD bay

Expansion Slots

- One PCIe® 4.0 x16, low-profie (length < 167.65mm, height < 68.90mm)
- One PCIe® 3.0 x1, low-profie (length < 167.65mm, height < 68.90mm)
- Two M.2 slots (one for WLAN, one for SSD)

Stand

- Vertical stand
- No stand

Others

(Optional) Smart Cable (USB-A to USB-C®)

Notes:

[1] The system dimensions may vary depending on configurations.
[2] The system weight is approximate and based on results in Lenovo® lab, which varies depending on the source of component, variance of the distribution of each component, and manufacturing process. It may not be the exact weight for each specific model.

CONNECTIVITY

Network

Onboard Ethernet

Gigabit Ethernet, Realtek® RTL8111HN, 1x RJ-45, supports Wake-on-LAN

WLAN + Bluetooth®**

- Realtek® Wi-Fi® 6 RTL8852BE, 802.11ax Dual Band 2x2 Wi-Fi® + Bluetooth® 5.1, M.2 card
- Intel® Wi-Fi® 6 AX201, 802.11ax 2x2 Wi-Fi® + Bluetooth® 5.1 (Bluetooth® 5.2 hardware ready), M.2 Card[1]
- Intel® Wi-Fi® 6E AX211, 802.11ax 2x2 Wi-Fi® + Bluetooth® 5.1 (Bluetooth® 5.3 hardware ready), M.2 Card[2]
- No WLAN and Bluetooth®

Notes:

[1] Bluetooth® 5.2 is hardware ready but may run at a lower version due to OS limitations.
[2] Bluetooth® 5.3 is hardware ready but may run at a lower version due to OS limitations.

Ports[1]

Front Ports

- 1x USB-C® 3.2 Gen 1 (support data transfer and 5V@3A charging)
- 2x USB 3.2 Gen 1
- 1x headphone / microphone combo jack (3.5mm)
- 1x microphone (3.5mm)

Optional Front Ports

1x card reader

Rear Ports

- 2x USB 2.0
- 2x USB 3.2 Gen 1 (one supports Smart Power On)
- 1x HDMI® 2.1 TMDS
- 1x DisplayPort™ 1.4
- 1x VGA
- 1x Ethernet (RJ-45)
- 1x line-out (3.5mm)

Optional Rear Ports***

- 2x USB 2.0
- 1x parallel
- 1x serial
- 1x 2nd serial
- None

Notes:

[1] The transfer speed of following ports will vary and, depending on many factors, such as the processing speed of the host device, file attributes and other factors related to system configuration and your operating environment, will be slower than theoretical speed.
USB 2.0: 480 Mbit/s;
USB 3.2 Gen 1 (SuperSpeed USB 5Gbps, formerly USB 3.0 / USB 3.1 Gen 1): 5 Gbit/s;
USB 3.2 Gen 2 (SuperSpeed USB 10Gbps, formerly USB 3.1 Gen 2): 10 Gbit/s;
USB4® 20Gbps / USB 3.2 Gen 2x2 (SuperSpeed USB 20Gbps): 20 Gbit/s;
USB4® 40Gbps (USB 40Gbps): 40 Gbit/s;
Thunderbolt™ 3/4: 40 Gbit/s.

SECURITY & PRIVACY

Security

Security Chip

Discrete TPM 2.0, TCG certified

Physical Locks

- (Optional) Smart Cable Clip
- Kensington® Security Slot™, 3 x 7 mm
- Padlock Loop

Chassis Intrusion Switch

- Chassis intrusion switch
- No chassis intrusion switch

Fingerprint Reader

No fingerprint reader

BIOS Security

- Secure Wipe
- Power-on password
- Supervisor password
- Hard disk password
- Cover presence switch
- Self-healing BIOS
- Smart USB protection (allows keyboard / mouse only, blocks all storage devices)
- Individual USB port disablement
- Intel® BIOS guard

MANAGEABILITY

System Management

System Management

Non-vPro®

SERVICE

Warranty[1]

Base Warranty**

- 1-year courier or carry-in service
- 1-year limited onsite service
- No base warranty

Notes:

[1] The warranty upgrades may be bundled with some models, please check the "Included upgrade" column in the specific model's configurations. For more service extensions, please go to https://smartfind.lenovo.com/. To learn more details of warranty policy, please access https://pcsupport.lenovo.com/warranty.

ACCESSORIES

Bundled Accessories

Bundled Accessories

- DP to DVI dongle
- DP to Dual DP dongle
- DP to HDMI® dongle
- DP to VGA dongle
- HDMI® to HDMI® dongle
- HDMI® to VGA dongle
- None

OPERATING REQUIREMENTS

Operating Environment

Temperature

- Operating: 5°C (41°F) to 35°C (95°F)
- Storage: -40°C (-40°F) to 60°C (140°F)

Relative Humidity

- Operating: 20% to 80%
- Storage: 10% to 90%

Altitude

- Operating: 0 m (0 ft) to 3048 m (10,000 ft)
- Storage: 0 m (0 ft) to 12192 m (40,000 ft)

CERTIFICATIONS

Green Certifications[1]

Green Certifications

- (Optional) ENERGY STAR® 8.0
- (Optional) EPEAT™ Silver Registered[2]
- (Optional) EPEAT™ Gold Registered[3]
- ErP Lot 3
- RoHS compliant
- TCO Certified

Notes:

[1] The items listed under the "Green Certifications" section may not only refer to certification but also registration or self-declaration. For ESG & regulatory compliance documents, please visit https://compliance.lenovo.com.
[2], [3] EPEAT™ is registered where applicable, please visit epeat.net for registration status by country.

Other Certifications

Other Certifications

- (Optional) TÜV Rheinland® Low Noise
- (Optional) TÜV Rheinland® Ultra Low Noise

- Feature with ** means that only one offering listed under the feature is configured on selected models.
- Feature with *** means that one or more offerings listed under the feature could be configured on selected models.
- Lenovo reserves the right to change specifications or other product information without notice. Lenovo is not responsible for photographic or typographical errors. LENOVO PROVIDES THIS PUBLICATION “AS IS,” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore this disclaimer may not apply to you.
- The specifications on this page may not be available in all regions, and may be changed or updated without notice.


ThinkCentre
neo5
Lenovo


ThinkCentre
neo5
Lenovo


ThinkCentre
neo5
Lenovo

Rugged compact performance primed for business

ThinkCentre Neo series offers organizations enhanced manageability and security features, along with additional configuration and expansion options.

ThinkCentre neo 50s Gen 4

This fast and intuitive 7.4-liter small form factor equipped with the processing power of Intel Celeron, Intel Pentium, or up to 12th or 13th Intel Core Gen i7 processor delivers high performance to business professionals. Combined with integrated Intel UHD graphics, the desktop enables faster responsiveness for memory-intensive data applications. Additionally, the modern workforce can work efficiently and store heavy files with up to 64GB DDR4 memory and up to 2TB SSD storage.

Enhanced accessibility with better performance

For enhanced accessibility, the desktop allows professionals to access up to three independent displays via HDMI, DisplayPort, and VGA ports; plus plugging in USB drives, extra cables, or checking a connection is a lot less tedious.

Better ergonomics with smart security features

Discreet TPM 2.0 chipset, optional smart cable clip, optional chassis intrusion switch, Kensington security slot, Padlock loop, and BIOS security prevent unauthorized access into the interior of the system.

Effective power management with compact design

WIth optional EPEAT Gold and EPEAT Silver cetifiacations, the device is energy efficient, thus helping businesses reduce their environemental impact.

Updated 2024-07-01

Lenovo Services

Lenovo delivers tailored sustainability services, devices, and infrastructure solutions from our broad portfolio, working closely with you to support your target outcomes across the IT lifecycle..

Return To Depot Repair Warranty

- No-hassle repair process at a Lenovo service center
- Lenovo pays for all shipping between the customer and service facility
- Avoid unplanned operational expense with a simple annual fee

Accessories

Lenovo Go Wired Speakerphone

- Microsoft Teams certified, omni-directional far-field 2x microphones array
- Portable plug-and-play capabilities and effortless PC UC support
- Comes with intuitive control with volume wheel, tactile keys, and readable LEDs

PN: 4XD1C82055, GXD1C82051

Lenovo Professional Wireless Laser Mouse

- Full-size efficient laser mouse offers ergonomic comfort and precision tracking
- Longer battery life: 2 year battery life provides more convenience for everyday use
- Sleek and stylish design to match a ThinkCentre or ThinkPad system

PN: 4X30H56886

ThinkCentre neo 50s Gen 4

Performance

Processor
Intel Celeron, Pentium, or 13th Gen Core i3 / i5 / i7

Operating System*
Windows 11 Pro 64
Windows 11 Home 64
Windows 11 DG Windows 10 Pro 64
Ubuntu Linux

Graphics
Intel UHD Graphics (integrated)

Chipset
Intel B660 chipset

Memory [1]
Up to 64GB DDR4-3200, two UDIMM slots

[1]The max memory is based on the test results with current Lenovo memory offerings.

Storage [2]
Up to two drives, 1x 3.5" HDD + 1x M.2 SSD
3.5" HDD up to 2TB
M.2 SSD up to 1TB

[2]The max capacity of each disk type is based on the test results with current Lenovo storage offerings.

Optical*
DVD-ROM or DVD±RW*

Audio
High Definition (HD) Audio with single speaker

Power Supply*
260W 90%,180W 85% PSU

Design

Form factor
SFF (7.4L)

Dimensions [3]
100 x 308 x 274.8 mm (3.9 x 12.1 x 10.8 inches)

[3]The system dimensions may vary depending on configurations.

Weight [4]
Around 4.5 kg (9.9 lbs)

[4]The system weight is approximate and may vary depending on configurations

Color
Black

Bays
1x 2.5"/3.5" disk bay
1x slim ODD bay

Expansion Slots
One PCIe 3.0 x1
One PCIe 4.0 x16
Two M.2 slots (one for WLAN, one for SSD)

Connectivity

WLAN + Bluetooth*
802.11ax (Wi-Fi 6), Bluetooth 5.1
Up to Intel Wi-Fi 6E AX201, Bluetooth 5.1

Front ports
2x USB 3.2 Gen 1
1x USB-C 3.2 Gen 1 (support data transfer and 5V@3A charging)
1x headphone / microphone combo jack (3.5mm)
1x microphone (3.5mm)
1x card reader*

Rear ports
2x USB 2.0
2x USB 3.2 Gen 1
1x VGA
1x HDMI 2.1 TMDS
1x DisplayPort 1.4
1x Ethernet (RJ-45)
1x line-out (3.5mm)
2x USB 2.0*
1x serial*
1x 2nd serial*
1x parallel*

Security & Privacy

Security
Discrete TPM 2.0
Smart Cable Clip*
Kensington Security Slot
Padlock Loop
Chassis Intrusion Switch*

Lenovo services

Base Warranty
Up to 1-year limited onsite service

Certifications

Green Certifications [5] [6]
EPEAT Gold Registered*
EPEAT Silver Registered*
ENERGY STAR 8.0*
ErP Lot 3
TCO Certified 9.0
RoHS compliant

[5]The items listed under the "Green Certifications" section may not only refer to certification but also registration or self-declaration.

[6]EPEAT is registered where applicable, please see https://www.epeat.net for registration status by country.

Other Certifications
TÜV Rheinland Low Noise*
TÜV Rheinland Ultra Low Noise*

Suporte

Informações sobre o TPM (Trusted Platform Module) para Intel® NUC

Nota O Windows* 11 requer o Trusted Platform Module (TPM) conforme declarado em seus requisitos de sistema .

Visão geral

- **Trusted Platform Module (TPM 2.0) -** O TPM 2.0 é um microcontrolador que armazena chaves, senhas e certificados digitais. Um TPM 2.0 dedicado também suporta a tecnologia Intel® vPro™ e os Intel® Trusted Execution Technology (Intel® TXT).
- **Intel® Platform Trust Technology (Intel® PTT) -** Intel® Platform Trust Technology (Intel® PTT) oferece os recursos do TPM 2.0 dedicado. Intel PTT é uma funcionalidade de plataforma para armazenamento de credenciais e gerenciamento de chaves usada pelo Windows 8*, Windows® 10 e Windows* 11. Intel PTT suporta BitLocker* para criptografia de disco rígido e suporta todos os requisitos da Microsoft para o Módulo de plataforma confiável 2.0 (fTPM) 2.0 de firmware.

Determinar se o seu NUC é compatível com essas tecnologias

Consulte as especificações da sua Intel NUC em ark.intel.com , na seção Tecnologias avançadas.

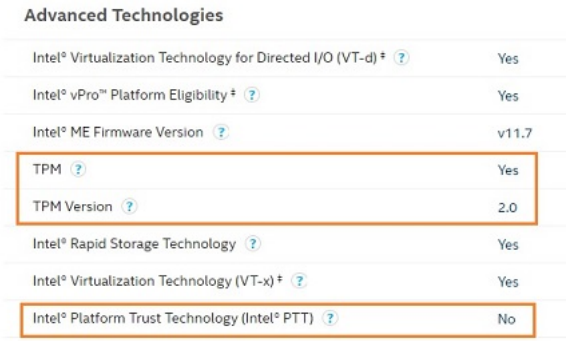
Documentação

Tipo de conteúdo
Instalação e configuração

ID do artigo
000007452

Última revisão
20/02/2024

Comentários



Advanced Technologies	
Intel® Virtualization Technology for Directed I/O (VT-d) ‡	Yes
Intel® vPro™ Platform Eligibility ‡	Yes
Intel® ME Firmware Version	v11.7
TPM	Yes
TPM Version	2.0
Intel® Rapid Storage Technology	Yes
Intel® Virtualization Technology (VT-x) ‡	Yes
Intel® Platform Trust Technology (Intel® PTT)	No

Solucionando problemas

- Como habilitar o Trusted Platform Module (TPM 2.0) no Intel® NUC

- Erro de dispositivo desconhecido no Gerenciador de Dispositivos relacionado a TPM ou PTT
- Intel-SA-00104 para o Trusted Platform Module (TPM) do Infineon*

- Intel® Platform Trust Technology (Intel® PTT) Serviço de recertificação usa 30% a 40% do uso da CPU

Tópicos relacionados

Recomendações do Microsoft TPM com informações do fabricante do computador

*

- Para a sua conveniência, o conteúdo deste site foi traduzido utilizando-se uma combinação de programas de computador de tradução automática e tradutores. Este conteúdo é fornecido somente como informação de caráter genérico, não devendo ser considerado como uma tradução completamente correta do idioma original.

Produtos relacionados

Este artigo aplica-se a 40 produtos.

Mostrar tudo ❯

Mais ajuda? Entrar em contato com o suporte

Comentários





Comentários

Programas de Certificação TCG

Recursos adicionais

PRODUTOS CERTIFICADOS DE ARMAZENAMENTO (HTTPS://TRUSTEDCOMPUTINGGROUP.ORG/MEMBERSHIP/CERTIFICATION/STORAGE-CERTIFIED-PRODUCTS/)

PRODUTOS CERTIFICADOS PELA TNC (HTTPS://TRUSTEDCOMPUTINGGROUP.ORG/MEMBERSHIP/CERTIFICATION/TNC-CERTIFIED-PRODUCTS/)

PRODUTOS CERTIFICADOS TPM (HTTPS://TRUSTEDCOMPUTINGGROUP.ORG/MEMBERSHIP/CERTIFICATION/TPM-

A TCG oferece programas de certificação para promover qualidade consistente entre produtos construídos de acordo com as especificações da TCG. Isso fornece uma ferramenta útil para auxiliar os clientes a verificar a segurança e a conformidade funcional de produtos construídos de acordo com as especificações da TCG.

CERTIFIED-PRODUCTS/)

Atualmente, a TCG oferece programas de certificação em três áreas: Trusted Platform Modules (TPM), Trusted Network Communications (TNC) e Storage Devices.

Certificação Trusted Platform Module (TPM)

A Certificação TPM permite que os membros do TCG demonstrem que seus produtos TPM atendem a um conjunto de requisitos de Avaliação de Conformidade e Segurança que foi desenvolvido com a participação da associação TCG e da indústria. Os produtos TPM aprovados na certificação estão listados na Lista de Produtos Certificados (http://www.trustedcomputinggroup.org/certification/tpm-certified-products/) . A certificação TPM é um benefício da associação TCG e, portanto, a associação é obrigatória.

Os requisitos de certificação para que o produto TPM de um membro obtenha a Certificação TCG incluem:

Teste de conformidade TPM

Avaliação de Segurança TPM

Certificação Trusted Network Communications (TNC)

A Certificação TNC permite que os implementadores do TCG demonstrem que os produtos de comunicação de rede atendem a um conjunto de requisitos de Conformidade e Interoperabilidade que foram desenvolvidos com a participação da indústria e da associação TCG. Os produtos TNC aprovados na certificação estão listados na Lista de Produtos Certificados (http://www.trustedcomputinggroup.org/certification/tnc-certified-products/) . A Certificação TNC está aberta tanto para membros do TCG quanto para não membros do TCG.

Os requisitos de certificação para produtos TNC para obter a Certificação TCG incluem:

Teste de conformidade TNC

Teste de interoperabilidade TNC

Recursos do Programa de Certificação TNC

Certificação de Armazenamento

A Certificação de Armazenamento permite que os membros do TCG demonstrem que seus produtos de armazenamento atendem a um conjunto de requisitos de Avaliação de Conformidade e Segurança que foi desenvolvido com a participação da associação TCG e da indústria. Os produtos de armazenamento que passam na certificação são listados na Lista de Produtos Certificados. A certificação de armazenamento é um benefício da associação TCG e, portanto, a associação é necessária.

Os requisitos de certificação para que o produto de armazenamento de um membro obtenha a Certificação TCG incluem:

Teste de conformidade de armazenamento

Recursos do Programa de Certificação de

Armazenamento

Avaliação de Segurança

Recursos do Programa de Certificação

O Comitê do Programa de Certificação disponibilizou os recursos abaixo ao público para educação e para aumentar a compreensão do cliente sobre os procedimentos e princípios usados para desenvolver cada programa.

- Critérios Comuns – Portal Principal de Critérios Comuns (https://www.commoncriteriaportal.org/)
- Laboratórios licenciados por critérios comuns (https://www.commoncriteriaportal.org/labs/)

Entre em contato com certification@trustedcomputinggroup.org (mailto:certification@trustedcomputinggroup.org) para obter mais informações.

Perguntas frequentes

Participação da Indústria (http://www.trustedcomputinggroup.org/industry-participation)
Diretório de Recursos (http://www.trustedcomputinggroup.org/resources)
Certificação (http://www.trustedcomputinggroup.org/membership/certification/)
Acesso de membro (https://members.trustedcomputinggroup.org/kws/)
Entrar (http://www.trustedcomputinggroup.org/membership/)

Inscrição no boletim informativo

Fique por dentro das atividades do Trusted Computing Group (TCG), incluindo estudos de caso recentes, comunicados à imprensa, notícias do setor e próximos eventos por meio do boletim informativo do TCG!

Primeiro nome

Sobrenome

E-mail * (obrigatório)

Empresa/Organização

Contate-nos

Administração do Trusted Computing Group

3855 SW 153rd Drive

Beaverton, Oregon 97003

Telefone: +1.503.619.0562 (tel:+1.503.619.0562)
Fax: +1.503.644.6708 (tel:+1.503.644.6708)
E-mail: admin@trustedcomputinggroup.org (mailto:admin@trustedcomputinggroup.org)

Inscrever-se

Ao enviar este formulário, você está consentindo em receber e-mails de marketing de: . Você pode revogar seu consentimento para receber e-mails a qualquer momento usando o link SafeUnsubscribe®, encontrado na parte inferior de cada e-mail. Os e-mails são atendidos pela Constant Contact (https://www.constantcontact.com/legal/service-provider)

Noticias legais (https://trustedcomputinggroup.org/legal-notices/)
política de Privacidade (https://trustedcomputinggroup.org/privacy-policy/)

(https://www.linkedin.com/company/trusted-computing-group/)

(https://twitter.com/TrustedComputin)

(https://www.youtube.com/user/TCGadmin)

Número do artigo: 000131631

Comparação dos recursos do TPM 1.2 com o 2.0

Resumo: Recursos do TPM 1.2 vs. 2.0, TPM 1.2 em comparação ao TPM 2.0, TPM 1.2 vs. 2.0 - suporte a aplicativos e recursos, TPM 2.0 diferente de um TPM de firmware

Conteúdo do artigo

Instruções

TPM 1.2 em comparação ao TPM 2.0 — suporte criptográfico

A tabela de algoritmos de criptografia abaixo apresenta um resumo. Para obter uma lista mais abrangente de algoritmos TPM, consulte o **Registro de algoritmo TCG**. A lista de algoritmos obrigatórios para o TPM 2.0 em um computador pessoal é definida no **Perfil de TPM da plataforma do client PC** mais recente.

Tipo de algoritmo	Nome do algoritmo	TPM 1.2	TPM 2.0
Assimétrico	RSA 1024	Sim	Opcional
	RSA 2048	Sim	Sim
	ECC P256	Não	Sim
	ECC BN256	Não	Sim

Tipo de algoritmo	Nome do algoritmo	TPM 1.2	TPM 2.0
Simétrico	AES 128	Opcional	Sim
	AES 256	Opcional	Opcional
Hash	SHA-1	Sim	Sim
	SHA-2 256	Não	Sim
HMAC	SHA-1	Sim	Sim
	SHA-2 256	Não	Sim

Tabela 1: TPM 1.2 vs. 2.0

TPM 1.2 versus TPM 2.0 — diferenças de comportamento

O TPM 1.2 oferece suporte a uma única autorização de "proprietário", com uma Chave de endosso (EK) RSA 2048b para autenticação/atestado e uma única Chave raiz de armazenamento (SRK) RSA 2048b para criptografia. Isso significa que um único usuário ou entidade ("proprietário") tem controle sobre as funções de autenticação/atestado e criptografia do TPM. Em geral, a SRK serve como pai para quaisquer chaves criadas no TPM 1.2. O TPM 1.2 foi especificado como um dispositivo de entrada (consulte o artigo O caso para ativar **módulos** de plataforma confiável para obter mais informações sobre o significado de "opt-in" conforme aplicável ao TPM).

O TPM 2.0 tem as mesmas funcionalidades representadas pela EK para autenticação/atestado e SRK para criptografia como no 1.2, mas o controle é dividido em duas hierarquias diferentes no 2.0: a Hierarquia de endosso (EH) e a Hierarquia de armazenamento (SH). Além da EH e da SH, o TPM 2.0 também contém uma Hierarquia de Plataforma (PH) para as funções de manutenção, e uma Hierarquia Nula. Cada hierarquia tem seu próprio "proprietário" exclusivo para autorização. Por esse motivo, o TPM 2.0 oferece suporte a quatro autorizações, o que seria análogo ao "proprietário" único do TPM 1.2.

No TPM 2.0, a nova Hierarquia De Plataforma deve ser usada pelos fabricantes de plataforma. As hierarquias de Armazenamento e de Endosso e a hierarquia Nula serão usadas pelo sistema operacional e pelos aplicativos presentes no SO. O TPM 2.0 foi especificado de uma maneira que torna a descoberta e o gerenciamento menos complicados do que no 1.2. O TPM 2.0 pode oferecer suporte a algoritmos RSA e ECC para Chaves de endosso e SRKs.

TPM 1.2 vs. 2.0 - Aplicativos e recursos compatíveis:

Recurso ou aplicativo	TPM 1.2	TPM 2.0
DDP|ST - Cliente OTP	Sim	Não*
DDP|Criptografia	Sim	Sim
Tecnologia de execução confiável Intel®	Sim	Sim
Microsoft BitLocker™	Sim	Sim
Smart Card Virtual da Microsoft	Sim	Sim
Microsoft Credential Guard™	Sim	Sim
Microsoft Passport™	Sim	Sim

Recurso ou aplicativo	TPM 1.2	TPM 2.0
Inicialização medida TCG	Sim	Sim
Inicialização segura UEFI	Sim	Sim
Microsoft Device Guard™	Sim	Sim

Tabela 2: TPM 1.2 vs. 2.0 - Aplicativos e recursos suportados

Nota: * O DDP | ST funciona em um computador configurado com o TPM 2.0, mas não utiliza o TPM 2.0 no momento.

Como o TPM 2.0 discreto difere de um TPM firmware (fTPM)?

Um TPM baseado em firmware (fTPM) é um TPM que opera usando os recursos e o contexto de um dispositivo de computação multifuncional/de recurso (como um SoC, CPU ou outro ambiente de computação semelhante).

Um TPM discreto é implementado como um chip de função/recurso isolado e separado, com todos os recursos de computação necessários contidos no discreto pacote do chip físico. Um TPM discreto tem controle total sobre os recursos internos dedicados (como memória volátil, memória não volátil e lógica criptográfica), e é a única função que acessa e utiliza esses recursos.

Um TPM baseado em firmware não tem seu próprio armazenamento dedicado. Ele conta com os serviços do sistema operacional e da plataforma para obter acesso ao armazenamento dentro da plataforma. Uma das implicações de não ter um armazenamento dedicado envolve a presença de um certificado de Chave de endosso (EK). Dispositivos de TPM discretos podem ser entregues pelo fabricante do TPM ao fabricante da plataforma com um certificado de EK instalado no armazenamento do TPM para a Chave de endosso do TPM. Isso não é possível com um TPM de firmware. Os fornecedores de TPM de firmware disponibilizam os certificados para os usuários finais por meio de processos específicos do fabricante. Para adquirir o certificado de EK para um computador, os proprietários de plataforma precisam entrar em contato com o fornecedor de chipset/CPU para essa plataforma

Além disso, exige-se um **TPM discreto com certificado TCG** para atender aos requisitos de conformidade e segurança, incluindo a proteção do chip e dos seus recursos internos semelhantes aos Smart Cards. A conformidade com o TCG verifica se o TPM implementa corretamente as especificações do TCG. A proteção exigida pela certificação TCG permite que um TPM discreto certificado se proteja contra ataques físicos mais complicados.

Operating System Support matrix:

Suporte ao fornecedor do sistema operacional

Sistema operacional	TPM 1.2	TPM 2.0
Windows 7	Sim	Não (1)
Windows 8	Sim	Sim (2)
Windows 8.1	Sim	Sim (2)
Windows 10	Sim	Sim
RHEL	Sim	Sim (3)(4)
Ubuntu	Sim	Sim (3)(5)

Tabela 3: Suporte ao fornecedor do sistema operacional

- O Windows 7 de 64 bits com SP configurada no modo de inicialização UEFI + CSM pode oferecer suporte ao TPM 2.0, compatível com algumas plataformas.
- O Windows 8 foi lançado com suporte para TPM 2.0, mas oferece suporte apenas ao SHA-1.

- Requer o kernel upstream do Linux versão 4.4 ou mais recente. Os fornecedores de distribuição do Linux podem optar por oferecer suporte a backport de kernels mais antigos.
- O Red Hat® Enterprise Linux® 7.3 e posterior têm suporte básico a kernel. O RHEL 7.4 tem uma visualização de tecnologia das ferramentas de espaço do usuário.
- Compatível com o Ubuntu 16.04 e versão posterior.

Suporte do sistema operacional da plataforma comercial da Dell

Sistema operacional	TPM 1.2	TPM 2.0
Windows 7	Sim	Não
Windows 8	Sim	Não (5)
Windows 8.1	Sim	Não (5)
Windows 10	Sim	Sim (6)
RHEL	Não (7)	Sim (8)
Ubuntu 14.04	Não (7)	Não
Ubuntu 16.04	Não (7)	Sim (9)

Tabela 4: Suporte do sistema operacional da plataforma comercial da Dell

- A Dell oferece suporte ao TPM 2.0 com o Windows 8 e 8.1 em um número limitado de tablets e computadores pessoais removíveis compatíveis com o modo em espera conectado da Microsoft.
- O suporte ao TPM 2.0 ficou disponível em todas as Plataformas comerciais no outono de 2016, e o modo TPM de padrão de fábrica no Windows 10 é o TPM 2.0.
- O TPM 1.2 não é oficialmente suportado pela Dell com o Linux, exceto em plataformas IoT selecionadas.
- Requer Red Hat® Enterprise Linux® 7.3 ou posterior. O usuário pode precisar alterar manualmente o modo TPM de 1.2 para 2.0.
- A Dell colaborou com a Canonical no suporte do TPM 2.0 em computadores client que são enviados com o TPM 2.0. Isso exige que o Ubuntu 16.04 seja enviado junto com o computador.

Mais informações

Artigos recomendados

Aqui estão alguns artigos recomendados relacionados a este tópico que podem ser de seu interesse.

- Computadores Dell que podem fazer upgrade do TPM 1.2 para 2.0
- Processo de upgrade ou downgrade do Trusted Platform Module (TPM) para o sistema operacional Windows 10
- Perguntas frequentes sobre o Trusted Platform Module (TPM) para Windows 11

Propriedades do artigo

Data da última publicação

03 jan. 2024

Versão

5

Tipo de artigo

How To

Avalie este artigo

Preciso

☆ ☆ ☆ ☆ ☆

Úteis

☆ ☆ ☆ ☆ ☆

Fácil de entender

☆ ☆ ☆ ☆ ☆

Este artigo foi útil?

◯ Sim ◯ Não

Mais informações (opcional) 0/3000 characters

Letras, números e todos os caracteres especiais, exceto < > ( ) \

Enviar feedback

Entre em contato com o suporte

Voltar ao início

Conceitos básicos do TPM

Artigo • 15/07/2024 • Aplica-se a: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Este artigo fornece uma descrição dos componentes Trusted Platform Module (TPM 1.2 e TPM 2.0) e explica como são utilizados para mitigar ataques de dicionário.

Um TPM é um microchip concebido para fornecer funções básicas relacionadas com a segurança, principalmente envolvendo chaves de encriptação. O TPM é instalado na placa principal de um computador e comunica com o resto do sistema através de um barramento de hardware.

Os dispositivos que incorporam um TPM podem criar chaves criptográficas e encriptá-las, para que as chaves só possam ser desencriptadas pelo TPM. Este processo, muitas vezes denominado "encapsulamento" ou "enlace" uma chave, pode ajudar a proteger a chave da divulgação. Cada TPM tem uma chave de encapsulamento primária, denominada **chave de raiz de armazenamento**, que é armazenada no próprio TPM. A parte privada de uma chave de raiz de armazenamento ou **chave de endossamento** que é criada num TPM nunca é exposta a qualquer outro componente, software, processo ou utilizador.

Pode especificar se as chaves de encriptação criadas pelo TPM podem ou não ser migradas. Se especificar que podem ser migradas, as partes públicas e privadas da chave podem ser expostas a outros componentes, software, processos ou utilizadores. Se especificar que as chaves de encriptação não podem ser migradas, a parte privada da chave nunca será exposta fora do TPM.

Os dispositivos que incorporam um TPM também podem criar uma chave encapsulada e associada a determinadas medidas da plataforma. Este tipo de chave só pode ser desembrulhado quando essas medições de plataforma têm os mesmos valores que tinham quando a chave foi criada. Este processo é referido como *selagem da chave para o TPM*. Desencriptar a chave chama-se *anular a linha*. O TPM também pode selar e anular dados não selados que são gerados fora do TPM. Com a chave selada e o software, como a Encriptação de Unidade BitLocker, os dados podem ser bloqueados até que sejam cumpridas condições específicas de hardware ou software.

Com um TPM, partes privadas de pares de chaves são mantidas separadas da memória que é controlada pelo sistema operativo. As chaves podem ser seladas ao TPM e determinadas garantias sobre o estado de um sistema (garantias que definem a fiabilidade de um sistema) podem ser feitas antes de as chaves serem não seladas e libertadas para utilização. O TPM utiliza o seu próprio firmware interno e circuitos lógicos para processar instruções. Por conseguinte, não depende do sistema operativo e não está exposto a vulnerabilidades que possam existir no sistema operativo ou no software de aplicação.

- Para obter informações sobre as versões do Windows que suportam as versões do TPM, consulte Descrição geral da tecnologia trusted Platform Module.
- Para obter mais informações sobre quais os serviços TPM que podem ser controlados centralmente através das definições da Política de Grupo, veja Definições de Política de Grupo do TPM.

As funcionalidades disponíveis nas versões são definidas em especificações pelo Grupo de Computação Fidedigno (TCG). Para obter mais informações, veja a página Trusted Platform Module (Módulo de Plataforma Fidedigna) no site Trusted Computing Group (Grupo de Computação Fidedigno).

As secções seguintes fornecem uma descrição geral das tecnologias que suportam o TPM:

- Arranque Medido com suporte para atestado
- Smart Card Virtual baseado em TPM
- Armazenamento de certificados baseado em TPM
- TPM Cmdlets
- Interface de presença física
- Estados e inicialização do TPM 1.2
- Chaves de endossamento
- Atestado de Chave TPM
- Anti-martelação

Arranque Medido com suporte para atestado

A funcionalidade Arranque Medido fornece software antimalware com um registo fidedigno (resistente ao spoofing e adulteração) de todos os componentes de arranque. O software antimalware pode utilizar o registo para determinar se os componentes executados antes do mesmo são fidedignos ou infetados com software maligno. Também pode enviar os registos de Arranque Medido para um servidor remoto para avaliação. O servidor remoto pode iniciar ações de remediação ao interagir com o software no cliente ou através de mecanismos fora de banda, conforme adequado.

Smart Card Virtual baseado em TPM

> ⚠ **Aviso**
>
> As chaves de segurança do Windows Hello para Empresas e FIDO2 são métodos de autenticação de dois fatores modernos para o Windows. Os clientes que utilizam smart cards virtuais são incentivados a mudar para o Windows Hello para Empresas ou FIDO2. Para novas instalações do Windows, recomendamos chaves de segurança do Windows Hello para Empresas ou FIDO2.

O Smart Card Virtual emula a funcionalidade dos smart cards tradicionais. Os Smart Cards Virtuais utilizam o chip TPM, em vez de utilizarem um smart card e leitor físicos separados. Isto reduz consideravelmente o custo de gestão e implementação de smart cards numa empresa. Para o utilizador final, o Smart Card Virtual está sempre disponível no dispositivo. Se um utilizador precisar de utilizar mais do que um dispositivo, tem de ser emitido um Smart Card Virtual para cada dispositivo. Um computador partilhado entre vários utilizadores pode alojar vários Smart Cards Virtuais, um para cada utilizador.

Armazenamento de certificados baseado em TPM

O TPM protege certificados e chaves RSA. O fornecedor de armazenamento de chaves TPM (KSP) proporciona uma utilização fácil e conveniente do TPM como forma de proteger fortemente as chaves privadas. O KSP do TPM gera chaves quando uma organização se inscreve para certificados. O TPM também protege os certificados importados de uma origem externa. Os certificados baseados em

TPM são certificados padrão. O certificado nunca poderá sair do TPM a partir do qual as chaves são geradas. O TPM também pode ser utilizado para operações criptográficas através da API de Criptografia: Próxima Geração (CNG).

TPM Cmdlets

Você pode gerenciar o TPM usando Windows PowerShell. Para obter detalhes, consulte Cmdlets do TPM no Windows PowerShell.

Interface de presença física

Para o TPM 1.2, as especificações de TCG para TPMs requerem presença física (normalmente, premir uma tecla) para ativar o TPM, desativá-lo ou limpá-lo. Normalmente, estas ações não podem ser automatizadas com scripts ou outras ferramentas de automatização, a menos que o OEM individual as forneça.

Estados e inicialização do TPM 1.2

O TPM 1.2 tem vários estados possíveis. O Windows inicializa automaticamente o TPM, o que o coloca num estado ativado, ativado e propriedade.

Chaves de endossamento

Uma aplicação fidedigna só pode utilizar o TPM se o TPM contiver uma chave de endossamento, que é um par de chaves RSA. A metade privada do par de chaves é mantida dentro do TPM e nunca é revelada ou acessível fora do TPM.

Atestado de chave

O atestado de chave TPM permite que uma autoridade de certificação verifique se uma chave privada está protegida por um TPM e que o TPM é aquele em que a autoridade de certificação confia. As chaves de endossamento comprovadas são utilizadas para vincular a identidade do utilizador a um dispositivo. O certificado de utilizador com uma chave com atestado de TPM fornece uma maior garantia de segurança suportada pela não acessibilidade, anti-martelar e isolamento de chaves fornecidas por um TPM.

Anti-martelação

Quando um TPM processa um comando, fá-lo num ambiente protegido. Por exemplo, um microcontrolador dedicado num chip discreto ou um modo especial protegido por hardware na CPU principal. Um TPM é utilizado para criar uma chave criptográfica que não é divulgada fora do TPM. É utilizado no TPM depois de ser fornecido o valor de autorização correto.

Os TPMs têm proteção anti-martelada concebida para impedir ataques de força bruta ou ataques de dicionário mais complexos, que tentam determinar valores de autorização para utilizar uma chave. A abordagem básica é que o TPM permita apenas um número limitado de falhas de autorização antes de impedir mais tentativas de utilização de chaves e bloqueios. Fornecer uma contagem de falhas para chaves individuais não é tecnicamente prático, pelo que os TPMs têm um bloqueio global quando ocorrem demasiadas falhas de autorização.

Uma vez que muitas entidades podem utilizar o TPM, um único êxito de autorização não pode repor a proteção anti-martelada do TPM. Isto impede um atacante de criar uma chave com um valor de autorização conhecido e, em seguida, utilizá-la para repor a proteção do TPM. Os TPMs foram concebidos para esquecer falhas de autorização após um período de tempo, para que o TPM não introduza um estado de bloqueio desnecessariamente. Uma palavra-passe de proprietário do TPM pode ser utilizada para repor a lógica de bloqueio do TPM.

TPM 2.0 anti-martelar

O TPM 2.0 tem um comportamento anti-martelada bem definido. Isto contrasta com o TPM 1.2 para o qual a protecção anti-martelar foi implementada pelo fabricante e a lógica variou bastante em toda a indústria.

Para sistemas com o TPM 2.0, o TPM é configurado pelo Windows para bloquear após 32 falhas de autorização e esquecer uma falha de autorização a cada 10 minutos. Isto significa que um utilizador pode tentar utilizar rapidamente uma chave com o valor de autorização incorreto 32 vezes. Para cada uma das 32 tentativas, o TPM regista se o valor de autorização estava correto ou não. Isto faz com que o TPM entre num estado bloqueado após 32 tentativas falhadas.

As tentativas de utilização de uma chave com um valor de autorização para os próximos 10 minutos não devolveriam êxito ou falha. Em vez disso, a resposta indica que o TPM está bloqueado. Após 10 minutos, uma falha de autorização é esquecida e o número de falhas de autorização memorizadas pelo TPM cai para 31. O TPM deixa o estado bloqueado e regressa ao funcionamento normal. Com o valor de autorização correto, as chaves podem ser utilizadas normalmente se não ocorrerem falhas de autorização durante os próximos 10 minutos. Se decorridos 320 minutos sem falhas de autorização, o TPM não se lembra de falhas de autorização e poderão ocorrer 32 tentativas falhadas novamente.

O Windows não necessita que os sistemas TPM 2.0 se esqueçam de falhas de autorização quando o sistema está totalmente desligado ou quando o sistema está em hibernação. O Windows requer que as falhas de autorização sejam esquecidas quando o sistema está em execução normalmente, num modo de suspensão ou em estados de baixa potência que não estejam desligados. Se um sistema Windows com o TPM 2.0 estiver bloqueado, o TPM deixa o modo de bloqueio se o sistema ficar ativado durante 10 minutos.

A proteção anti-martelada para o TPM 2.0 pode ser totalmente reposta imediatamente ao enviar um comando de reposição de bloqueio para o TPM e ao fornecer a palavra-passe do proprietário do TPM. Por predefinição, o Windows aprovisiona automaticamente o TPM 2.0 e armazena a palavra-passe do proprietário do TPM para utilização pelos administradores de sistema.

Em algumas implementações, o valor de autorização do proprietário do TPM é armazenado centralmente no Active Directory e não no sistema local. Um administrador pode executar `tpm.msc` e optar por repor o tempo de bloqueio do TPM. Se a palavra-passe do proprietário do TPM estiver armazenada localmente, será utilizada para repor o tempo de bloqueio. Se a palavra-passe do proprietário do TPM não estiver disponível no sistema local, o administrador tem de a indicar. Se um administrador tentar repor o estado de bloqueio do TPM com a palavra-passe do proprietário do TPM errada, o TPM não permite outra tentativa de repor o estado de bloqueio durante 24 horas.

O TPM 2.0 permite a criação de algumas chaves sem um valor de autorização associado às mesmas. Estas chaves podem ser utilizadas quando o TPM está bloqueado. Por exemplo, o BitLocker com uma configuração apenas TPM predefinida consegue utilizar uma chave no TPM para iniciar o Windows, mesmo quando o TPM está bloqueado.

Lógica por trás das predefinições

Originalmente, o BitLocker permitia entre 4 e 20 carateres para um PIN. O Windows Hello tem o seu próprio PIN para início de sessão, que pode ter entre 4 e 127 carateres. Tanto o BitLocker como o Windows Hello utilizam o TPM para impedir ataques de força bruta de PIN.

O Windows 10, versão 1607 e os parâmetros de Prevenção de Ataques de Dicionário utilizados anteriormente. Os Parâmetros de Prevenção de Ataques do Dicionário fornecem uma forma de equilibrar as necessidades de segurança com a usabilidade. Por exemplo, quando o BitLocker é utilizado com uma configuração TPM + PIN, o número de estimativas de PIN é limitado ao longo do tempo. Um TPM 2.0 neste exemplo poderia ser configurado para permitir apenas 32 estimativas de PIN imediatamente e, em seguida, apenas mais uma estimativa a cada duas horas. Isto totaliza um máximo de cerca de 4.415 palpites por ano. Se o PIN for de quatro dígitos, todas as combinações de PIN 9999 possíveis podem ser tentadas em pouco mais de dois anos.

A partir do Windows 10, versão 1703, o comprimento mínimo do PIN do BitLocker foi aumentado para seis carateres, para melhor se alinhar com outras funcionalidades do Windows que utilizam o TPM 2.0, incluindo o Windows Hello. Aumentar o comprimento do PIN requer um maior número de estimativas para um atacante. Por conseguinte, a duração do bloqueio entre cada estimativa foi abreviada para permitir que os utilizadores legítimos repetissem uma tentativa falhada mais cedo, mantendo um nível de proteção semelhante. Caso os parâmetros legados para o limiar de bloqueio e o tempo de recuperação precisem de ser utilizados, confirme que o GPO está ativado e configure o sistema para utilizar a definição Parâmetros de Prevenção de Ataques de Dicionário legados para o TPM 2.0.

Smart cards baseados em TPM

O smart card baseado no Windows TPM, que é um smart card virtual, pode ser configurado para permitir o início de sessão no sistema. Ao contrário dos smart cards físicos, o processo de início de sessão utiliza uma chave baseada em TPM com um valor de

autorização. A lista seguinte mostra as vantagens dos smart cards virtuais:

- Os smart cards físicos podem impor o bloqueio apenas para o PIN do smart card físico e podem repor o bloqueio após a introdução do PIN correto. Com um smart card virtual, a proteção anti-martelada do TPM não é reposta após uma autenticação bem-sucedida. O número permitido de falhas de autorização antes de o TPM entrar no bloqueio inclui muitos fatores.
- Os fabricantes de hardware e os programadores de software podem utilizar as funcionalidades de segurança do TPM para cumprir os seus requisitos.
- A intenção de selecionar 32 falhas como limiar de bloqueio é evitar que os utilizadores bloqueiem o TPM (mesmo quando aprendem a escrever novas palavras-passe ou se bloquearem e desbloquearem frequentemente os respetivos computadores). Se os utilizadores bloquearem o TPM, têm de aguardar 10 minutos ou utilizar outras credenciais para iniciar sessão, como um nome de utilizador e palavra-passe.

Comentários

Esta página foi útil? Yes No

Fornecer comentários sobre o produto

Visão Geral do Trusted Platform Module (TPM)

Conheça mais sobre a tecnologia Trusted Platform Module (TPM), entenda como ela torna os computadores mais seguros e saiba por que a atualização para o TPM 2.0 é agora imperativa para todos os usuários do Windows 11.[1]

Principais conclusões:

- Um TPM é um chip de segurança que reside na placa-mãe de um PC ou em seu processador, e aplica recursos de segurança para armazenar informações confidenciais.
- A maioria dos PCs comprados nos últimos cinco anos é compatível com o TPM 2.0.
- Alguns usuários podem precisar habilitar o TPM 2.0 em seus dispositivos, acessando as configurações por meio do BIOS UEFI.

A tecnologia Trusted Platform Module (TPM) mantém os PCs seguros, oferecendo proteção na camada do hardware contra malwares e ataques cibernéticos sofisticados. A tecnologia TPM pode ser incorporada a CPUs modernas e "armazenar com segurança os artefatos usados para autenticar a plataforma".[2] Os artefatos que os TPMs protegem variam de senhas a certificados e impressões digitais, isto é, qualquer informação importante que os usuários desejam que seja armazenada com segurança.

O que é o Trusted Platform Module?

As empresas e os consumidores que fizerem o upgrade para o Windows 11 agora se beneficiarão de novos requisitos de segurança baseados em hardware

, que tornarão seus PCs mais seguros. Um dos requisitos de segurança baseado em hardware é que todos os PCs com Windows 11 precisam ter o TPM 2.0 para executar o sistema operacional.

Um TPM, ou um módulo de plataforma confiável, é uma tecnologia de segurança física ou integrada (microcontrolador) que reside na placa-mãe de um computador ou em seu processador. Os TPMs usam criptografia para

- O Windows 11 requer

que todos os PCs usem o Trusted Platform Module (TPM) 2.0.

Veja os benefícios de economia de custos e negócios

Comentários

armazenar com segurança informações essenciais e cruciais em PCs para permitir a autenticação da plataforma. Eles armazenam uma variedade de informações confidenciais (como credenciais de usuários, senhas, impressões digitais, certificados, chaves de criptografia ou outros documentos importantes para o consumidor) por trás de uma barreira de hardware para mantê-las protegidas contra ataques externos.

Embora o uso da tecnologia TPM faça parte da TI empresarial há mais de uma década, esta é uma das primeiras instâncias da Microsoft que exige seu uso para todos, incluindo pequenas e médias empresas, bem como consumidores.

As implementações do TPM são tipicamente projetadas para atender a um padrão internacional criado pelo Trusted Computing Group (TCG) . O TCG é um consórcio do setor de informática que criou o padrão TPM original, posteriormente adotado pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC), e então classificado como ISO/IEC 11889 .

Como Funciona o TPM?

O TPM gera e armazena partes de chaves de criptografia para PCs.

A título de exemplo de como um TPM funciona, considere a etapa de ativação de um dispositivo, como um notebook. Quando o dispositivo é ligado, o TPM autentica-o. O TPM fornece uma chave criptográfica para desbloquear a unidade criptografada e, se a chave for validada, o computador inicializará normalmente. Se a chave criptográfica for adulterada, o computador não será inicializado.

Por que Preciso de um TPM?

Os ataques cibernéticos estão em um nível mais alto, e as habilidades dos hackers estão ficando mais sofisticadas a cada dia. O TPM é uma tecnologia que ajuda as empresas a combaterem esses ataques. Além disso, é importante contar com um PC capaz de executar o TPM 2.0 para atender ao

novo requisito do TPM 2.0

da Microsoft para o sistema operacional Windows 11

.

Requisito do TPM 2.0 para o Windows 11

Em adição aos outros requisitos de processador, RAM, armazenamento e firmware, o uso do Windows 11 em um PC requer o TPM versão 2.0

.

O requisito do TPM 2.0 visa elevar a linha de base de segurança do Windows dos milhões de PCs individuais usados em todo o mundo. Isso ajudará a manter todos os usuários de computadores mais seguros e, ao mesmo tempo, tornará muito mais difícil para os hackers cometerem crimes cibernéticos.

Leia mais sobre o requisito do TPM 2.0 no Windows 11

Comentários

Como Posso Saber se o Meu PC já Tem o TPM 2.0?

A boa notícia é que, se você comprou um PC nos últimos anos, é altamente provável que você já tenha um TPM instalado no seu computador capaz de executar o TPM 2.0. No entanto, é possível que o seu TPM tenha sido desligado no firmware pelo fabricante do computador e possa exigir que você o habilite para atender ao novo requisito.

Se o seu computador for baseado na família de processadores Intel® Core™ da 8ª Geração ou posterior

, você pode ficar tranquilo, sabendo que o seu sistema inclui a Intel® Platform Trust Technology (Intel® PTT)

, um TPM integrado compatível com as especificações da versão 2.0. A Intel® PTT oferece os mesmos recursos de um TPM dedicado, mas reside no firmware do sistema, dispensando, assim, a necessidade de recursos de processamento ou memória dedicados.

Verifique se o seu modelo de processador Intel® específico é compatível com os novos dispositivos Windows 11

Como Atualizar para o TPM 2.0

Caso tenha comprado um PC recentemente, a atualização para o TPM 2.0 deve ser relativamente fácil, pois o seu sistema já deve ter um TPM instalado capaz de executá-lo.

Siga estas etapas recomendadas pela Microsoft

para habilitar o TPM 2.0 no seu PC:

1. Confirme se o seu computador é elegível

   para atualizar para o Windows 11.
2. Após a confirmação da elegibilidade, escolha uma das duas opções

   para verificar se o seu TPM satisfaz os requisitos do Windows 11.
   - Opção 1: use o aplicativo de segurança do Windows.
   - Opção 2: use o Console de Gerenciamento da Microsoft.
3. Se concluir que precisa habilitar o TPM

   na sua máquina, você precisará acessar as configurações gerenciadas no BIOS UEFI.

Comentários

- Se não souber como fazer alterações nas configurações do TPM, recomendamos verificar as informações de suporte do fabricante do seu PC. Os links para as informações de suporte de alguns fabricantes comuns incluem:
  - ASUS
  - Dell
  - HP
  - Lenovo
  - Microsoft Surface

Permanecer Seguro no Cenário Atual Requer o TPM 2.0

A segurança cibernética hoje é tudo menos constante. Os hackers estão ficando mais sofisticados a cada hora. Os ataques estão acelerando, e os custos ultrajantes associados a crimes cibernéticos e violações de segurança podem facilmente prejudicar as empresas. Para as empresas que desejam enfrentar esses desafios e permanecer seguras, a atualização para o TPM 2.0 é imperativa. Além de fornecer segurança profunda e baseada em hardware, ele também garante que o seu PC esteja pronto para atualizar para o Windows 11 quando você estiver pronto para dar a partida.

Perguntas frequentes

O que é o TPM?

Como o TPM funciona?

O meu PC possui o TPM 2.0?

Benefícios de Segurança da Intel vPro® Enterprise para Windows

A Intel vPro® foi projetada para empresas, fornecendo recursos de segurança aprimorados por hardware que ajudam a proteger todas as camadas da pilha de computação. As empresas podem aproveitar a transparência e a rastreabilidade da cadeia de suprimento de componentes de PC, verificações avançadas de memória e suporte baseado em hardware dos serviços de segurança do Windows 11. Além disso, a área de TI tem a capacidade de implementar rapidamente correções de software em vulnerabilidades cruciais para PCs gerenciados.

Conheça a plataforma Intel vPro®

Comentários

Segurança de Pontos de Extremidade

Pontos de extremidade são os portais que os hackers usam para acessar os seus dados cruciais ou inserir um código mal-intencionado nos seus sistemas. O ambiente de trabalho atual tem uma grande variedade de dispositivos capazes de desafiar a segurança dos pontos de extremidade. Integrado a todos os PC Windows com Intel vPro®, o Intel® Hardware Shield

Hardening do Sistema

A TI geralmente usa a proteção do sistema para otimizar sua estratégia de segurança de terminais, e o Intel® Hardware Shield torna esse processo mais abrangente. Os benefícios para a sua organização incluem proteção configurável de firmware, segurança do BIOS para reduzir a sua superfície de ataque e detecção avançada de

Patches de Segurança e Remediação de Ameaças

A Intel® Active Management Technology (Intel® AMT)

, exclusiva da Intel vPro® Enterprise para Windows, permite acesso e gerenciamento remotos em toda a organização. A sua equipe de TI pode usar essas tecnologias para executar correções de segurança e remediação de ameaças em tempo hábil. Os patches de segurança podem atualizar grandes

permite que a sua equipe de TI implemente políticas na camada do hardware para garantir que, se um código malicioso for injetado, ele não possa acessar dados.

ameaças

.

populações de dispositivos, independentemente de sua localização. A remediação de ameaças é conduzida com a implementação de contramedidas para ajudar a reduzir a suscetibilidade de um ponto de extremidade a um ataque específico.

Tópicos de segurança relacionados

- O gerenciamento eficaz de patches protege sua empresa
- O fortalecimento do PC reduz as vulnerabilidades de segurança
- Os recursos de segurança baseados em hardware protegem sua empresa
- Proteja os dispositivos para garantir a produtividade com segurança nos terminais
- A tecnologia de módulo de plataforma confiável mantém os PCs seguros
- Proteja a infraestrutura de TI virtualizada com segurança de virtualização
- Pequenas empresas: proteja os terminais contra ameaças cibernéticas
- Os recursos de segurança protegem contra ataques de dia zero

Comentários

Saiba Mais Sobre os Tópicos de PCs Empresariais

Segurança Baseada em Hardware

Soluções de Implantação de Imagens de PC

Tecnologia de Gerenciamento Remoto

Desempenho de PC Premium

Recursos para Profissionais de TI

Informações de produto e desempenho

[1] As tecnologias Intel® podem exigir ativação de hardware, software específico ou de serviços. Nenhum produto ou componente pode ser totalmente seguro. A Intel não controla ou audita dados de terceiros. Você deve consultar outras fontes para avaliar a precisão. Os custos e resultados podem variar. © Intel Corporation. Intel, o logotipo Intel e outras marcas Intel são marcas comerciais da Intel Corporation ou de suas subsidiárias. Outros nomes e marcas podem ser propriedade de outras empresas.

[2] "Trusted Platform Module (TPM) Summary," Trusted Computing Group, https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/

Informações sobre a empresa

Nosso compromisso

Diversidade e inclusão

Relações com investidores

Fale conosco

Sala de imprensa

Mapa do site

Empregos

Comentários

As tecnologias Intel® podem exigir ativação de hardware, software específico ou de serviços. // Nenhum produto ou componente pode ser totalmente seguro. // Os seus custos e resultados podem variar. // O desempenho varia de acordo com o uso, a configuração e outros fatores. // Veja nossos Avisos e isenções de responsabilidade legais completos . // A Intel está comprometida em respeitar os direitos humanos e evitar cumplicidade com abusos de direitos humanos. Consulte Princípios Globais de Direitos Humanos da Intel. Os produtos e software da Intel são destinados a serem utilizados apenas em aplicações que não causem ou contribuam com a violação de um direito humano reconhecido internacionalmente.

Comentários

Recomendações do TPM

Artigo • 15/07/2024 • Aplica-se a: ✅ Windows 11, ✅ Windows 10, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Este artigo fornece recomendações para a tecnologia Trusted Platform Module (TPM) para Windows.

Para obter uma descrição do recurso básico do TPM, consulte a Visão geral da tecnologia Trusted Platform Module.

Design e implementação do TPM

Tradicionalmente, os TPMs são chips discretos vendidos na placa principal de um computador. Estas implementações permitem que o fabricante de equipamento original (OEM) do computador avalie e certifique o TPM separado do resto do sistema. As implementações discretas do TPM são comuns. No entanto, podem ser problemáticos para dispositivos integrados que são pequenos ou têm baixo consumo de energia. Algumas implementações de TPM mais recentes integram a funcionalidade TPM no mesmo chipset que outros componentes da plataforma, embora ainda forneçam separação lógica semelhante a chips TPM discretos.

Os TPMs são passivos: eles recebem comandos e retornam respostas. Para obter todos os benefícios de um TPM, o OEM deve integrar cuidadosamente o hardware e o firmware do sistema ao TPM para enviar comandos a ele e reagir às suas respostas. Os TPMs foram originalmente concebidos para proporcionar benefícios de segurança e privacidade aos proprietários e utilizadores de uma plataforma, mas as versões mais recentes podem proporcionar benefícios de segurança e privacidade ao próprio hardware do sistema. Antes de ser usado para cenários avançados, entretanto, um TPM deve ser provisionado. O Windows aprovisiona automaticamente um TPM, mas se o utilizador estiver a planear reinstalar o sistema operativo, poderá ter de limpar o TPM antes de reinstalar para que o Windows possa tirar o máximo partido do TPM.

O TCG (Trusted Computing Group) é uma organização sem fins lucrativos que publica e mantém a especificação TPM. O TCG existe para desenvolver, definir e promover normas da indústria globais neutras em termos de fornecedores. Estas normas suportam uma raiz de confiança baseada em hardware para plataformas de computação fidedignas interoperáveis. O TCG também publica a especificação TPM, como o padrão internacional ISO/IEC 11889, usando o processo de envio de especificação publicamente disponível

que o Joint Technical Committee 1 define entre a ISO (Organização Internacional de Normalização) e o IEC (International Electrotechnical Commission).

Os OEMs implementam o TPM como um componente em uma plataforma de computação confiável, como um computador, tablet ou telefone. As plataformas de computação fidedignas utilizam o TPM para suportar cenários de privacidade e segurança que o software por si só não consegue alcançar. Por exemplo, o software por si só não pode comunicar de forma fiável se o software maligno está presente durante o processo de arranque do sistema. A integração próxima entre o TPM e a plataforma aumenta a transparência do processo de inicialização e dá suporte à avaliação da integridade do dispositivo habilitando a medição e o relatório do software que inicia o dispositivo confiável. A implementação de um TPM como parte de uma plataforma de computação fidedigna fornece uma raiz de hardware de confiança, ou seja, comporta-se de forma fidedigna. Por exemplo, se uma chave armazenada num TPM tiver propriedades que não permitem exportar a chave, essa chave não pode realmente sair do TPM.

O TCG projetou o TPM como uma solução de segurança de mercado de massa de baixo custo que atende aos requisitos de diferentes segmentos de clientes. Existem variações nas propriedades de segurança de diferentes implementações de TPM, assim como existem variações em requisitos regulatórios e de clientes e para diferentes setores. Nos contratos públicos, por exemplo, alguns governos definem claramente os requisitos de segurança para os TPMs, enquanto outros não.

Comparação do TPM 1.2 x 2.0

A partir de um padrão do setor, a Microsoft tem sido líder do setor na mudança e uniformização no TPM 2.0, que tem muitos benefícios importantes realizados em algoritmos, criptografia, hierarquia, chaves de raiz, autorização e RAM NV.

Por que o TPM 2.0?

Produtos e sistemas TPM 2.0 têm vantagens de segurança importantes em relação ao TPM 1.2, inclusive:

- A especificação do TPM 1.2 só possibilita o uso de RSA e do algoritmo de hash SHA-1.

- Por motivos de segurança, algumas entidades estão se afastando de SHA-1. Nomeadamente, o NIST exige que muitas agências federais mudem para SHA-256 a partir de 2014, e os líderes tecnológicos, incluindo a Microsoft e a Google, removeram o suporte para assinaturas ou certificados baseados em SHA-1 em 2017.
- O TPM 2.0 **permite mais agilidade criptográfica** por ser mais flexível em relação a algoritmos criptográficos.
  - O TPM 2.0 dá suporte a algoritmos mais novos, que podem melhorar o desempenho de assinatura e a geração de chave. Para obter a lista completa de algoritmos compatíveis, consulte o Registro de algoritmo TCG. Alguns TPMs não suportam todos os algoritmos.
  - Para obter a lista de algoritmos compatíveis com o Windows no provedor de armazenamento criptográfico da plataforma, consulte Provedores de algoritmos de criptografia CNG.
  - O TPM 2.0 obteve a padronização ISO (11889:2015 ISO/IEC).
  - O uso do TPM 2.0 pode ajudar a eliminar a necessidade de OEMs abrir uma exceção a configurações padrão para determinados países e regiões.
- O TPM 2.0 oferece uma **experiência mais consistente** em implementações diferentes.
  - As implementações do TPM 1.2 têm configurações de política variadas. Isso pode resultar em problemas de suporte porque as políticas de bloqueio variam.
  - A política de bloqueio do TPM 2.0 é configurada pelo Windows, garantindo uma proteção contra ataques de dicionário consistente.
- Enquanto as partes do TPM 1.2 são componentes de silício discretos, normalmente vendido na placa principal, o TPM 2.0 está disponível como um componente de silício **discreto (dTPM)** num único pacote de semicondutores, um componente **integrado** incorporado num ou mais pacotes de semicondutores , juntamente com outras unidades lógicas nos mesmos pacotes e como um componente baseado em **firmware (fTPM)** em execução num ambiente de execução fidedigno (TEE) num SoC para fins gerais.

> **Observação**
>
> Não há suporte para o TPM 2.0 nos modos Herdado e CSM do BIOS. Os dispositivos com TPM 2.0 devem ter seu modo BIOS configurado apenas como UEFI nativo. As opções do Módulo de Suporte herdado e de compatibilidade (CSM) devem ser desabilitadas. Para maior segurança, habilite o recurso Inicialização Segura.

O sistema operacional instalado no hardware no modo herdado impedirá que o sistema operacional seja inicializado quando o modo BIOS for alterado para a UEFI. Use a ferramenta **MBR2GPT** antes de alterar o modo BIOS que preparará o sistema operacional e o disco para dar suporte à UEFI.

TPM Discreto, Integrado ou De Firmware?

Há três opções de implementação para TPMs:

- Chip TPM discreto como um componente separado no seu próprio pacote de semicondutores.
- Solução TPM integrada, com hardware dedicado integrado num ou mais pacotes de semicondutores juntamente, mas logicamente separados de outros componentes.
- Solução TPM de firmware, a executar o TPM em firmware num modo de Execução Fidedigna de uma unidade de computação para fins gerais.

O Windows usa qualquer TPM compatível da mesma forma. A Microsoft não toma uma posição sobre a forma como um TPM deve ser implementado e existe um vasto ecossistema de soluções TPM disponíveis, que devem corresponder a todas as necessidades.

Existe alguma importância do TPM para os consumidores?

Para os consumidores finais, o TPM está em segundo plano, mas continua a ser relevante. O TPM é usado para o Windows Hello, o Windows Hello para Empresas e, no futuro, será um componente de vários outros recursos de segurança importantes no Windows. O TPM protege o PIN, ajuda a encriptar palavras-passe e baseia-se na nossa história geral da experiência do Windows para a segurança como um pilar crítico. O uso do Windows em um sistema com um TPM permite um nível mais amplo e profundo de cobertura de segurança.

Conformidade do TPM 2.0 para Windows

Windows para edições de ambiente de trabalho (Home, Pro, Enterprise e Education)

- Desde 28 de julho de 2016, todos os novos modelos, linhas ou séries de dispositivos (ou se estiver a atualizar a configuração de hardware de um modelo, linha ou série existente com uma atualização principal, como CPU, placas gráficas) têm de implementar e ativar por predefinição o TPM 2.0 (detalhes na secção 3.7 da página Requisitos mínimos de hardware). O requisito para habilitar o TPM 2.0 aplica-se somente à fabricação de novos dispositivos. Para obter recomendações do TPM sobre recursos específicos do Windows, consulte TPM e recursos do Windows.

IoT Core

- O TPM é opcional no IoT Core.

Windows Server 2016

- O TPM é opcional para SKUs do Windows Server, a menos que o SKU cumpra os outros critérios de qualificação (AQ) para o cenário dos Serviços Guardião de Anfitrião, caso em que é necessário o TPM 2.0.

TPM e recursos do Windows

A tabela a seguir define quais recursos do Windows exigem suporte a TPM.

Expandir a tabela

Recursos do Windows	TPM necessário	Suporte a TPM 1.2	Suporte a TPM 2.0	Detalhes
Inicialização Medida	Sim	Sim	Sim	O Arranque Medido requer O TPM 1.2 ou 2.0 e o Arranque Seguro UEFI. O TPM 2.0 é recomendado, uma vez que suporta algoritmos criptográficos mais recentes. O TPM 1.2 só suporta o algoritmo SHA-1, que está a ser preterido.
BitLocker	Não	Sim	Sim	O TPM 1.2 ou 2.0 é suportado, mas recomenda-se o TPM 2.0. A Encriptação de Dispositivos necessita do Modo de Espera Moderno , incluindo suporte para o TPM 2.0
Criptografia do dispositivo	Sim	N/D	Sim	A Criptografia de Dispositivo requer a certificação Modern Standby/Connected Standby, que exige TPM 2.0.
Controlo de Aplicações do Windows Defender (Device Guard)	Não	Sim	Sim	
System Guard (DRTM)	Sim	Não	Sim	É necessário firmware TPM 2.0 e UEFI.
Credential Guard	Não	Sim	Sim	O Windows 10, versão 1507 (fim da vida útil a partir de maio de 2017) oferece suporte somente a TPM 2.0 para o Credential Guard. A partir do Windows 10, versão 1511, há suporte para TPM 1.2 e 2.0. Emparelhado com o System Guard, o TPM 2.0 fornece segurança melhorada para o Credential Guard. Por predefinição, o Windows 11 requer o TPM 2.0 para facilitar a ativação desta segurança melhorada para os clientes.
Atestado de Integridade do Dispositivo	Sim	Sim	Sim	O TPM 2.0 é recomendado, uma vez que suporta algoritmos criptográficos mais recentes. O TPM 1.2 só suporta o algoritmo SHA-1, que está a ser preterido.
Windows Hello/Windows Hello para Empresas	Não	Sim	Sim	A associação ao Microsoft Entra suporta ambas as versões do TPM, mas requer o TPM com o código de autenticação de mensagens com chave hash (HMAC) e o certificado de Chave de Endossamento (EK) para o suporte de atestado de chaves. O TPM 2.0 é recomendado através do TPM 1.2 para um melhor desempenho e

Recursos do Windows	TPM necessário	Suporte a TPM 1.2	Suporte a TPM 2.0	Detalhes
				segurança. O Windows Hello como um autenticador de plataforma FIDO tira partido do TPM 2.0 para armazenamento de chaves.
Inicialização segura da UEFI	Não	Sim	Sim	
Provedor de armazenamento de chaves do provedor de criptografia da plataforma TPM	Sim	Sim	Sim	
Cartão inteligente virtual	Sim	Sim	Sim	
Armazenamento de certificados	Não	Sim	Sim	TPM é necessário somente quando o certificado é armazenado no TPM.
Autopilot	Não	N/D	Sim	Se pretender implementar um cenário, que requer TPM (como o modo de implementação automática e luva branca), é necessário firmware TPM 2.0 e UEFI.
SecureBIO	Sim	Não	Sim	É necessário firmware TPM 2.0 e UEFI.

Status de OEM em disponibilidade do sistema TPM 2.0 e peças certificadas

Os clientes públicos e corporativos em setores regulamentados podem ter padrões de aquisição que exijam o uso de peças TPM certificadas em comum. Com isso, os OEMs, que fornecem os dispositivos, talvez precisem usar apenas componentes TPM certificados nos sistemas de classe comercial. Para obter mais informações, entre em contato com o OEM ou o fornecedor de hardware.

Comentários

Esta página foi útil? Yes No

Fornecer comentários sobre o produto

TPM (Trusted Platform Module) – Tudo o que precisa saber

No Windows 11, a TPM (Trusted Platform Module), tornou-se um pré-requisito para prosseguir com a sua instalação.

Criado pela TCG (Trusted Computing Group), uma organização sem fins lucrativos, a TPM (Módulo de Plataforma Confiáve), é um microchip de criptografia implementado na placa-mãe do computador. com a finalidade de fornecer maior segurança e privacidade ao usuário, garantindo que não houve violações ou adulterações no sistema operacional durante o seu processo de boot.

ARTIGOS ALEATÓRIOS

Redação PTI

ESET lança solução de gerenciamento de segurança baseada em nuvem para empresas de todos os portes

Vitor Vidal

Banco Britânico troca senhas por biometria de íris

Marcos Henrique

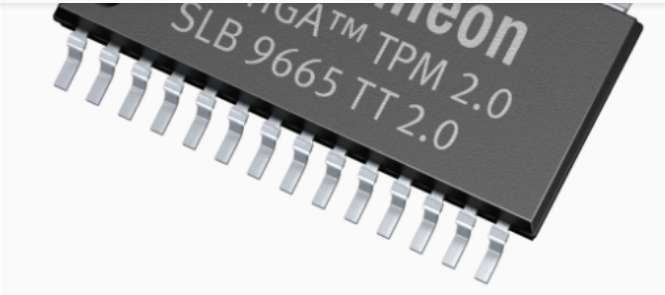
Acesso via SSH com validação do Google Authenticator

M

Segurança da Informação: Privacidade das Crianças na Internet

William Meller

É difícil começar a carreira em gerenciamento de projetos?



A versão do chip TPM tem que ser a depois 2.0 ou superior, requer que nas configurações da BIOS, o boot esteja no modo UEFI e que o Windows a ser instalado seja na versão 64 bits.

Como funciona?

Durante o processo de boot do sistema, O TPM gera e armazena chaves criptográficas que só podem ser decodificados através de softwares específicos e autorizados.

As informações armazenadas nestas chaves criptografadas são firmwares, componentes do sistema operacional entre outras opções relevantes que podem ser medidos e armazenados dentro destas chaves criptografadas, garantindo assim a integridade na inicialização do sistema, impedindo assim que software mal intencionados violem e tenham acesso a estas informações.

Por que é um pré-requisito ao Windows 11

O TPM já estava nos requisitos do Windows 10, porém não era obrigatório para a sua instalação. Agora no Windows 11, tornou-se obrigatório devido o aumento significativo de ataques de fishing e tentativas de instalações de softwares mal intencionados. A segurança do sistema é baseada em hardware.

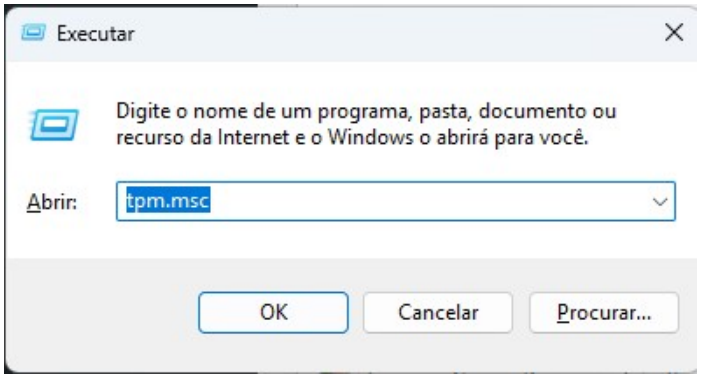
madas dentro do chip

- Ajuda a garantir a integridade da plataforma, usando e armazenando medidas de segurança no processo de boot.

Problemas com o chip TPM?

Caso tenha problemas com recursos do TPM no Windows e queira fazer uma instalação limpa do Sistema Operacional para corrigir problemas do TPM, antes de mais nada, podemos utilizar o "Console de Gerenciamento do TPM" e limpá-lo.

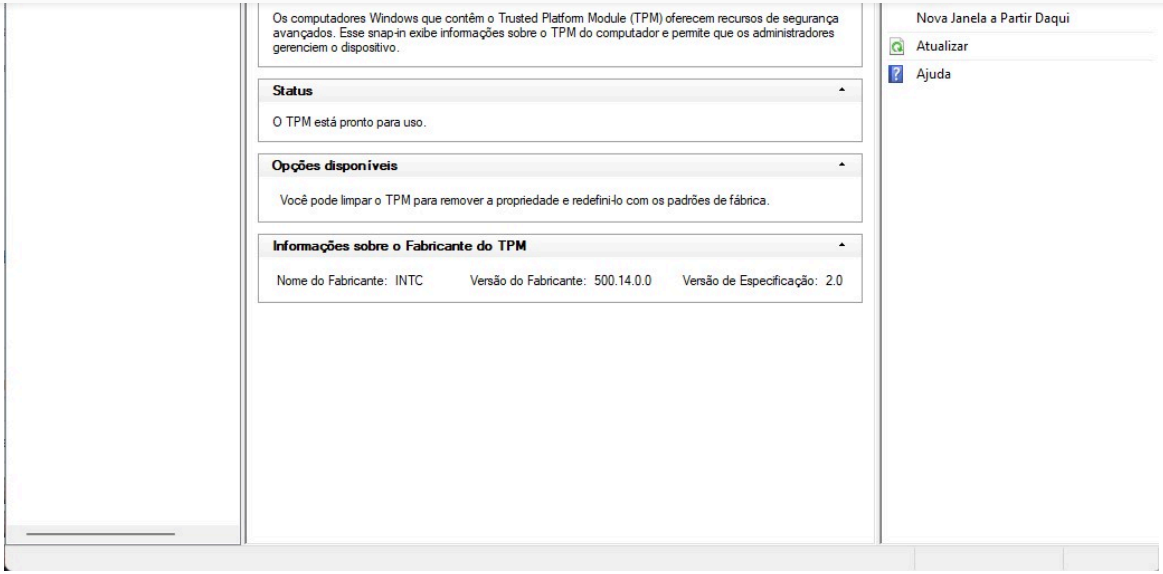
Para isso iremos abrir a janela "Executar" pressionando as teclas (Windows R), digitar "tpm.msc" e clicar em "OK".



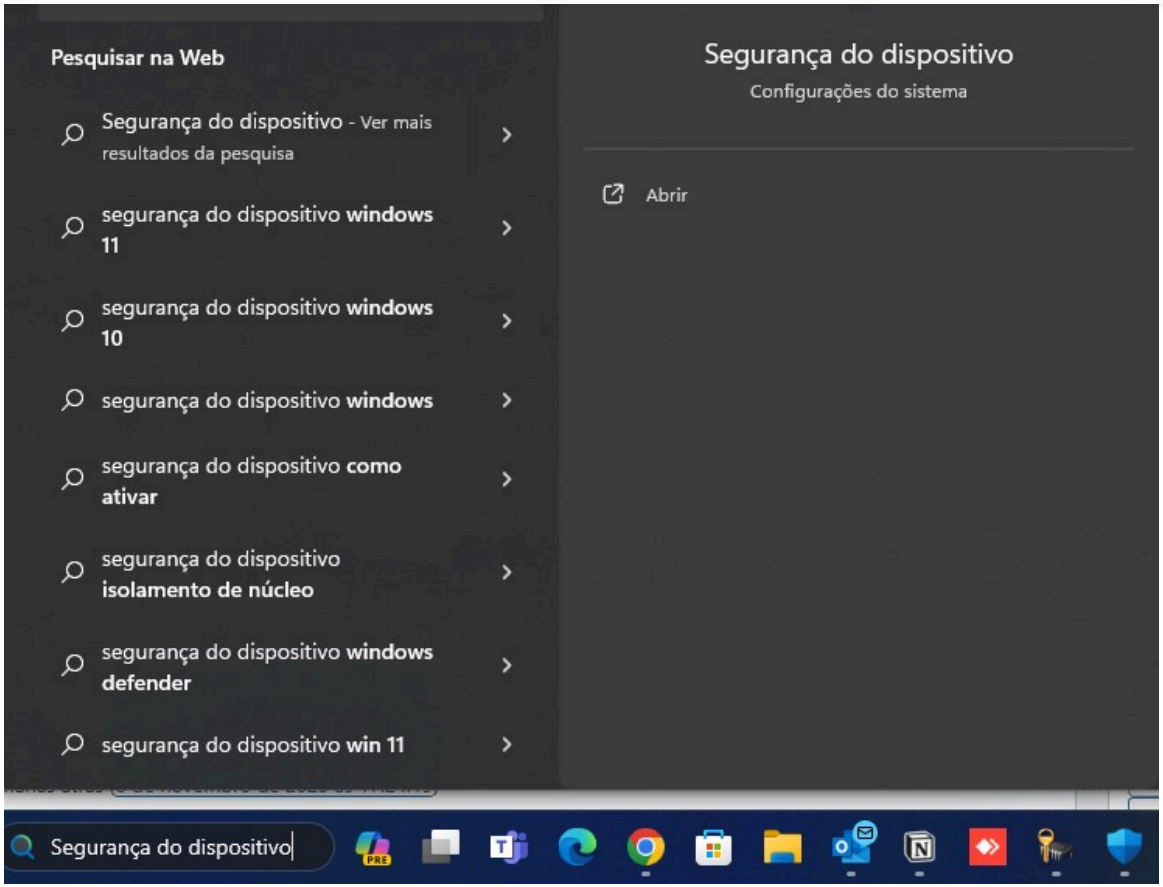
Abrirá a janela do Console de Gerenciamento como é mostrada na imagem abaixo.

Ao clicar em "Limpar TPM" que está na parte superior da coluna da direita, excluirá todas as chaves armazenadas, excluíndo assim todas as informações do seu proprietário, deixando assim este chip

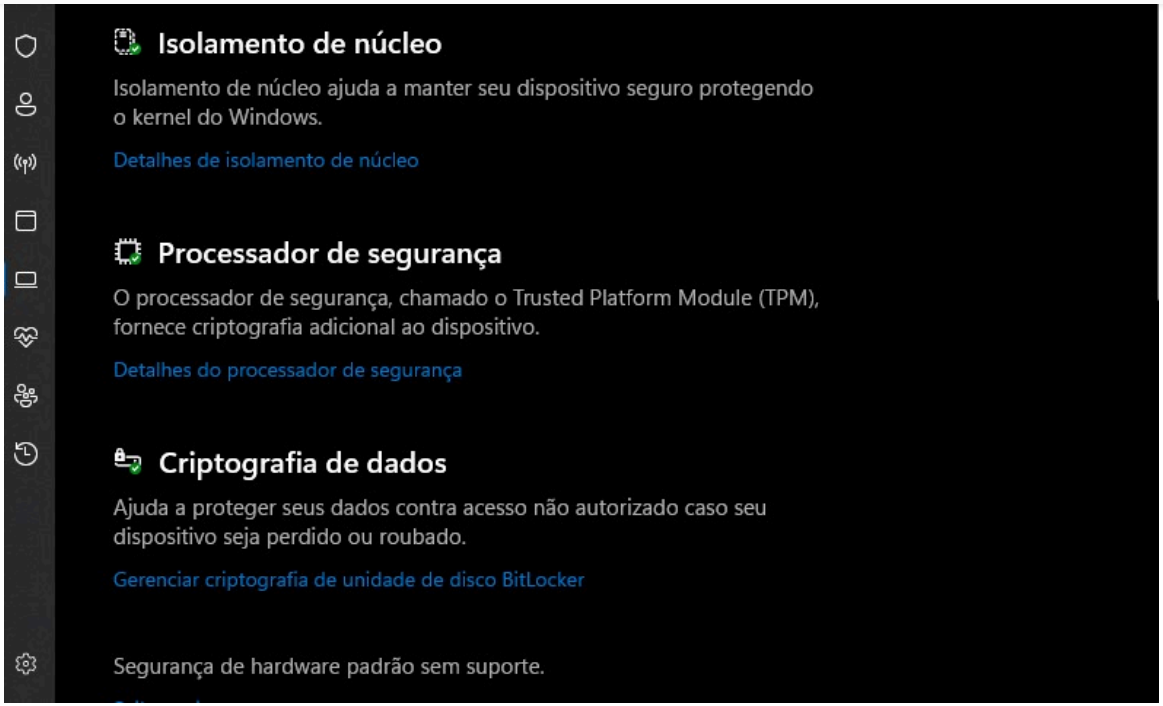
Mas devemos ter o máximo de cuidado, utilizando esta opção se realmente for necessário e é importante ler o manual do fabricante do computador sobre o hardware TPM antes de limpá-lo.



Outra forma de resolver problemas do TPM e limpá-lo é digitar “Segurançã do dispositivo” no campo “Pesquisar” da barra de tarefas e selecionar opção correspondente à pesquisa.



Ao abrir a janela “Segurança do dispositivo”, clicar em “Detalhes do Processador de Segurança”.

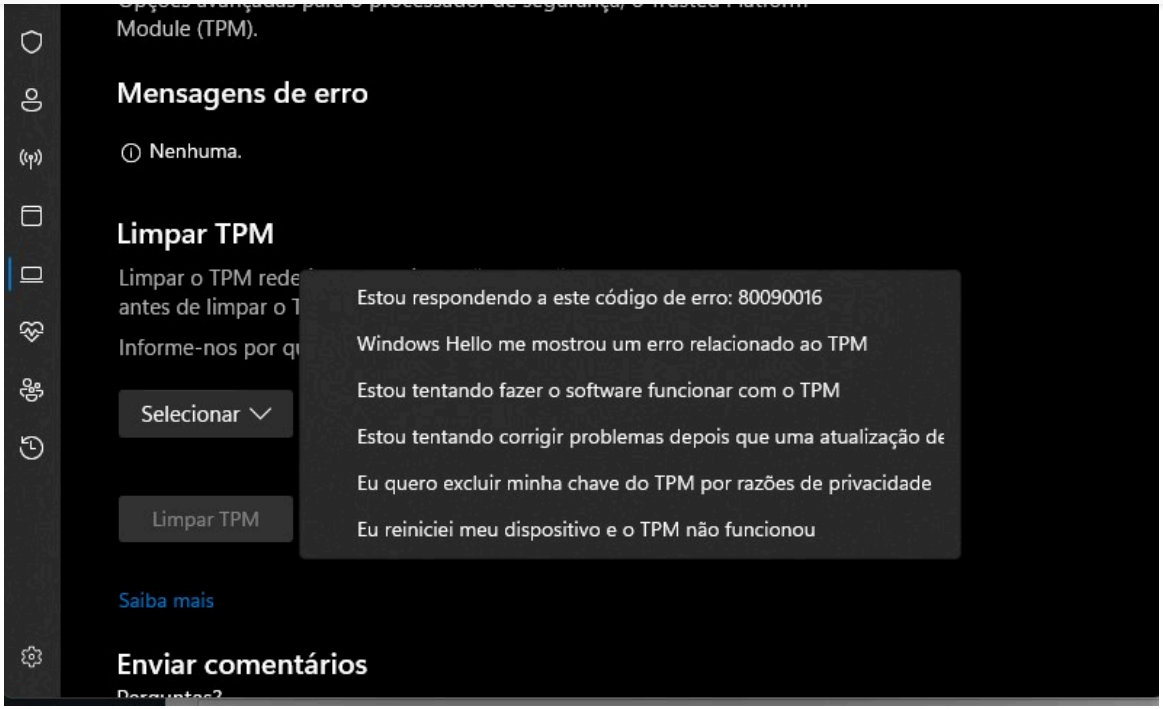


Ao entrar em “Detalhes do processador de segurança”, clicaremos em “Solução de problemas do processador de segurança”.

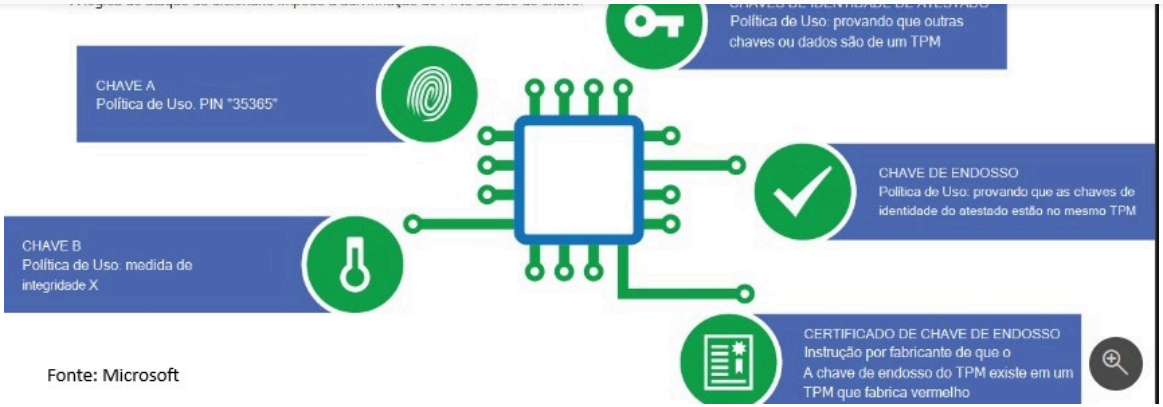
Abrirá as opçãos avançadas da solução de problemas.

Em selecionar, escolheremos a opção do motivo de limpeza e depois clicaremos em “Limpar TPM”. Será solicitado para reiniciarmos o computador e assim o TPM estará sem nenhuma informação e pronto para o uso no Windows.

Neste caso pode ser que não precise instalar novamente o sistema, mas é bom estar preparado para qualquer eventualidade, tendo o dispositivo de boot para instalação do Windows e com os backups feitos.



Logo abaixo, está um gráfico monstrando como o Windows utiliza o TPM.



Aqui passei alguns pontos importantes sobre o chip de criptografia TPM.

Tem fabricantes de computadores e laptops que já possuem o TPM discreto, ou seja, sem aparecer na BIOS e outros que precisam ativá-los na BIOS caso necessite.

Aqui no PTI, tem um artigo meu, sobre como instalar o Windows 11 que possui maiores detalhes para a configuração da BIOS para a instalação do sistema.

Este artigo é o resultado de estudos em diversos sites para trazer de forma mais esclarecida sobre este chip de segurança. Caso tenha algum complemento ou ajuste, deixe seu comentário abaixo.

Luciano Gusso

Trabalhando há mais de 20 anos na área de TI, prestando suporte técnico e consultoria a empresas e usuários finais.

CONTEÚDOS RELACIONADOS

Ticiano Benetti

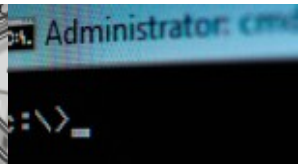
Inteligência em Segurança da Informação

Yuri Ladeia

A necessidade jurídica e técnica de Avaliar o Impacto à proteção de dados (AIPD/DPIA) nos setores da Saúde e Financeiro

Gustavo de

Ransomware: como mitigar os riscos envolvidos



José Ferreira

Erro ao instalar qualquer versão do Microsoft Office: Problema e Solução

Desenvolvimento de Software

Gerência de Projetos

Governança de TI

Carreira

Certificação

Segurança

Infraestrutura

Engenharia de Software

Cargos de TI

Crimes Digitais

Dinheiro

Direito

Educação

Empreendedorismo

Emprego

Equipamentos

Games

Gestão do Conhecimento

ITIL

Mercado

Papinho de TI

Redes

Software Livre

Suporte

Tendências