**RECURSO ADMINISTRATIVO**

**Pregão Eletrônico nº 002/2026/NCP/ALE/RO**

**Processo Administrativo nº 100.173.000006/2026-97**

**UASG 926919 – Grupo 1**

**Recorrente: NETSAFE CORP LTDA – CNPJ nº 03.476.184/0002-30**

**Recorrida/licitante aceita: ESYWORLD SISTEMAS E INFORMÁTICA LTDA – CNPJ nº 03.899.222/0001-86**

**Órgão: Assembleia Legislativa do Estado de Rondônia – ALE/RO**

**NETSAFE CORP LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº **03.476.184/0002-30**, com endereço indicado nos autos, neste ato representada por seu representante legal e/ou procurador infra-assinado, com fundamento no art. 165, inciso I, da Lei nº 14.133/2021, no edital, no Termo de Referência, no Caderno de Especificações Técnicas e nos princípios da legalidade, isonomia, julgamento objetivo, vinculação ao edital, motivação, razoabilidade, proporcionalidade, competitividade, segurança jurídica e seleção da proposta mais vantajosa, interpor o presente **RECURSO ADMINISTRATIVO** em face da decisão que desclassificou sua proposta e da posterior aceitação/habilitação da empresa ESYWORLD SISTEMAS E INFORMÁTICA LTDA, pelas razões a seguir expostas.

## 1. Tempestividade e efeito suspensivo

A NETSAFE registrou intenção de recurso em 09/06/2026. O relatório do sistema registra, ainda, que o Grupo 1 permaneceu “aberto para recursos” e que a fase recursal foi instaurada após a sessão de 09/06/2026.

Nos termos do art. 165 da Lei nº 14.133/2021, cabe recurso contra o julgamento das propostas e contra atos de habilitação/inabilitação, observado o prazo legal. O art. 168 da mesma lei confere efeito suspensivo ao recurso e ao

pedido de reconsideração até a decisão final pela autoridade competente. Assim, o presente recurso deve ser recebido como tempestivo e processado com efeito suspensivo.

## 2. Síntese objetiva dos fatos

O objeto do certame é o registro de preços para contratação de solução de prevenção contra vazamento de informações em meio digital – Data Loss Prevention – DLP, com fornecimento de licenças de software, implantação, configuração, repasse de conhecimento, suporte técnico e garantia do fabricante.

Em 28/05/2026, a NETSAFE foi desclassificada, sob o fundamento de suposto não atendimento aos subitens 1.1, 1.9.2, 1.9.3, 1.11.2, 1.11.3, 1.12.1, 1.13.4, 1.13.11, 1.13.17, 1.14.1, 1.14.2, 1.14.3, 1.14.4 e 1.14.5 do Caderno de Especificações Técnicas, além do subitem 4.20.1 do Termo de Referência, "**conforme parecer técnico fundamentado emitido pela STI**".

O relatório não foi disponibilizado no processo, em que pese o requerimento formal da Netsafe m 11/06/2026. Ou seja, o ato administrativo careceu de motive e fundamento, tendo apenas, apenas a conclusão de não atendimento.

Posteriormente, a ESYWORLD foi aceita e habilitada, embora a própria Administração tenha registrado inconsistências relevantes, incluindo documentação com características idênticas às da NCT, divergência entre proposta comercial/técnica indicando SAFETICA e arquivo PAP com composição de licenciamento e part numbers correspondentes à solução FORCEPOINT, além de referência a outro órgão e outro pregão.

A ESYWORLD chegou a informar que havia anexado planilha PAP incorreta e requereu a reabertura do campo de anexos para substituir os arquivos e anexar versões corretas.

Anote-se que nada disso foi registrado como diligência no portal de contratações, tudo foi feito via CHAT, tendo sido oportunizada a alteração da substância de proposta, o que é vedado por lei.

## 3. Preliminar — necessidade de juntada e disponibilização do parecer técnico integral da STI

A decisão recorrida remete a “parecer técnico fundamentado emitido pela STI”, mas o relatório da sessão apenas lista os itens supostamente não atendidos.

O parecer integral, com assinatura digital, como manda a Lei, com análise item a item, não foi localizado nos documentos disponibilizados, ferindo o princípio do contraditório e ampla defesa.

### Informação não localizada nos documentos disponibilizados.

A ausência de motivação acessível prejudica o contraditório e a ampla defesa, pois impede a NETSAFE de conhecer precisamente: qual documento foi desconsiderado; qual trecho foi reputado insuficiente; qual interpretação técnica foi adotada; se houve ou não análise dos catálogos, links e declarações apresentados; e se a exigência foi lida de modo funcional ou restritivo.

Nos termos da Lei nº 9.784/1999, atos que neguem, limitem ou afetem direitos ou interesses devem ser motivados com indicação dos fatos e fundamentos jurídicos.

Requer-se, portanto, a declaração de nulidade da decisão que desclassificou a Netsafe, pela falta de juntada do suposto parecer técnico integral da STI, com assinatura digital para verificação de data e hora do ato administrativo e sua disponibilização à recorrente.

## 4. Mérito — ilegalidade e inconsistência da desclassificação da NETSAFE

### 4.1. O julgamento técnico deve ser objetivo, motivado e aderente ao requisito funcional

O Caderno Técnico estabelece requisitos funcionais.

O próprio Termo de Referência afirma que não há indicação de preferência por marca/modelo e que as especificações foram

definidas com base em requisitos funcionais e de desempenho, vedado direcionamento restritivo.

Portanto, a análise da solução da NETSAFE deve verificar se a solução ofertada **cumpre a função exigida no TR**, e não se utiliza exatamente a nomenclatura empregada no edital ou a arquitetura imaginada pela área técnica.

Além disso, o edital prevê que suas normas devem ser interpretadas em favor da ampliação da disputa, desde que preservados interesse público, isonomia, finalidade e segurança da contratação. Também dispõe que exigências formais não essenciais não afastarão licitante quando o ato puder ser aproveitado.

### 4.2. Correlação técnica dos itens impugnados

A NETSAFE ofertou solução baseada em tecnologias Skyhigh CASB e Trellix DLP, conforme documentação técnica indicada na planilha ponto a pontop.

Os documentos oficiais dessas soluções demonstram aderência funcional aos itens apontados como não atendidos, ao menos em grau suficiente para exigir reanálise técnica motivada.

**Item 1.1 – formato software ou hardware.**

A solução é entregue em formato de Software, tanto o DLP Endpoint quanto o CASB.

A console de gerenciamento do CASB é entregue em formato SaaS devido a estrutura da solução e o gerenciamento do DLP Endpoint é entregue em formato SaaS e hardware, ficando livre a escolha da forma de utilização.

Para o CASB:

https://success.skyhighsecurity.com/Skyhigh_CASB/01_Start_Here_with_Skyhigh_CASB/Skyhigh_CASB_Overview/About_Skyhigh_CASB

O requisito é atendido, pois a documentação do fabricante caracteriza expressamente a solução ofertada como software fornecido em nuvem (cloud-based service), operando em

arquitetura multi-tenant e compatível com os modelos SaaS (Software as a Service), PaaS (Platform as a Service) e IaaS (Infrastructure as a Service).

A comprovação consta dos seguintes trechos da documentação:

"Skyhigh CASB is the leading Cloud Access Security Broker (CASB). This cloud-based, multi-tenant service enables companies to embrace cloud services..."

O trecho identifica expressamente a solução como um serviço baseado em nuvem (cloud-based service) e de arquitetura multi-tenant, características inerentes a soluções de software ofertadas como serviço.

Adicionalmente, a documentação dispõe que:

"The three cloud service models that Skyhigh CASB considers are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)."

E ainda:

"Skyhigh Security Cloud for SaaS enables secure adoption of cloud services..."

"Customers deploying Skyhigh Security Cloud for SaaS can immediately benefit from centralized activity monitoring."

Por fim, o fabricante declara expressamente que:

"Skyhigh Security Cloud is designed to secure all three models."

Dessa forma, a documentação demonstra de forma inequívoca que a solução ofertada possui formato de software em nuvem, sendo disponibilizada como serviço e operando nos modelos SaaS, PaaS e IaaS, atendendo integralmente ao requisito do item 1.1.

A eventual conclusão de não atendimento ao requisito não encontra respaldo no próprio conteúdo da documentação técnica apresentada, a qual identifica repetidamente a solução como serviço em nuvem, multi-tenant e compatível com os modelos de software e infraestrutura em nuvem amplamente reconhecidos pelo mercado.

Para o DLP:

https://docs.trellix.com/pt-PT/bundle/data-loss-prevention-saas-product-guide/page/UUID-cfaa53ea-c715-d29b-f938-b91ca0460ba2.html

O requisito é atendido, pois a documentação do fabricante identifica expressamente a solução como software fornecido no modelo SaaS (Software as a Service), conforme os trechos:

**“Trellix Data Loss Prevention - SaaS is a suite of products”;**

**“ePO – SaaS is a multi-tenant, globally scaled management service that runs in the cloud”;**

**“Trellix DLP - SaaS is a data protection product”.**

Tais declarações demonstram de forma inequívoca que a solução ofertada possui formato de software, operando em arquitetura SaaS e gerenciamento em nuvem, atendendo ao requisito relativo ao formato da solução.

Desta forma, a solução atende o item 1.1. e o recurso deve ser provido para a classificação da Netsafe.

Assim, a decisão que desclassificou a Netsafe merece reforma, pois as soluções cumprem o item 1.1 do Edital.

### 1.9.2 A solução deve permitir auditoria de mensagens instantâneas (Teams, Slack, WhatsApp, etc.).

A solução, ou se integra com serviços de mensagens instantâneas, como Teams e Slackware, via Skyhigh CASB, quando for solução sancionada, permitindo auditoria mensagens.

https://success.skyhighsecurity.com/Skyhigh_CASB/06_Skyhigh_CASB_Sanctioned_Applications/01_Skyhigh_CASB_Native_Sanctioned_Apps/Skyhigh_CASB_for_Microsoft_Teams/About_Skyhigh_CASB_for_Microsoft_Teams

O requisito do item 1.9.2 é atendido, pois a documentação técnica demonstra expressamente que a solução permite a auditoria, monitoramento, inspeção, análise histórica e aplicação de políticas DLP sobre mensagens instantâneas do

Microsoft Teams, abrangendo tanto canais quanto conversas privadas e em grupo.

A comprovação consta dos seguintes trechos:

"Skyhigh CASB for Microsoft Teams allows Security Operations Center (SOC) Admins to monitor user activity in Teams, enforce DLP policies (...) and review threats detected..."

O trecho demonstra que a solução monitora atividades dos usuários no Microsoft Teams, permitindo auditoria das interações realizadas na plataforma.

Adicionalmente, a documentação estabelece:

"Monitor messages posted in Teams channels and 1:1/1:many chat conversations (including messages to and from guest users) to make sure confidential data is not shared with unauthorized external parties."

Tal funcionalidade comprova expressamente a capacidade de monitorar mensagens em canais, conversas individuais e conversas em grupo, inclusive envolvendo usuários externos.

Também consta:

"Perform a historical data scan to identify sensitive messages present in 1:1 and 1:many chat conversations (On-Demand Scan)."

Esse recurso demonstra capacidade de auditoria retrospectiva sobre mensagens já existentes, permitindo análise histórica das comunicações.

A documentação reforça ainda:

"Content-aware collaboration is supported for messages posted in Teams channels and also for messages posted in 1:1 or 1:many user chats in the Chat app."

E:

"If a chat conversation/thread is initiated by an internal user with any external user, then this conversation can be monitored by Skyhigh CASB for DLP."

Tais trechos evidenciam a inspeção do conteúdo das mensagens, inclusive em chats individuais e em grupo.

Por fim, a funcionalidade de proxy reverso contempla diretamente as comunicações instantâneas:

"Skyhigh CASB Reverse Proxy integration for Microsoft Teams supports the following features: 1:1 or 1: many (group) chats."

Dessa forma, a documentação comprova de maneira inequívoca que a solução permite auditoria de mensagens instantâneas no Microsoft Teams, mediante monitoramento de mensagens, inspeção de conteúdo, aplicação de políticas DLP, análise de conversas individuais e em grupo e realização de auditoria histórica por meio de On-Demand Scan.

A eventual conclusão de não atendimento ao item 1.9.2 não encontra suporte na documentação técnica apresentada, a qual descreve expressamente múltiplas funcionalidades de auditoria e monitoramento de mensagens instantâneas no Microsoft Teams.

https://success.skyhighsecurity.com/Skyhigh_CASB/06_Skyhigh_CASB_Sanctioned_Applications/01_Skyhigh_CASB_Native_Sanctioned_Apps/Skyhigh_CASB_for_Slack/About_Skyhigh_CASB_for_Slack

O requisito do item 1.9.2 é atendido, pois a documentação técnica demonstra expressamente que a solução permite a **auditoria, monitoramento, inspeção de conteúdo, aplicação de políticas DLP e controle em tempo real sobre mensagens instantâneas do Slack**, incluindo mensagens diretas (DMs), conversas em grupo, canais, Huddles e Canvas.

A comprovação consta dos seguintes trechos:

**"Skyhigh CASB for Slack provides compliance and security governance through Data Loss Prevention (DLP) policies for data stored in Slack."**

O fabricante informa expressamente que a solução fornece governança e conformidade sobre os dados armazenados no Slack mediante aplicação de políticas DLP.

Adicionalmente, a documentação estabelece:

**"Skyhigh CASB for Slack supports real-time scanning of active files within a Slack implementation through the Slack API, and nearly all aspects of Threat Protection and activity monitoring."**

Tal funcionalidade comprova capacidade de monitoramento contínuo e auditoria das atividades realizadas na plataforma.

Ainda, a documentação descreve:

**"Best for those who want to have an inline real-time control over the data (Files/Chat messages/Snippets) being transferred to Slack."**

Esse trecho demonstra expressamente controle e inspeção em tempo real sobre **mensagens de chat (Chat Messages)** transmitidas no Slack.

A documentação também comprova auditoria sobre comunicações realizadas em Huddles:

**"Skyhigh CASB for Slack provides a way for organizations to extend existing data loss prevention (DLP) policies to Slack huddles."**

E:

**"Identifies the sensitive content of the messages or files shared by any user in the huddle and takes Quarantine/Delete as remediation actions."**

Tal funcionalidade evidencia a inspeção do conteúdo das mensagens trocadas durante reuniões instantâneas (Huddles), com aplicação de políticas de segurança e ações corretivas.

Além disso, a solução suporta auditoria em Slack Canvas, incluindo mensagens e comunicações colaborativas:

**"Messages - Yes - Messages sent in Canvas comments."**

Com as seguintes ações de resposta:

**"Create an Incident"**
**"Delete"**
**"Send Bot Notification"**

A documentação também demonstra suporte para comunicações realizadas por mensagens diretas:

**"Canvas shared via Direct Messages (DMs) - Yes"**

E:

**"Canvas shared via Multi-Party DMs (MPDM) - Yes"**

Dessa forma, a documentação comprova de forma inequívoca que a solução permite auditoria de mensagens instantâneas no Slack mediante monitoramento de atividades, inspeção de conteúdo, aplicação de políticas DLP, análise de mensagens em chats, canais, mensagens diretas (DMs), conversas em grupo (MPDM), Huddles e Canvas, com geração de incidentes e aplicação de ações corretivas.

A eventual conclusão de não atendimento ao item 1.9.2 não encontra suporte na documentação técnica apresentada, a qual descreve expressamente funcionalidades de monitoramento, auditoria, inspeção e governança sobre mensagens instantâneas do Slack, uma das plataformas nominalmente exemplificadas pelo próprio requisito editalício.

https://success.skyhighsecurity.com/Skyhigh_Data_Loss_Prevention/03_Skyhigh_DLP_for_GenAI/About_DLP_for_Gen_AI_Application

O requisito do item 1.9.2 é atendido, pois a documentação técnica demonstra expressamente que a solução realiza inspeção e proteção em tempo real sobre comunicações e transferências de dados em aplicações de mensagens instantâneas, incluindo **WhatsApp**.

A comprovação consta dos seguintes trechos:

**"The Inline DLP Proxy mode provides immediate, real-time data protection for sensitive data across a wide range of GenAI applications..."**

O fabricante informa que a solução opera em modo Inline DLP Proxy, realizando proteção e inspeção em tempo real dos dados trafegados.

Mais especificamente, a documentação dispõe:

**"Additionally, all uploads, including those on web socket-based applications such as Microsoft 365 Copilot and end-to-end encryption-based applications such as WhatsApp and Facebook Messenger, are instantly scanned to prevent the leakage of sensitive information."**

Esse trecho comprova expressamente que a solução realiza **varredura instantânea (instantly scanned)** sobre conteúdos trafegados por aplicações de comunicação protegidas por criptografia ponta a ponta, incluindo **WhatsApp** e **Facebook Messenger**, com o objetivo de prevenir vazamento de informações sensíveis.

Adicionalmente, o fabricante declara:

**"This capability is a core component of Skyhigh Web DLP offerings, enabling enterprises to establish and enforce DLP policies tailored to their specific data governance requirements."**

Tal funcionalidade demonstra a aplicação de políticas de DLP sobre os dados trafegados nas aplicações monitoradas.

Dessa forma, a documentação comprova que a solução possui capacidade de inspeção, monitoramento e aplicação de políticas DLP em tempo real sobre conteúdos transmitidos por aplicações de mensagens instantâneas, incluindo expressamente o **WhatsApp**, uma das plataformas exemplificadas no item 1.9.2 do edital.

A eventual conclusão de não atendimento ao requisito não encontra respaldo na documentação técnica apresentada, que identifica nominalmente o WhatsApp como aplicação suportada para inspeção instantânea de conteúdo e aplicação de controles DLP em tempo real.

Utilizando Trellix DLP Endpoint, é possível aplicar regras de proteção a sites web, como Whatsapp WEB, Slack, entre outros, direto no navegador, bem como aplicar a proteção em Aplicativos, como o aplicativo do Whatsapp instalado na máquina e assim aplicar os controles de proteção de dados.

https://docs.trellix.com/bundle/data-loss-prevention-saas-product-guide/page/UUID-74695d4c-aa20-5b49-f412-06ef04921113.html

O requisito do item 1.9.2 é atendido, pois a documentação técnica demonstra que a solução permite o **monitoramento, inspeção e controle de conteúdo publicado em aplicações web**, incluindo mensagens, formulários web e serviços de webmail, com geração de incidentes e aplicação de regras de proteção de dados.

A comprovação consta dos seguintes trechos:

**"Web protection rules monitor or block data from being posted to websites, including web-based email sites."**

O fabricante informa expressamente que a solução monitora ou bloqueia dados enviados para websites, incluindo serviços de correio eletrônico baseados na web, evidenciando capacidade de fiscalização das comunicações realizadas por esses canais.

Adicionalmente, a documentação dispõe:

**"Trellix DLP Network Monitor - SaaS also supports web protection rules."**

Tal funcionalidade demonstra suporte à monitoração das informações trafegadas em aplicações web.

A documentação também estabelece:

**"Web protection rules aggregate repeat incidents."**

E:

**"it produces a single incident in the DLP Protection Workspace."**

Esses trechos comprovam a capacidade de auditoria e registro de eventos decorrentes das tentativas de transmissão de informações por meio dos canais monitorados.

Por fim, o fabricante descreve especificamente a monitoração de publicações textuais:

**"For text posts, the web protection rule evaluates the Web Address (URL) condition with the HTTP request URL."**

E conclui:

**"text posts can only be monitored."**

Tal funcionalidade demonstra expressamente a capacidade de monitoramento de conteúdos textuais publicados em aplicações web.

Dessa forma, a documentação comprova que a solução possui mecanismos de monitoramento, inspeção e auditoria sobre conteúdos publicados em aplicações web, incluindo mensagens e comunicações realizadas por websites e serviços webmail, com geração de incidentes e aplicação de políticas de proteção de dados.

https://docs.trellix.com/bundle/data-loss-prevention-saas-product-guide/page/UUID-4b6eaa67-e502-b040-5a1f-4c5d5dbc33d4.html

A documentação estabelece:

**"Application file access protection rules monitor files based on the application or applications that created them."**

Esse trecho demonstra que a solução é capaz de monitorar arquivos com base na aplicação utilizada para sua criação ou manipulação.

Adicionalmente, o fabricante informa:

**"To limit the rule to specific applications, select an application or URL definition."**

Tal funcionalidade evidencia que as políticas de proteção podem ser associadas a aplicações específicas.

Por fim, a documentação dispõe:

**"Use classification definitions to limit the rule to specific content fingerprinting or content classification criteria."**

O trecho demonstra que a solução permite aplicar controles baseados em classificação e identificação de conteúdo.

Desta forma, o requisito do item 1.9.2 foi totalmente cumprido pela documentação da Netsafe e a decisão de desclassificação deve ser reformada.

1.9.3 A solução deve permitir integração com ferramentas de Business Intelligence como PowerBI e Tableau.

É possível se conectar via API aos serviços Skyhigh CASB e Trellix DLP para efetuar a coleta das informações e incidentes de DLP gerado por estes sistemas, para então disponibilizar os dados baixados para o PowerBI fazer uso.

https://success.skyhighsecurity.com/Skyhigh_SSE_APIs/Data_Retrieval_API/About_the_Data_Retrieval_API

O requisito do item 1.9.3 é atendido, pois a documentação técnica demonstra que a solução disponibiliza **API para extração automatizada de dados e relatórios**, permitindo sua importação para sistemas de terceiros destinados à análise, correlação e visualização de informações, incluindo plataformas de Business Intelligence.

A comprovação consta dos seguintes trechos:

**"For users looking to automatically access reports from Skyhigh Security Service Edge, the Data Retrieval API can generate several reports for import into your third-party system for additional analysis and reporting."**

O fabricante informa expressamente que a solução disponibiliza uma **Data Retrieval API**, capaz de gerar relatórios para importação em sistemas de terceiros, destinados à realização de análises e relatórios adicionais.

Adicionalmente, a documentação dispõe:

**"SSE reports can include events generated within SSE, such as anomalies and audits, along with API-based events imported from cloud service providers."**

Tal funcionalidade demonstra que a API disponibiliza informações estruturadas para consumo externo, abrangendo eventos, auditorias e dados operacionais da plataforma.

A documentação também estabelece:

**"Other reports data from across your entire tenant, including user directories, DRM and DLP policies, along with MDM-related data that you may want to import into SIEMs."**

E:

**"Security, firewall, perimeter security devices, and UEBA solution reports can be accessed as well."**

Esses trechos demonstram que a solução permite a exportação e integração de amplo conjunto de dados corporativos para ferramentas externas de análise.

Dessa forma, a documentação comprova que a solução disponibiliza mecanismo formal de integração por API para extração de relatórios e dados estruturados, permitindo sua importação em plataformas de terceiros para fins de análise, consolidação, correlação e construção de dashboards.

A eventual conclusão de não atendimento ao item 1.9.3 não encontra respaldo na documentação apresentada, uma vez que o fabricante prevê expressamente a utilização da **Data Retrieval API** para importação de dados e relatórios por sistemas externos de análise.

https://developer.manage.trellix.com/public/mvision/apis/incident

O requisito do item 1.9.3 é atendido, pois a documentação técnica demonstra a existência de **API documentada para recuperação estruturada de dados e incidentes**, permitindo integração com sistemas externos para análise, correlação, consolidação e visualização de informações, incluindo plataformas de Business Intelligence.

A comprovação consta dos seguintes trechos:

**"Incident APIs."**

A documentação confirma expressamente a disponibilização de APIs para acesso aos dados da solução.

Adicionalmente, o fabricante estabelece:

**"The following API allows for the retrieval of these incidents in bulk."**

Tal funcionalidade demonstra que a solução permite a extração automatizada de incidentes em massa, característica essencial para integração com ferramentas externas de análise e BI.

A documentação também dispõe:

**"with the ability to constrain the results to a specific time period."**

Esse recurso comprova a possibilidade de consultas parametrizadas e filtragem temporal dos dados extraídos, funcionalidade tipicamente utilizada por plataformas de Business Intelligence para geração de dashboards, relatórios e análises históricas.

Dessa forma, a documentação comprova que a solução disponibiliza mecanismos de integração baseados em API para acesso estruturado aos dados de incidentes, permitindo sua coleta, processamento e consumo por sistemas de terceiros.

A eventual conclusão de não atendimento ao item 1.9.3 não encontra respaldo na documentação apresentada, uma vez que o fabricante documenta expressamente APIs destinadas à recuperação automatizada de informações operacionais da plataforma.

Utilizando a feature Custom Apps, também é possível cadastrar aplicações customizadas no Skyhigh CASB, definir a categoria de Business Intelligence, para mapear as ações e chamadas destas aplicações e configurar políticas de proteção de dados como se fosse uma aplicação sancionada.

https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Custom_Apps/About_Custom_Applications/About_Custom_Apps

O requisito do item 1.9.3 é atendido, pois a documentação técnica demonstra que a solução permite integração com aplicações corporativas personalizadas, possibilitando a aplicação de políticas DLP, coleta de atividades, monitoramento de comportamento e processamento de dados provenientes de sistemas desenvolvidos internamente ou por terceiros.

A comprovação consta dos seguintes trechos:

**"With Custom Apps, you can deploy DLP policies across all custom cloud applications, without writing new code."**

O fabricante informa expressamente que a solução permite integração com aplicações customizadas em nuvem, dispensando desenvolvimento adicional para aplicação das políticas de proteção.

Adicionalmente, a documentação estabelece:

**"This is accomplished by mapping activities involving content uploads or updates using the Custom Apps framework and deploying it to a production environment."**

Tal funcionalidade demonstra que a plataforma é capaz de mapear e consumir eventos e atividades provenientes de aplicações externas.

A documentação também dispõe:

**"Mapped activities are also fed into the Skyhigh CASB Threat Protection engine."**

Esse trecho comprova que os dados oriundos das aplicações integradas são processados pela plataforma, permitindo correlação e análise centralizada.

Além disso, o fabricante informa:

**"Because of the way activities are mapped, tell Skyhigh CASB what to look for, then Skyhigh CASB builds user behavior analytics to identify issues."**

Tal funcionalidade evidencia a capacidade de gerar análises comportamentais a partir dos dados coletados das aplicações integradas.

Por fim, a documentação estabelece:

**"Any IDM solutions currently in use for external users can be integrated with the Custom Apps workflow."**

Esse trecho demonstra expressamente a existência de mecanismos de integração com soluções externas.

Dessa forma, a documentação comprova que a solução possui arquitetura aberta de integração com aplicações corporativas personalizadas, permitindo ingestão de eventos, monitoramento de atividades, aplicação de políticas DLP e geração de análises sobre os dados coletados.

Desta forma, o requisito do item 1.9.3 foi totalmente cumprido pela documentação da Netsafe e a decisão de desclassificação deve ser reformada.

### 1.11.2 A solução deve oferecer Shadow Copy para análise de arquivos envolvidos em incidentes de segurança.

Para efetuar análise de arquivos envolvidos em incidentes de segurança, no caso de Data Loss Prevention (Proteção de Dados), o shadow copy refere-se ao chamado “Evidências”.

Tanto o Trellix DLP Endpoint quanto o Skyhigh CASB oferecem a funcionalidade de Evidêncais, sendo necessário um storage do cliente (como S3 bucket da AWS), para que a custódia sobre o dado da evidência seja exclusivamente do cliente e não do fabricante.

https://docs.trellix.com/pt-PT/bundle/data-loss-prevention-saas-product-guide/page/UUID-a3a33021-dd03-1fe2-bb0b-2316ab49b4dd.html

O requisito do item 1.11.2 é atendido, pois a solução mantém e disponibiliza cópias dos arquivos associados aos incidentes de segurança, permitindo sua preservação, recuperação e análise posterior pelos administradores, funcionalidade que corresponde materialmente ao conceito de **Shadow Copy** exigido pelo edital.

A comprovação consta dos seguintes trechos:

**"Irrespective of the rule violation, you can access all evidences."**

O fabricante informa que todas as evidências relacionadas ao incidente permanecem acessíveis, independentemente do resultado da violação analisada.

Adicionalmente:

**"Evidences of unmatched email attachments (...) are also hyperlinked and made downloadable."**

Tal funcionalidade demonstra que os anexos envolvidos no incidente são preservados pela solução e permanecem disponíveis para recuperação posterior.

Ainda:

**"click the evidence files of unmatched email attachments to download the evidence."**

Esse trecho comprova que os arquivos coletados como evidência permanecem armazenados e podem ser recuperados para análise posterior.

Por fim:

**"Select Store all evidence to evidence share (used by DLP Network Prevent and DLP Network Monitor)."**

O fabricante prevê expressamente o armazenamento de todas as evidências em repositório dedicado ("evidence share"), garantindo a retenção dos arquivos relacionados ao incidente.

Dessa forma, a solução não apenas registra metadados ou alertas, mas efetivamente preserva e armazena os arquivos envolvidos nos eventos detectados, disponibilizando-os para consulta e download posterior pelos administradores.

O conceito de **Shadow Copy**, no contexto de soluções DLP e investigação de incidentes, consiste justamente na manutenção de uma cópia do conteúdo ou arquivo envolvido na ocorrência de segurança para posterior análise, auditoria, investigação ou produção de evidências. É exatamente essa funcionalidade que a documentação descreve ao prever o armazenamento integral das evidências ("Store all evidence"), bem como a disponibilização dos arquivos envolvidos para recuperação e análise posterior.

Assim, ainda que a documentação utilize a nomenclatura técnica **Evidence Files**, **Evidence Share** ou **Stored Evidence**, e não a expressão literal "Shadow Copy", a funcionalidade implementada é materialmente equivalente ao requisito

editalício, uma vez que permite a retenção, preservação e posterior análise dos arquivos relacionados ao incidente de segurança.

https://success.skyhighsecurity.com/Skyhigh_Data_Loss_Prevention/Sanctioned_DLP_Policies_and_Rules/Sanctioned_DLP_Policies/Save_CASB_Evidence

O requisito do item 1.11.2 é atendido de forma expressa e inequívoca, pois a documentação técnica do fabricante descreve funcionalidade que corresponde exatamente ao conceito de **Shadow Copy**, mediante captura automática, preservação, armazenamento seguro, retenção e disponibilização de cópia dos arquivos envolvidos em incidentes de segurança para posterior análise forense.

A comprovação consta dos seguintes trechos:

**"When a CASB policy is triggered, the system automatically captures, encrypts, and securely stores the relevant files."**

O fabricante informa expressamente que, quando ocorre uma violação de política, a solução captura automaticamente os arquivos relacionados ao incidente e os armazena de forma segura.

Adicionalmente:

**"This ensures that critical evidence is preserved instantly and remains protected from unauthorized access or tampering from the moment a violation occurs."**

Tal funcionalidade demonstra que os arquivos são preservados imediatamente após a ocorrência do incidente, impedindo alterações, exclusões ou adulterações posteriores.

A documentação define expressamente o conceito de evidência:

**"DLP evidence is a copy of the compromised content that violates a CASB policy detected during the policy evaluation."**

Esse trecho é particularmente relevante, pois o fabricante afirma literalmente que a evidência consiste em uma **cópia do**

**conteúdo comprometido** identificado durante a detecção do incidente.

Além disso:

**"This copy of compromised content is linked to the relevant incident and saved in your data storage, enabling further forensic analysis of generated incidents."**

A solução não apenas cria a cópia, mas a vincula ao incidente correspondente e a armazena para análise forense posterior.

O fabricante também informa:

**"A backup of the evidence file is retained and stored in the data storage provider (AWS and Azure)."**

Esse trecho comprova a retenção permanente da cópia do arquivo, mesmo após eventos posteriores relacionados à política.

Ainda:

**"It represents the exact information at the point of detection, providing an unaltered snapshot of the possible data breach."**

Tal funcionalidade demonstra que a solução preserva uma fotografia exata ("snapshot") do conteúdo no exato momento da detecção da ocorrência.

Por fim:

**"Source Files. These files contain the complete, raw, or unmodified data processed by the DLP classification engine."**

E:

**"it serves as an accurate and comprehensive record of the transferred data."**

Esses trechos demonstram que a cópia preservada corresponde ao conteúdo integral, original e não modificado do arquivo envolvido no incidente.

**Conclusão técnica**

A documentação comprova expressamente que a solução:

- Captura automaticamente os arquivos envolvidos no incidente;
- Cria uma cópia do conteúdo comprometido;
- Preserva o conteúdo no momento exato da detecção;
- Mantém uma cópia inalterada ("unaltered snapshot");
- Armazena a evidência de forma persistente;
- Mantém backup da evidência;
- Permite posterior recuperação e análise forense;
- Disponibiliza download individual ou em massa via interface e API.

Trata-se precisamente da funcionalidade conhecida no mercado como **Shadow Copy**, ainda que o fabricante utilize a nomenclatura **DLP Evidence**, **Save Evidence**, **Evidence Files**, **Source Files** ou **Unaltered Snapshot**.

A eventual conclusão de não atendimento ao item 1.11.2 não encontra respaldo na documentação técnica apresentada, uma vez que o próprio fabricante descreve a funcionalidade como a criação e retenção de uma **cópia do conteúdo comprometido**, preservada para investigação posterior, o que corresponde materialmente ao conceito de Shadow Copy exigido pelo edital.

Desta forma, o requisito do item 1.11.12 foi totalmente cumprido pela documentação da Netsafe e a decisão de desclassificação deve ser reformada.

1.12.1 A solução deve monitorar operações em OneDrive e SharePoint Online.

Skyhigh CASB para Sharepoint e para OneDrive efetua proteção em detecção de anomalias, monitoramento de atividades, e proteção de DLP para os arquivos armazenados tanto no OneDrive quanto no Sharepoint. Requer licença Office365 E1 ou superior devido as API da Microsoft disponíveis nestes TIERs.

https://success.skyhighsecurity.com/Skyhigh_CASB/06_Skyhigh_CASB_Sanctioned_Applications/01_Skyhigh_CASB_Native_Sanctioned_Apps/Skyhigh_CASB_for_OneDrive

O requisito do item 1.12.1 é atendido, pois a documentação técnica demonstra expressamente que a solução realiza **monitoramento de atividades e operações executadas no Microsoft OneDrive**, além de aplicar controles de segurança, detecção de anomalias e políticas de prevenção contra vazamento de dados.

A comprovação consta do seguinte trecho:

**"Skyhigh CASB for Microsoft OneDrive helps ensure compliance and security requirements by providing an additional layer of control through Data Loss Prevention (DLP) policies, anomaly detection, and activity monitoring for data stored in OneDrive."**

O fabricante informa expressamente que a solução disponibiliza:

- **Activity Monitoring** (monitoramento de atividades);
- **Anomaly Detection** (detecção de anomalias);
- **DLP Policies** (políticas de prevenção contra perda de dados);

aplicadas aos dados armazenados no Microsoft OneDrive.

Adicionalmente, a documentação estabelece:

**"It also provides a way for organizations to leverage their existing enterprise data loss prevention (DLP) policies and extend them to the cloud."**

Tal funcionalidade demonstra que as atividades realizadas no ambiente OneDrive são submetidas às políticas corporativas de monitoramento e proteção.

Dessa forma, a documentação comprova de maneira inequívoca que a solução monitora operações realizadas no Microsoft OneDrive, mediante monitoramento de atividades, detecção de

comportamentos anômalos e aplicação de políticas de segurança e conformidade.

https://success.skyhighsecurity.com/Skyhigh_CASB/06_Skyhigh_CASB_Sanctioned_Applications/01_Skyhigh_CASB_Native_Sanctioned_Apps/Skyhigh_CASB_for_OneDrive/About_Skyhigh_CASB_for_OneDrive

O requisito do item 1.12.1 é atendido, pois a documentação técnica demonstra expressamente que a solução monitora continuamente operações realizadas tanto no **Microsoft OneDrive** quanto no **Microsoft SharePoint Online**, utilizando APIs nativas da Microsoft para acompanhar alterações de conteúdo, atividades de usuários e eventos ocorridos nesses ambientes.

A comprovação consta dos seguintes trechos:

**"Skyhigh CASB continuously monitors OneDrive for content changes using APIs from OneDrive (Office 365)."**

O fabricante informa expressamente que a solução realiza monitoramento contínuo das alterações de conteúdo ocorridas no OneDrive.

Adicionalmente:

**"As employees add/modify new files in OneDrive, Skyhigh CASB scans the files according to DLP policies."**

Esse trecho demonstra que a solução monitora operações de inclusão e modificação de arquivos realizadas pelos usuários no OneDrive.

A documentação também estabelece:

**"When Microsoft OneDrive is enabled using the API integration method, the Azure AD activities are listed on the Activity Monitoring dashboard."**

Tal funcionalidade comprova a existência de painel de monitoramento de atividades relacionadas ao ambiente integrado.

No que se refere ao SharePoint Online, a documentação dispõe expressamente:

**"Integrate Skyhigh CASB with SharePoint Online and OneDrive using Microsoft Graph Delta API."**

Além disso:

**"Enable Delta APIs for SharePoint Online and OneDrive."**

E ainda:

**"Migrate existing SharePoint Online and OneDrive instances from the traditional OneDrive Add-in app model to the advanced Delta API model."**

Tais trechos demonstram que a solução integra-se simultaneamente ao SharePoint Online e ao OneDrive por meio das APIs Microsoft Graph Delta, mecanismo utilizado para acompanhamento de alterações, sincronização de eventos e monitoramento contínuo das atividades realizadas nesses ambientes.

Por fim, a documentação prevê:

**"Integrate Skyhigh CASB with new SharePoint Online and OneDrive instances using Delta APIs."**

Dessa forma, a documentação comprova que a solução monitora operações realizadas tanto no Microsoft OneDrive quanto no Microsoft SharePoint Online, por meio de integração nativa com as APIs Microsoft Graph Delta, monitoramento contínuo de alterações de conteúdo, atividades de usuários e aplicação de políticas DLP.

A eventual conclusão de não atendimento ao item 1.12.1 não encontra respaldo na documentação técnica apresentada, uma vez que o fabricante menciona expressamente a integração e monitoramento de ambos os ambientes requeridos pelo edital.

https://success.skyhighsecurity.com/Skyhigh_CASB/06_Skyhigh_CASB_Sanctioned_Applications/01_Skyhigh_CASB_Native_Sanctioned_Apps/Skyhigh_CASB_for_SharePoint/About_Skyhigh_CASB_for_SharePoint

O requisito do item 1.12.1 é atendido de forma expressa, pois a documentação técnica do fabricante demonstra que a solução monitora continuamente operações realizadas tanto no **Microsoft SharePoint Online** quanto no **Microsoft OneDrive**, incluindo criação, alteração, compartilhamento e colaboração sobre arquivos armazenados nesses ambientes.

A comprovação consta dos seguintes trechos:

**"Skyhigh CASB for SharePoint continuously monitors SharePoint accounts for any file activity."**

O fabricante informa expressamente que a solução realiza monitoramento contínuo de qualquer atividade de arquivos em contas SharePoint.

Adicionalmente:

**"Skyhigh CASB continuously monitors SharePoint for content changes using APIs from SharePoint (Microsoft 365)."**

Tal funcionalidade comprova que a solução monitora continuamente alterações de conteúdo realizadas no ambiente SharePoint.

A documentação também estabelece:

**"As users add or modify files in SharePoint, Skyhigh CASB scans the files according to your DLP policies."**

Esse trecho demonstra expressamente o acompanhamento das operações realizadas pelos usuários, incluindo inclusão e modificação de arquivos.

No que se refere à integração conjunta dos ambientes exigidos pelo edital, o fabricante informa:

**"Integrate Skyhigh CASB with SharePoint Online and OneDrive using Microsoft Graph Delta API."**

Além disso:

**"Enable Delta APIs for SharePoint Online and OneDrive."**

E ainda:

**"Integrate Skyhigh CASB with new SharePoint Online and OneDrive instances using Delta APIs."**

Tais trechos comprovam a integração nativa da solução com os ambientes Microsoft SharePoint Online e Microsoft OneDrive por meio das APIs Microsoft Graph Delta, utilizadas para monitoramento contínuo de alterações e eventos ocorridos nos repositórios.

A documentação reforça ainda a capacidade de monitoramento das operações de colaboração:

**"Make sure that collaboration with external users is monitored and controlled for SharePoint sites."**

Esse trecho demonstra expressamente o monitoramento das operações de compartilhamento e colaboração realizadas no SharePoint.

Dessa forma, a documentação comprova de maneira inequívoca que a solução monitora operações realizadas no Microsoft SharePoint Online e no Microsoft OneDrive, incluindo atividades sobre arquivos, alterações de conteúdo, colaboração com usuários externos e eventos capturados por meio das APIs Microsoft Graph Delta.

A eventual conclusão de não atendimento ao item 1.12.1 não encontra respaldo na documentação técnica apresentada, uma vez que o fabricante declara expressamente o monitoramento contínuo de atividades e alterações tanto no SharePoint quanto no OneDrive.

Conclusão: Desta forma, o item 1.12.1 foi totalmente atendido pela solução da Netsafe, devendo a decisão de desclassificação ser reformada.

**1.13.4 A solução deve utilizar métodos estatísticos e machine learning para identificar desvios de comportamento.**

As anomalias dentro do Skyhigh CASB são ações ou comportamentos que excedem um limiar (threshold) dentro do Threat Protection, podendo indicar um comportamento malicioso dos usuários e são calculados com base na pontuação das categorias de anomalias detectadas pela ferramenta para cada usuário.

Há também as atividades dos usuários nos serviços sancionados que permite monitorar a utilização do serviço sancionado pelos usuários.

https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Incidents/Anomalies/About_Anomalies/About_Anomalies

O requisito do item 1.13.4 é atendido, pois a documentação técnica demonstra expressamente que a solução utiliza mecanismos de **detecção de anomalias**, **análise comportamental de usuários**, **atribuição de pontuação de risco**, **correlação de eventos** e **identificação de desvios em padrões de comportamento**, funcionalidades inerentemente baseadas em métodos estatísticos e modelos de análise comportamental compatíveis com técnicas de Machine Learning e User Behavior Analytics (UEBA).

A comprovação consta dos seguintes trechos:

**"The default anomalies table displays information about specific clusters of anomalies that strongly suggest your cloud services may have been compromised."**

O fabricante informa que a solução identifica agrupamentos ("clusters") de anomalias capazes de indicar comprometimento de serviços em nuvem, evidenciando mecanismos automatizados de detecção de desvios comportamentais.

Adicionalmente:

**"Adjust Anomaly Thresholds. Administrators may want to manually adjust anomaly detection thresholds to control the generation of new anomalies."**

Esse trecho demonstra a utilização de limiares estatísticos para detecção de comportamentos anômalos, característica típica de mecanismos de análise comportamental.

A documentação também estabelece:

**"Generate and download a User Risk Report to identify high, medium, and low-risk users."**

E:

**"Historical User Risk Score is a risk score assigned to the user whenever an anomaly is created, and it is rated on a scale of 1-9."**

Tais funcionalidades demonstram que a solução calcula e atribui pontuações de risco aos usuários com base em comportamentos observados.

O fabricante descreve ainda:

**"This score is measured based on various factors such as the severity of the violation, the user’s security posture, and metadata about the user's overall compliance history."**

Esse trecho evidencia a utilização de múltiplas variáveis comportamentais para classificação de risco e identificação de desvios.

Além disso:

**"The Historical User Risk Score allows you to track and manage users’ typical usage patterns related to data security."**

A documentação afirma expressamente que a solução acompanha e analisa padrões típicos de utilização dos usuários, permitindo identificar comportamentos que fogem ao padrão esperado.

Por fim, o fabricante informa:

**"The User UID consolidates all anomalies under one identifier across Sanctioned, Shadow/Web, and Private applications, enabling SOC analysts to view a complete list of anomalies. This consolidation allows security teams to**

**correlate events across different systems, reduce duplication in investigations, and respond to suspicious activity with greater speed and precision."**

Tal funcionalidade demonstra correlação automatizada de eventos e análise comportamental consolidada entre múltiplos sistemas.

**Conclusão técnica**

A documentação comprova que a solução:

- Detecta anomalias;
- Identifica clusters de comportamentos suspeitos;
- Utiliza limiares de detecção configuráveis;
- Calcula pontuações de risco dos usuários;
- Analisa padrões históricos de comportamento;
- Correlaciona eventos entre múltiplos sistemas;
- Classifica usuários em níveis de risco;
- Permite identificar desvios em relação ao comportamento habitual.

Essas funcionalidades caracterizam precisamente mecanismos de **User and Entity Behavior Analytics (UEBA)** e análise comportamental baseada em métodos estatísticos.

A eventual conclusão de não atendimento ao item 1.13.4 não encontra respaldo na documentação apresentada, uma vez que a solução realiza identificação automatizada de anomalias, análise de padrões de comportamento, cálculo de risco e correlação de eventos para detecção de atividades suspeitas.

https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Incidents/Anomalies/About_Anomalies/Anomaly_Cloud_Card

O requisito do item 1.13.4 é atendido, pois a documentação técnica demonstra expressamente que a solução utiliza

**análise de anomalias baseada em limiares estatísticos (thresholds)**, avaliação de desvios em relação ao comportamento esperado dos usuários, análise geográfica, correlação de atividades e cálculo de risco para identificar comportamentos anômalos e potenciais ameaças.

A comprovação consta dos seguintes trechos:

**"The Anomaly Cloud Card provides specific information on a selected anomaly, including information on how the anomaly was determined."**

O fabricante informa expressamente que a solução registra e apresenta os critérios utilizados para determinar a ocorrência da anomalia.

Adicionalmente:

**"Severity. The value (on a Low/Medium/High scale) of by how much the anomaly exceeds the threshold for the action."**

Esse trecho demonstra que a solução utiliza limiares de comportamento ("thresholds") para identificar desvios, classificando sua gravidade de acordo com a magnitude da ultrapassagem desses parâmetros.

A documentação também estabelece:

**"Threshold-Based Anomaly"**

e

**"Anomaly thresholds are the foundation of the Skyhigh CASB Threat Protection platform."**

Tal declaração é particularmente relevante, pois o próprio fabricante afirma que os limiares de anomalia constituem a base da plataforma de detecção de ameaças.

Além disso:

**"It displays a chart that shows the threshold and by how much the activity exceeded the threshold."**

E:

**"Any activity that exceeds the thresholds is registered as an anomaly."**

Esses trechos demonstram claramente a utilização de métodos estatísticos para identificação de desvios de comportamento em relação a padrões previamente estabelecidos.

O fabricante também informa:

**"This can be used to estimate the severity of an anomaly; an anomaly that significantly exceeds the threshold may indicate a larger security risk than an anomaly that just slightly crosses the threshold."**

Tal funcionalidade evidencia análise quantitativa da intensidade do desvio comportamental observado.

Adicionalmente, a solução realiza análise comportamental baseada em atividade histórica:

**"No. of Activities. How many times during this period the activity occurred."**

E:

**"Knowing how many activities contributed to the anomaly may help determine if this was a continued pattern of attack or a single event."**

Esses mecanismos demonstram análise de padrões de comportamento ao longo do tempo.

A documentação ainda prevê:

**"Geography-Based Anomaly"**

E:

**"It can be used to monitor the activity of the users within your organization and detect risk activity trends for the entire organization over time."**

Tal funcionalidade demonstra monitoramento contínuo de padrões de comportamento e identificação de tendências anômalas.

Por fim, o fabricante estabelece:

**"This allows you to drill down to specific activities that led to an anomaly."**

Comprovando a correlação entre atividades observadas e o comportamento anômalo detectado.

**Conclusão técnica**

A documentação demonstra que a solução:

- Utiliza limiares estatísticos (thresholds);
- Mede desvios em relação aos padrões esperados;
- Detecta comportamentos anômalos automaticamente;
- Analisa frequência e recorrência de atividades;
- Identifica tendências de comportamento ao longo do tempo;
- Realiza análise geográfica de comportamento;
- Calcula níveis de risco com base nos desvios observados;
- Correlaciona atividades para identificar comportamentos suspeitos.

Dessa forma, a solução implementa mecanismos de detecção comportamental fundamentados em métodos estatísticos e análise de padrões de uso, atendendo ao requisito de identificação de desvios de comportamento.

https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Incidents/Anomalies/About_Anomalies/User_Details_Page_on_Anomalies

O requisito do item 1.13.4 é atendido, pois a documentação técnica demonstra que a solução realiza **análise comportamental de usuários**, **atribuição dinâmica de pontuação de risco**, **monitoramento de tendências**, **avaliação de múltiplos atributos de comportamento** e **correlação estatística de eventos**, com o objetivo de identificar desvios de comportamento e potenciais ameaças aos ambientes corporativos.

A comprovação consta dos seguintes trechos:

**"On the User Details Page, you can monitor the trend and change in the User Risk Score."**

O fabricante informa expressamente que a solução acompanha a evolução temporal da pontuação de risco dos usuários, permitindo identificar alterações de comportamento ao longo do tempo.

Adicionalmente:

**"allows admins to discover at a glance any possible threats posed by the user to an organization's cloud services and data."**

Esse trecho demonstra que a análise comportamental é utilizada para identificar potenciais ameaças associadas ao comportamento dos usuários.

A documentação também estabelece:

**"The default Risk Score provided by Skyhigh CASB is based on sanctioned user activities and incidents."**

Tal funcionalidade comprova que a solução calcula pontuações de risco com base nas atividades efetivamente realizadas pelos usuários.

Além disso:

**"Change in Risk Score. The change in risk score for a specific duration."**

Esse recurso evidencia a análise estatística da evolução comportamental ao longo de períodos determinados.

O fabricante informa ainda:

**"The Risk tab displays specific details about 44 Risk Attributes associated with the user."**

E:

**"Category Weight."**

**"Attribute Weight."**

**"Weighted Score."**

Esses trechos são particularmente relevantes porque demonstram que a avaliação de risco não é baseada em um único evento isolado, mas em um modelo composto por dezenas de atributos ponderados, cada qual possuindo pesos específicos para cálculo da pontuação final.

A documentação estabelece que a análise considera atributos relacionados a:

**"Download"**
**"Upload"**
**"Login"**
**"Access"**
**"Cloud Usage"**
**"Privilege"**
**"Incident"**
**"Threat"**
**"Collaboration"**

Tais categorias demonstram análise multidimensional do comportamento do usuário.

Por fim, a solução monitora:

**"Top cloud services, top locations, and activity count of the user."**

E:

**"Top Locations. Displays a world map denoting the top locations the user has used."**

Esses mecanismos permitem identificar desvios geográficos, operacionais e comportamentais em relação ao padrão histórico do usuário.

**Conclusão técnica**

A documentação comprova que a solução:

- Analisa comportamento de usuários ao longo do tempo;
- Calcula pontuação de risco baseada em atividades observadas;
- Monitora tendências e alterações de comportamento;
- Utiliza múltiplos atributos comportamentais;

- Aplica pesos estatísticos a categorias e atributos;
- Calcula pontuações ponderadas (Weighted Score);
- Correlaciona eventos, incidentes, acessos, uploads, downloads e atividades;
- Identifica usuários de alto, médio e baixo risco.

Dessa forma, a solução implementa mecanismos de análise comportamental e avaliação estatística de risco destinados à identificação de desvios de comportamento e potenciais ameaças, atendendo ao requisito previsto no item 1.13.4.

https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Incidents/User_Activity/About_Activities

O requisito do item 1.13.4 é atendido, pois a documentação técnica demonstra que a solução realiza monitoramento contínuo de atividades dos usuários, correlação de eventos, análise histórica de comportamento, cálculo de pontuação de risco, categorização de usuários por níveis de risco e identificação de desvios em relação aos padrões normais de utilização dos serviços em nuvem.

A comprovação consta dos seguintes trechos:

**"The Activities page provides details on the user activities captured within your organization. It can be used to monitor the activity of how users within your organization use cloud services over time."**

O fabricante informa expressamente que a solução monitora o comportamento dos usuários ao longo do tempo, permitindo identificar alterações e desvios nos padrões de utilização dos serviços em nuvem.

Adicionalmente:

**"Track User Activities Using User UID."**

E:

**"The User UID consolidates all activities under one identifier across Sanctioned, Shadow/Web, and Private applications."**

Esses trechos demonstram a capacidade de consolidar atividades provenientes de múltiplos sistemas e aplicações, permitindo correlação comportamental centralizada.

A documentação também estabelece:

**"This consolidation allows security teams to correlate events across different systems, reduce duplication in investigations, and respond to suspicious activity with greater speed and precision."**

Tal funcionalidade evidencia mecanismos de correlação e análise de comportamento voltados à identificação de atividades suspeitas.

O fabricante informa ainda:

**"Historical User Risk Score is a risk score assigned to the user whenever the activity is created."**

E:

**"This score is measured based on various factors such as the severity of the violation, the user’s security posture, and metadata about the user's overall compliance history."**

Esses trechos demonstram que a solução utiliza múltiplos fatores comportamentais e históricos para calcular a pontuação de risco dos usuários.

Além disso:

**"The Historical User Risk Score allows you to track and manage users’ typical usage patterns related to data security."**

Essa declaração é particularmente relevante, pois o fabricante afirma expressamente que a solução acompanha os padrões típicos de utilização dos usuários, permitindo identificar desvios em relação ao comportamento esperado.

A documentação também prevê:

**"High (7-9)"**

**"Medium (4-6)"**

**"Low (1-3)"**

Tais classificações demonstram a existência de um modelo quantitativo de avaliação de risco baseado em comportamento observado.

Por fim, a solução incorpora análise geográfica e comportamental:

**"The Activity Geo Location view displays a world map with bubbles based on the number of unique detected users."**

E:

**"You can prioritize your cloud security strategy by the location where specific activities and anomalies occur most often."**

Demonstrando capacidade de identificação de padrões e desvios geográficos de comportamento.

**Conclusão técnica**

A documentação comprova que a solução:

- Monitora atividades dos usuários ao longo do tempo;
- Consolida eventos provenientes de múltiplos sistemas;
- Correlaciona atividades entre aplicações distintas;
- Calcula pontuações de risco;
- Utiliza fatores históricos e comportamentais;
- Identifica padrões típicos de utilização;
- Classifica usuários por níveis de risco;
- Monitora anomalias e atividades suspeitas;
- Analisa comportamento geográfico;
- Permite identificação de desvios em relação ao padrão histórico dos usuários.

Dessa forma, a solução implementa mecanismos de análise comportamental compatíveis com User Behavior Analytics (UBA/UEBA), empregando métodos estatísticos de correlação, classificação e avaliação de risco para identificar desvios

de comportamento, atendendo ao requisito previsto no item 1.13.4.

Desta forma, a documentação comprova de forma robusta a utilização de mecanismos típicos de UEBA e análise estatística comportamental para identificação de desvios, atendendo substancialmente ao requisito do item 1.13.4, devendo a decisão ser reformada e a Netsafe classificada.

**1.13.11 A solução deve manter histórico de comportamento de usuários por pelo menos 12 meses.**

A retenção de dados é extendida de acordo com SKU de extensão de retenção de logs para 12 meses, em ambos Skyhigh CASB e Trellix DLP.

https://success.skyhighsecurity.com/Start_Here_with_Skyhigh_Security/Skyhigh_Security_Service_Edge/Skyhigh_Security_Cloud_Data_Retention

O requisito do item 1.13.11 é atendido, pois a documentação técnica demonstra expressamente que a solução possui mecanismos de retenção e manutenção de dados comportamentais de usuários por período igual ou superior a 12 meses.

A comprovação consta dos seguintes trechos:

"The data in the Skyhigh CASB for Shadow IT cloud infrastructure is aggregated on a daily, weekly, and monthly basis."

O fabricante informa que os dados coletados são preservados e consolidados historicamente em diferentes períodos temporais, permitindo análise longitudinal do comportamento dos usuários.

Adicionalmente:

"Aggregation keeps daily data for 45 days, weekly data for 13 weeks, and monthly data for 14 months."

Esse trecho demonstra expressamente a manutenção de dados históricos por até 14 meses, prazo superior ao mínimo de 12 meses exigido pelo edital.

A documentação também estabelece:

"Any data older than 14 months is deleted by default."

Tal declaração confirma que os dados permanecem armazenados e disponíveis até o limite de 14 meses.

Além disso, o fabricante informa:

"If you have purchased the Extended Sanctioned Data Plan, your data retention period for Sanctioned Data is 12 months instead of 100 days."

E:

"If you have purchased the Extended Sanctioned Data Plan, your data retention period for Web DLP Data is 12 months instead of 100 days."

Esses trechos demonstram que a solução oferece retenção de dados por período mínimo de 12 meses para os conjuntos de dados relacionados às atividades, incidentes e comportamento dos usuários.

A tabela de retenção também estabelece:

"Threats"

"Anomalies"

"Activities"

"Incidents"

como categorias de dados mantidas pela plataforma.

Conclusão técnica

A documentação comprova que a solução:

Mantém histórico de atividades dos usuários;

Mantém histórico de anomalias comportamentais;

Mantém histórico de incidentes;

Mantém histórico de ameaças;

Consolida informações históricas em bases mensais;

Retém dados por até 14 meses;

Disponibiliza opção contratual para retenção de dados sancionados por 12 meses completos.

Dessa forma, a solução possui capacidade de manutenção de histórico comportamental por período igual ou superior a 12 meses, atendendo ao requisito previsto no item 1.13.11, devendo a decisão ser reformada e a Netsafe classificada.

**1.13.17 A solução deve permitir segregação de políticas e perfis por grupos de usuários ou áreas.**

No Skyhigh CASB e no Trellix ePO (gerenciamento do Trellix DLP) permite criação de Funções (Roles) para os usuários que acessarão a console.

https://docs.trellix.com/bundle/epolicy-orchestrator-saas-product-guide/page/UUID-8ee70889-de6e-4fd3-6d8d-211790261961.html

O requisito do item 1.13.17 é atendido, pois a documentação técnica demonstra que a solução permite a criação de perfis de acesso personalizados, a definição de permissões específicas para cada perfil e a atribuição dessas permissões a usuários distintos, possibilitando a segregação administrativa por grupos, funções e responsabilidades organizacionais.

A comprovação consta dos seguintes trechos:

**"Administradores do ePO – SaaS podem criar funções com o agrupamento de permissões específicas."**

O fabricante informa expressamente que a solução permite criar funções (roles) contendo conjuntos específicos de permissões, possibilitando a segmentação de acessos e capacidades administrativas.

Adicionalmente:

**"Depois, é possível atribuir essas funções a outros usuários."**

Esse trecho demonstra que os perfis criados podem ser vinculados a usuários específicos, permitindo segregação de acesso conforme a necessidade organizacional.

A documentação também estabelece:

**"Na lista Permissões não atribuídas, selecione as permissões que você quer atribuir à função."**

Tal funcionalidade comprova que cada perfil pode possuir permissões próprias e independentes dos demais.

Além disso:

**"não é possível editar as funções padrão, mas você pode duplicá-las e editar as cópias."**

Esse recurso demonstra a possibilidade de criação de perfis personalizados a partir de modelos existentes, adequando-os às necessidades de diferentes áreas ou grupos de usuários.

Por fim:

**"No painel Atribuições de usuário, selecione a conta de usuário à qual você quer atribuir a função."**

Esse trecho comprova a associação individualizada de perfis aos usuários da plataforma.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite criar perfis de acesso personalizados;
- Permite definir permissões específicas para cada perfil;
- Permite criar múltiplos perfis independentes;
- Permite atribuir perfis distintos a diferentes usuários;
- Permite segregação de responsabilidades administrativas;
- Permite controle granular de permissões.

Dessa forma, a solução possui mecanismos de segregação de perfis e permissões por grupos funcionais de usuários, atendendo materialmente ao requisito previsto no item 1.13.17.

https://docs.trellix.com/pt-PT/bundle/epolicy-orchestrator-saas-product-guide/page/UUID-bbfe3c4b-7ae4-d849-4da6-3e063af20cb4.html

**Redação objetiva para recurso**

O requisito do item 1.13.17 é atendido, pois a documentação técnica demonstra expressamente que a solução permite a criação, atribuição e gerenciamento de múltiplos perfis de acesso (roles), possibilitando a segregação de permissões e responsabilidades entre diferentes usuários, grupos funcionais e áreas da organização.

A comprovação consta dos seguintes trechos:

**"You can assign a role to the multiple users when it has appropriate permissions."**

O fabricante informa expressamente que uma mesma função pode ser atribuída a múltiplos usuários, permitindo a organização dos acessos por grupos de usuários que compartilham responsabilidades semelhantes.

Adicionalmente:

**"You can also assign multiple roles to users which give them an accumulation of permissions granted by each of the roles."**

Tal funcionalidade demonstra a possibilidade de composição de perfis específicos para diferentes áreas ou funções organizacionais, mediante combinação de permissões distintas.

A documentação também estabelece:

**"The details show which roles are assigned to the selected user."**

Esse trecho comprova a existência de controle individualizado dos perfis atribuídos a cada usuário.

Além disso:

**"From the Unassigned Roles list, select the roles that you want to assign."**

E:

**"From the Assigned Roles list, deselect the roles that you want to unassign."**

Tais funcionalidades demonstram gerenciamento granular dos perfis de acesso e segregação das permissões concedidas aos usuários.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite criar funções (roles) específicas;
- Permite atribuir diferentes perfis a diferentes usuários;
- Permite atribuir um mesmo perfil a múltiplos usuários;
- Permite associar múltiplos perfis ao mesmo usuário;
- Permite segregação granular de permissões;
- Permite controle individualizado dos acessos.

Dessa forma, a solução implementa mecanismo de controle baseado em perfis (RBAC - Role Based Access Control), permitindo segregação de acessos, responsabilidades e permissões por grupos de usuários e áreas organizacionais, atendendo ao requisito previsto no item 1.13.17.

https://docs.trellix.com/bundle/data-loss-prevention-saas-product-guide/page/UUID-b3292ed7-9b11-bc26-50ef-0b4f2358a560.html

O requisito do item 1.13.17 é atendido, pois a documentação técnica demonstra expressamente que a solução permite a criação de perfis com permissões distintas, a atribuição dessas permissões a usuários específicos e a segregação de acesso às funcionalidades, políticas e objetos administrativos da plataforma.

A comprovação consta dos seguintes trechos:

**"Administrators can add users and assign specific roles to them."**

O fabricante informa expressamente que a solução permite atribuir funções específicas aos usuários, possibilitando a segregação de acessos conforme a responsabilidade de cada perfil.

Adicionalmente:

**"Administrators control what users see and what they can access by adding and assigning roles to users."**

Esse trecho demonstra que os administradores controlam de forma granular quais funcionalidades e informações cada usuário pode acessar.

A documentação também estabelece:

**"All roles have specific permission sets."**

Tal funcionalidade comprova que cada perfil possui um conjunto próprio de permissões, permitindo a segregação de responsabilidades e acessos.

Além disso, o fabricante informa:

**"The permission sets cover Data Protection, including Classifications, DLP Definition, DLP Help Desk, DLP Policy Manager, DLP Settings, Incident Management, and Operational Event Management."**

Esse trecho é particularmente relevante porque demonstra que a segregação não se limita ao acesso à plataforma, mas alcança diretamente os módulos de políticas DLP, classificações, gerenciamento de incidentes e configurações da solução.

A documentação ainda prevê três níveis distintos de permissão:

**"Use"**

**"View and use"**

**"Full permissions"**

Com as seguintes capacidades:

**"Permission to view only names of objects"**

**"Permission to view details of objects, but not to change them"**

**"Permission to create and change objects"**

Tais níveis demonstram segregação hierárquica de acesso às funcionalidades administrativas da solução.

Por fim:

**"To assign or remove permissions for a user, select or deselect the permission checkboxes displayed for a role."**

Esse trecho comprova a atribuição granular de permissões de acordo com o perfil e a necessidade de cada usuário ou área.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite criação de perfis distintos;
- Permite atribuição de perfis específicos a usuários;
- Permite segregação de permissões;
- Permite controle granular de acesso;
- Permite segregação das funções de administração;
- Permite segregação de acesso às políticas DLP;
- Permite segregação de acesso às classificações;
- Permite segregação de gerenciamento de incidentes;
- Permite diferentes níveis hierárquicos de permissão.

Dessa forma, a solução implementa mecanismos de segregação de perfis e de administração de políticas por meio de controle baseado em funções (RBAC), atendendo ao requisito previsto no item 1.13.17.

https://success.skyhighsecurity.com/Skyhigh_CASB/03_Skyhigh_RBAC_and_User_Management/Manage_Users_and_Roles/02_Manage_Users/About_the_Users_Page

O requisito do item 1.13.17 é atendido de forma expressa, pois a documentação técnica demonstra que a solução permite a criação de perfis (roles), agrupamento de permissões, atribuição de múltiplos perfis a usuários, edição em massa de permissões e segregação administrativa por jurisdição, grupos e áreas de atuação.

A comprovação consta dos seguintes trechos:

**"You can group Permissions to create a role and assign it to users."**

O fabricante informa expressamente que as permissões podem ser agrupadas para formar perfis específicos, posteriormente atribuídos aos usuários da plataforma.

Adicionalmente:

**"Permissions define the actions users can perform, and roles group those permissions to manage access."**

Esse trecho demonstra que o controle de acesso é baseado em perfis com permissões específicas, permitindo segregação funcional e administrativa.

A documentação também estabelece:

**"You can assign multiple roles to an existing or a new user."**

Tal funcionalidade comprova a possibilidade de composição de perfis distintos conforme a necessidade de cada usuário, grupo ou área organizacional.

Além disso, o fabricante informa:

**"All Roles. The menu lists all the created roles for a specific tenant."**

E:

**"Select a role to narrow your search."**

Demonstrando a existência de múltiplos perfis independentes dentro do mesmo ambiente.

A documentação ainda prevê:

**"Bulk User Edit"**

Com as funcionalidades:

**"Edit user permissions"**

**"Edit Roles"**

**"Change Access (Manage/Read Only)"**

Tais recursos evidenciam a administração centralizada e segmentada dos perfis e permissões.

Particularmente relevante para o requisito é a funcionalidade de segregação por domínios organizacionais:

**"Set Shadow Jurisdiction"**

**"Set Sanctioned Jurisdiction"**

**"Set Web Jurisdiction"**

**"Set Saved View Jurisdiction"**

Esses mecanismos demonstram que a solução permite restringir acessos e atribuições conforme escopos específicos de atuação, promovendo segregação administrativa e operacional entre diferentes áreas ou grupos de usuários.

Por fim:

**"The table displays only users assigned to this role."**

Esse trecho reforça a capacidade de organização e segregação dos usuários por perfis específicos.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite criação de perfis personalizados;
- Permite agrupamento de permissões por perfil;
- Permite atribuição de múltiplos perfis aos usuários;

- Permite edição granular de permissões;
- Permite segregação de acessos;
- Permite segregação administrativa por jurisdição;
- Permite segregação por grupos de usuários;
- Permite segregação por escopos operacionais distintos;
- Permite administração centralizada dos perfis e permissões.

Dessa forma, a solução implementa mecanismos robustos de segregação de perfis, permissões e domínios administrativos, atendendo integralmente ao requisito previsto no item 1.13.17.

Desta forma é cabal que a Netsafe atendeu ao requisito do Edital, devendo a decisão ser reformada e a Netsafe classificada.

**1.14.1 A solução deve exportar logs e eventos para SIEMs de mercado (Splunk, QRadar, ArcSight, LogRhythm, Microsoft Sentinel, etc.).**

A solução Skyhigh permite exportação de logs e eventos para diversos SIEMs de mercado via Syslog utilizando componente onpremise Cloud Connector.

Para o Trellix DLP, é possível se conectar via API e efetuar a coleta dos eventos e exportar para Syslog ou outra localidade, a depender do conector existente no SIEM em questão ou Scripts (customizados). Se for utilizado ambiente onpremise para DLP Endpoint, os eventos de Trellix DLP podem ser exportados diretamente para um Syslog.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Cloud_Connector_Configuration/Advanced_Configuration_and_Migration/SIEM_Integration_(Inline)

O requisito do item 1.14.1 é atendido, pois a documentação técnica demonstra expressamente que a solução permite a

exportação de logs, eventos, incidentes, anomalias, ameaças e registros de auditoria para sistemas SIEM de terceiros, utilizando mecanismos padronizados de integração amplamente adotados pelo mercado, incluindo Syslog, JSON, CSV e KVP.

A comprovação consta dos seguintes trechos:

**"Use SIEM Integration (Inline) to export Security Service Edge (SSE) web access data to your third-party SIEM systems (Security Information and Event Management)."**

O fabricante informa expressamente que a solução permite exportar dados e logs para sistemas SIEM de terceiros.

Adicionalmente:

**"Use SIEM Integration (SaaS) to export Anomalies, Threats, Incidents, and Audit Logs to your third-party SIEM systems."**

Esse trecho comprova que a integração não se limita a logs de acesso, abrangendo também:

- Anomalies;
- Threats;
- Incidents;
- Audit Logs.

A documentação também estabelece:

**"The Log Collector retrieves and stores the logs at configured intervals."**

E:

**"send them from Skyhigh CASB to your third-party SIEM systems (Security Information and Event Management) through a Syslog server."**

Tal funcionalidade demonstra a exportação automatizada de eventos para plataformas SIEM por meio do protocolo Syslog, padrão amplamente suportado pelas principais soluções do mercado.

Além disso, o fabricante informa:

**"Use this option to send the log files to the Syslog server."**

E:

**"Protocol. Choose a protocol option for transport. It transfers the data to the Syslog server using TCP or UDP."**

Esses trechos comprovam compatibilidade com arquiteturas SIEM corporativas baseadas em Syslog TCP/UDP.

A documentação ainda prevê múltiplos formatos de exportação:

**"CSV"**

**"JSON"**

**"KVP"**

Demonstrando interoperabilidade com diferentes mecanismos de ingestão utilizados por plataformas de monitoramento e correlação de eventos.

Por fim:

**"The Log Collector can simultaneously download the data originating from different log types such as SWG, Remote Browser Isolation (RBI), Private Access, and Cloud Firewall."**

Esse trecho evidencia a capacidade de centralização e exportação de múltiplas fontes de eventos para sistemas externos de análise.

**Conclusão técnica**

A documentação comprova que a solução:

- Exporta logs para SIEMs de terceiros;
- Exporta anomalias;
- Exporta ameaças;
- Exporta incidentes;
- Exporta logs de auditoria;
- Utiliza protocolo Syslog;

- Suporta TCP e UDP;
- Exporta dados em JSON;
- Exporta dados em CSV;
- Exporta dados em KVP;
- Integra-se com plataformas externas de correlação de eventos.

Dessa forma, a solução possui mecanismos nativos de integração com sistemas SIEM de mercado, atendendo integralmente ao requisito previsto no item 1.14.1.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Cloud_Connector_Integrations/Cloud_Connector_SIEM_Integration/Exporting_Anomalies_and_Threats_to_a_SIEM

O requisito do item 1.14.1 é atendido de forma expressa e inequívoca, pois a documentação técnica do fabricante demonstra não apenas a capacidade de exportação de logs e eventos para plataformas SIEM de mercado, mas também identifica nominalmente diversas soluções SIEM compatíveis, incluindo aquelas exemplificadas no próprio edital.

A comprovação consta dos seguintes trechos:

**"You can export anomalies, threats, incidents, and the Audit Log from Skyhigh CASB to your third-party SIEM systems using Syslog export."**

O fabricante informa expressamente que a solução permite exportar:

- Anomalias;
- Ameaças;
- Incidentes;
- Logs de Auditoria;

para sistemas SIEM de terceiros.

Adicionalmente:

**"This export is handled through the Skyhigh Cloud Connector."**

Demonstrando a existência de mecanismo nativo de integração para exportação dos eventos.

A documentação também estabelece:

**"Use this feature to export data to another system for further analysis."**

Tal funcionalidade evidencia que os dados exportados podem ser consumidos por plataformas externas de monitoramento, correlação e análise.

Particularmente relevante para o atendimento do requisito, o fabricante identifica expressamente os SIEMs suportados:

**"Supported Third-Party SIEMs for Integration with Skyhigh CASB"**

E lista nominalmente:

**"IBM QRadar"**

**"ArcSight"**

**"LogRhythm"**

**"Splunk"**

Além de:

**"Securonix"**

**"AlienVault"**

**"NetWitness"**

**"FortiSIEM"**

**"Exabeam"**

**"Broadcom Information Centric Analytics (ICA)"**

**"SolarWinds Security Event Manager (SEM)"**

**"SolarWinds Loggly"**

A documentação também comprova compatibilidade com os principais formatos utilizados por SIEMs corporativos:

**"Common Event Format (CEF)"**

**"Log Event Extended Format (LEEF)"**

**"Skyhigh CASB Key Value"**

Além disso, a exportação ocorre via:

**"Syslog export"**

mecanismo universalmente suportado pelas plataformas SIEM corporativas.

**Conclusão técnica**

A documentação comprova que a solução:

- Exporta logs e eventos para SIEMs;
- Exporta anomalias;
- Exporta ameaças;
- Exporta incidentes;
- Exporta logs de auditoria;
- Utiliza Syslog;
- Suporta formato CEF;
- Suporta formato LEEF;
- Suporta formatos proprietários compatíveis;
- Integra-se nominalmente com Splunk;
- Integra-se nominalmente com IBM QRadar;
- Integra-se nominalmente com ArcSight;
- Integra-se nominalmente com LogRhythm;
- Integra-se com diversos outros SIEMs corporativos.

Dessa forma, a solução atende integralmente ao requisito previsto no item 1.14.1.

https://developer.manage.trellix.com/public/mvision/apis/incident

**Redação objetiva para recurso**

O requisito do item 1.14.1 é atendido, pois a documentação técnica demonstra que a solução disponibiliza APIs estruturadas para extração automatizada de incidentes de segurança, permitindo integração programática com plataformas externas de monitoramento, correlação de eventos, SIEM e SOAR.

A comprovação consta dos seguintes trechos:

**"Incident APIs."**

O fabricante informa expressamente a existência de APIs dedicadas ao acesso e integração dos incidentes registrados pela solução.

Adicionalmente:

**"The following API allows for the retrieval of these incidents in bulk."**

Esse trecho demonstra que a solução permite extração automatizada e massiva dos incidentes de segurança, característica essencial para integração com SIEMs corporativos.

A documentação também estabelece:

**"with the ability to constrain the results to a specific time period."**

Tal funcionalidade comprova a capacidade de consultas parametrizadas, permitindo sincronização incremental e ingestão contínua de eventos por plataformas externas.

Além disso, a documentação disponibiliza endpoints específicos:

**"GET /dpim/v2/incident"**

**"GET /dpim/v2/incident/{incidentId}"**

Demonstrando a capacidade de recuperação programática tanto de conjuntos de incidentes quanto de incidentes individuais.

Particularmente relevante é a estrutura de dados disponibilizada pela API, que contempla objetos como:

**"eventUser"**

**"policy"**

**"classification"**

**"application"**

**"cloudInfo"**

**"deviceInfo"**

**"endpoint"**

**"emailInfo"**

**"networkCommInfo"**

**"evidenceDetails"**

**"collaboration"**

**"status"**

Esses elementos demonstram que a API fornece dados ricos e estruturados para correlação de eventos, investigação e integração com plataformas de monitoramento e inteligência de segurança.

**Conclusão técnica**

A documentação comprova que a solução:

- Disponibiliza APIs para integração;
- Permite recuperação automatizada de incidentes;
- Permite recuperação em massa (bulk retrieval);
- Permite consultas por período;
- Permite integração contínua com sistemas externos;
- Disponibiliza metadados detalhados dos incidentes;

- Fornece informações de usuários, dispositivos, aplicações, políticas, classificações e evidências;
- Permite consumo programático por plataformas SIEM e SOAR.

Dessa forma, a solução possui mecanismos nativos de integração e exportação de eventos de segurança para ferramentas externas de correlação e monitoramento, atendendo ao requisito previsto no item 1.14.1.

https://docs.trellix.com/bundle/trellix-epolicy-orchestrator-on-prem-5.10.0-product-guide/page/UUID-8919f78f-0968-023f-449b-b2899a6d9c7f.html

O requisito do item 1.14.1 é atendido, pois a documentação técnica demonstra expressamente que a solução permite encaminhamento e exportação de eventos para servidores Syslog, mecanismo amplamente utilizado para integração com plataformas SIEM de mercado.

A comprovação consta dos seguintes trechos:

**"Você pode ativar o ePO – On-prem para sincronização com o servidor syslog."**

O fabricante informa expressamente que a solução possui integração nativa com servidores Syslog.

Adicionalmente:

**"Um syslog é uma forma de dispositivos de rede enviarem mensagens de eventos para um servidor de log separado."**

Esse trecho demonstra que a funcionalidade é destinada justamente ao envio e centralização de eventos em plataformas externas de monitoramento.

A documentação também estabelece:

**"Você pode usar o syslog para coletar informações sobre eventos de ameaça específicos."**

Tal funcionalidade comprova a exportação de eventos de segurança para sistemas externos.

Além disso:

**"Ativar encaminhamento de evento: clique para ativar o encaminhamento de evento no Manipulador de agentes para este servidor syslog."**

Esse trecho demonstra expressamente a capacidade de encaminhamento de eventos da plataforma para um servidor Syslog.

Por fim:

**"Após registrar o servidor syslog, você poderá configurar o ePO – On-prem para enviar eventos ao servidor syslog."**

O fabricante declara de forma inequívoca que a solução envia eventos para servidores Syslog externos.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite integração com servidores Syslog;
- Permite encaminhamento de eventos;
- Permite exportação de eventos de segurança;
- Permite envio de eventos para sistemas externos;
- Utiliza protocolo Syslog padronizado;
- Suporta comunicação via TCP/TLS;
- Permite centralização de logs e eventos.

Dessa forma, a solução possui mecanismo nativo de exportação de eventos compatível com arquiteturas SIEM de mercado, atendendo ao requisito previsto no item 1.14.1.

Desta forma, o item 1.14.1 foi integralmente atendido pela NETSAFE, sendo compatível com o requerido pelo Edital.

### 1.14.2 A integração deve utilizar protocolos padrão (Syslog, CEF).

A solução permite exportar em formato CEF ou LEEF e para Syslog. Para o Trellix DLP, a API permite efetuar a coleta dos eventos no serviço da Trellix. Se utilizar ambiente onpremise da Trellix, é possível exportar diretamente para servidor Syslog.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Cloud_Connector_Configuration/Advanced_Configuration_and_Migration/SIEM_Integration_(Inline)

O requisito do item 1.14.2 é atendido, pois a documentação técnica demonstra expressamente que a integração da solução com plataformas SIEM utiliza o protocolo padrão **Syslog**, amplamente adotado pelo mercado para transporte de logs e eventos de segurança.

A comprovação consta dos seguintes trechos:

**"Use SIEM Integration (Inline) to export Security Service Edge (SSE) web access data to your third-party SIEM systems (Security Information and Event Management)."**

O fabricante informa expressamente que a solução exporta logs e eventos para plataformas SIEM de terceiros.

Adicionalmente:

**"You can save the logs to a local directory or send them from Skyhigh CASB to your third-party SIEM systems (Security Information and Event Management) through a Syslog server."**

Esse trecho comprova expressamente a utilização do protocolo **Syslog** para integração com plataformas SIEM.

A documentação também estabelece:

**"Send as Syslogs"**

E:

**"Use this option to send the log files to the Syslog server."**

Demonstrando a existência de funcionalidade nativa de exportação por Syslog.

Além disso:

**"Protocol. Choose a protocol option for transport. It transfers the data to the Syslog server using TCP or UDP depending on your selection."**

Esse trecho comprova compatibilidade com os padrões de transporte normalmente utilizados em integrações Syslog corporativas.

**Complementação documental**

A compatibilidade com formatos padronizados utilizados por plataformas SIEM é reforçada pela documentação do fabricante que estabelece:

**"ArcSight – Common Event Format (CEF), LEEF"**

**"Splunk – CEF, LEEF"**

**"IBM QRadar – Log Event Extended Format (LEEF)"**

**"LogRhythm – LEEF"**

Esses trechos demonstram que a solução suporta formatos padronizados de mercado utilizados por SIEMs corporativos, incluindo expressamente o **Common Event Format (CEF)**, mencionado no próprio requisito editalício.

**Conclusão técnica**

A documentação comprova que a solução:

- Exporta eventos para SIEMs;
- Utiliza protocolo Syslog;
- Suporta transporte TCP;
- Suporta transporte UDP;
- Integra-se com servidores Syslog;
- Suporta Common Event Format (CEF);
- Suporta Log Event Extended Format (LEEF);
- Integra-se com Splunk;
- Integra-se com ArcSight;

- Integra-se com QRadar;
- Integra-se com LogRhythm.

Dessa forma, a solução utiliza protocolos e formatos padronizados de mercado para integração com plataformas SIEM, atendendo integralmente ao requisito previsto no item 1.14.2.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Cloud_Connector_Integrations/Cloud_Connector_SIEM_Integration/Exporting_Anomalies_and_Threats_to_a_SIEM

O requisito do item 1.14.2 é atendido de forma expressa, pois a documentação técnica do fabricante demonstra que a integração com plataformas SIEM utiliza os protocolos e formatos padronizados exigidos pelo edital, incluindo **Syslog** e **Common Event Format (CEF)**.

A comprovação consta dos seguintes trechos:

**"You can export anomalies, threats, incidents, and the Audit Log from Skyhigh CASB to your third-party SIEM systems using Syslog export."**

O fabricante informa expressamente que a exportação de eventos para SIEMs ocorre por meio de **Syslog**, protocolo expressamente previsto no requisito editalício.

Adicionalmente:

**"Configure a SIEM Syslog Service"**

Esse trecho reforça a utilização nativa do protocolo Syslog para integração com plataformas externas de monitoramento e correlação de eventos.

A documentação também estabelece:

**"Common Event Format"**

E:

**"For the full definition, see the ArcSight Common Event Format Guide."**

Tais trechos demonstram expressamente suporte ao formato **CEF (Common Event Format)**, exatamente o padrão mencionado no item 1.14.2.

Além disso, o fabricante informa compatibilidade direta com plataformas SIEM que utilizam CEF:

**"ArcSight – Common Event Format (CEF), LEEF"**

**"Splunk – CEF, LEEF, and Skyhigh CASB Key Value"**

**"Trellix Enterprise Security Manager (ESM) – CEF, LEEF"**

**"Securonix – CEF, LEEF"**

**"AlienVault – CEF, LEEF"**

**"NetWitness – CEF"**

**"FortiSIEM – CEF"**

**"Exabeam – CEF, LEEF"**

**"Broadcom Information Centric Analytics (ICA) – CEF, LEEF"**

**"SolarWinds Security Event Manager (SEM) – CEF, LEEF"**

**"SolarWinds Loggly – CEF"**

A documentação ainda demonstra compatibilidade com outro padrão amplamente adotado pelo mercado:

**"Log Event Extended Format (LEEF)"**

Utilizado por plataformas como IBM QRadar.

**Conclusão técnica**

A documentação comprova que a solução:

- Utiliza Syslog para exportação de eventos;
- Suporta Common Event Format (CEF);
- Suporta Log Event Extended Format (LEEF);
- Exporta anomalias;
- Exporta ameaças;
- Exporta incidentes;

- Exporta logs de auditoria;
- Integra-se com SIEMs corporativos por formatos padronizados de mercado.

Dessa forma, a solução atende integralmente ao requisito previsto no item 1.14.2.

https://developer.manage.trellix.com/public/mvision/apis/incident

O requisito do item 1.14.2 é atendido, pois a documentação técnica demonstra que a solução disponibiliza integração baseada em **API REST**, utilizando protocolos abertos e amplamente adotados pelo mercado para intercâmbio de eventos, incidentes e informações de segurança.

A comprovação consta dos seguintes trechos:

**"Incident APIs."**

O fabricante informa expressamente a existência de APIs destinadas à integração e recuperação de incidentes de segurança.

Adicionalmente:

**"The following API allows for the retrieval of these incidents in bulk, with the ability to constrain the results to a specific time period."**

Esse trecho demonstra que a solução permite a extração automatizada de incidentes por meio de integração programática, incluindo consultas filtradas por período.

A documentação também estabelece os seguintes endpoints:

**"GET /dpim/v2/incident"**

**"GET /dpim/v2/incident/{incidentId}"**

Tais recursos comprovam a disponibilização de interface de integração baseada em serviços REST para consulta de incidentes.

Além disso, a documentação identifica um endpoint dedicado:

**"https://api.manage.trellix.com"**

Demonstrando a existência de infraestrutura própria de APIs para integração com sistemas externos.

Por fim, a estrutura dos dados disponibilizados pela API contempla informações detalhadas relacionadas aos incidentes, incluindo:

**"eventUser"**

**"policy"**

**"classification"**

**"deviceInfo"**

**"cloudInfo"**

**"application"**

**"emailInfo"**

**"networkCommInfo"**

**"evidenceDetails"**

Esses elementos demonstram que a API fornece informações completas para consumo por plataformas externas de monitoramento, SIEM e automação de segurança.

**Conclusão técnica**

A documentação comprova que a solução:

- Disponibiliza APIs para integração;
- Permite recuperação automatizada de incidentes;
- Permite consultas em massa (bulk retrieval);
- Permite consultas filtradas por período;
- Disponibiliza endpoints REST;
- Permite integração com sistemas externos;

- Fornece informações estruturadas para correlação e análise de eventos.

https://docs.trellix.com/bundle/trellix-epolicy-orchestrator-on-prem-5.10.0-product-guide/page/UUID-8919f78f-0968-023f-449b-b2899a6d9c7f.html

O requisito do item 1.14.2 é atendido, pois a documentação técnica demonstra expressamente que a solução utiliza o protocolo padrão **Syslog** para encaminhamento e exportação de eventos de segurança, empregando ainda comunicação segura por meio de **TCP/TLS**.

A comprovação consta dos seguintes trechos:

**"Você pode ativar o ePO – On-prem para sincronização com o servidor syslog."**

O fabricante informa expressamente que a solução possui integração nativa com servidores Syslog.

Adicionalmente:

**"Um syslog é uma forma de dispositivos de rede enviarem mensagens de eventos para um servidor de log separado."**

Esse trecho demonstra que o protocolo Syslog é utilizado para transmissão de eventos e registros gerados pela solução.

A documentação também estabelece:

**"O encaminhamento de syslog do ePO – On-prem somente é compatível com o protocolo TCP e requer o Transport Layer Security (TLS)."**

Tal funcionalidade comprova que a integração utiliza protocolo padronizado de mercado (Syslog), transportado por TCP e protegido por TLS.

Além disso:

**"Ativar encaminhamento de evento: clique para ativar o encaminhamento de evento no Manipulador de agentes para este servidor syslog."**

Esse trecho demonstra expressamente a capacidade de encaminhamento de eventos para infraestrutura externa de coleta e correlação.

Por fim:

**"Após registrar o servidor syslog, você poderá configurar o ePO – On-prem para enviar eventos ao servidor syslog."**

O fabricante confirma de forma inequívoca que a solução exporta eventos utilizando Syslog.

**Conclusão técnica**

A documentação comprova que a solução:

- Utiliza protocolo Syslog;
- Permite exportação de eventos;
- Permite encaminhamento de eventos de segurança;
- Integra-se com servidores de logs externos;
- Utiliza TCP como protocolo de transporte;
- Utiliza TLS para proteção da comunicação;
- Possui mecanismo nativo de integração baseado em padrões de mercado.

Dessa forma, a solução atende ao requisito previsto no item 1.14.2 quanto à utilização de protocolos padrão para integração.

### 1.14.3 A solução deve permitir configuração granular de eventos exportados.

O Trellix DLP, para ambiente SaaS, via API pode ser definido o que deseja ser coletado.

Para Trellix DLP em ambiente onpremise, pode ser definido que tipo de evento será enviado para Syslog.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Cloud_Connector_Integrations/Cloud_Connector_SIEM_Integration/Exporting_Anomalies_and_Threats_to_a_SIEM

O requisito do item 1.14.3 é atendido, pois a documentação técnica demonstra que a solução permite selecionar os tipos de eventos exportados, configurar formatos de exportação distintos, definir periodicidade de coleta e personalizar a forma de envio dos dados para plataformas SIEM.

A comprovação consta dos seguintes trechos:

**"You can export anomalies, threats, incidents, and the Audit Log from Skyhigh CASB to your third-party SIEM systems using Syslog export."**

O fabricante informa expressamente que a exportação pode abranger diferentes categorias de eventos, incluindo:

- Anomalies;
- Threats;
- Incidents;
- Audit Logs.

Tal funcionalidade demonstra a capacidade de seleção dos conjuntos de eventos exportados.

Adicionalmente:

**"By default, Cloud Connector fetches incidents from Skyhigh CASB every four hours. You can customize this interval in the logprocessor.local.properties file using the property siem.frequency=."**

Esse trecho comprova a possibilidade de configuração da periodicidade de exportação dos eventos.

A documentação também estabelece diferentes formatos de exportação:

**"IBM QRadar – Log Event Extended Format (LEEF)"**

**"ArcSight – Common Event Format (CEF), LEEF"**

**"Splunk – CEF, LEEF, and Skyhigh CASB Key Value"**

Demonstrando que a exportação pode ser adaptada ao formato requerido por cada plataforma de destino.

Além disso, a documentação descreve configurações específicas para cada formato:

**"Export Format Details"**

**"Key Value Pairs"**

**"Log Event Extended Format (LEEF)"**

**"Common Event Format"**

O que evidencia controle sobre a estrutura e formatação dos eventos exportados.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite selecionar categorias distintas de eventos para exportação;
- Permite exportar anomalias;
- Permite exportar ameaças;
- Permite exportar incidentes;
- Permite exportar logs de auditoria;
- Permite configurar periodicidade de exportação;
- Permite utilizar formatos distintos de exportação;
- Permite adequar os eventos ao SIEM de destino;
- Permite personalização da estrutura dos registros exportados.

Dessa forma, a solução possui mecanismos de configuração e controle sobre os eventos exportados para plataformas SIEM, atendendo ao requisito previsto no item 1.14.3.

https://developer.manage.trellix.com/public/mvision/apis/incident

O requisito do item 1.14.3 é atendido, pois a documentação técnica demonstra que a solução permite recuperação seletiva, filtrada e estruturada dos eventos e incidentes de segurança por meio de APIs, possibilitando controle granular sobre os dados exportados e consumidos por sistemas externos.

A comprovação consta dos seguintes trechos:

**"The following API allows for the retrieval of these incidents in bulk, with the ability to constrain the results to a specific time period."**

O fabricante informa expressamente que a exportação dos incidentes pode ser restringida a períodos específicos, permitindo filtragem e seleção dos eventos a serem recuperados.

Adicionalmente, a documentação disponibiliza endpoints específicos para consulta:

**"GET /dpim/v2/incident"**

**"GET /dpim/v2/incident/{incidentId}"**

Esses recursos demonstram a possibilidade de recuperar tanto conjuntos de incidentes quanto incidentes individualizados, evidenciando controle detalhado sobre os dados exportados.

A documentação também estabelece uma estrutura rica e granular de informações associadas aos incidentes, incluindo:

**"policy"**

**"classification"**

**"application"**

**"cloudInfo"**

**"eventUser"**

**"deviceInfo"**

**"emailInfo"**

**"networkCommInfo"**

**"collaboration"**

**"evidenceDetails"**

**"status"**

Tais elementos demonstram que a exportação pode contemplar diferentes categorias de informações relacionadas ao incidente, permitindo elevado grau de detalhamento dos dados consumidos por plataformas externas.

Além disso, a presença dos objetos:

**"paginationCursorLinks"**

e

**"status"**

evidencia mecanismos de paginação, segmentação e controle sobre o volume de dados recuperados.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite exportação programática de incidentes;
- Permite recuperação em massa (bulk retrieval);
- Permite recuperação individual de incidentes;
- Permite filtragem por período;
- Disponibiliza metadados detalhados dos eventos;
- Permite segmentação dos dados exportados;
- Disponibiliza diferentes categorias de informações relacionadas ao incidente;
- Permite controle granular sobre o conteúdo recuperado pelas integrações.

Dessa forma, a solução possui mecanismos de configuração e seleção dos eventos exportados por meio de APIs

estruturadas, atendendo ao requisito previsto no item 1.14.3, ou seja, a possibilidade de restringir e filtrar os eventos recuperados. Esse é justamente um dos elementos mais relevantes quando se fala em **configuração granular de eventos exportados**.

https://docs.trellix.com/bundle/trellix-epolicy-orchestrator-on-prem-5.10.0-product-guide/page/UUID-90e1626b-da28-a42c-6a65-e20dcb107530.html

O requisito do item 1.14.3 é atendido de forma expressa, pois a documentação técnica demonstra que a solução permite selecionar individualmente quais eventos serão exportados, definir sua origem e configurar de forma específica o destino dos eventos, inclusive para encaminhamento ao servidor Syslog.

A comprovação consta dos seguintes trechos:

**"Você pode determinar quais eventos serão encaminhados para o servidor usando as configurações do servidor e a filtragem de eventos."**

O fabricante informa expressamente que a solução permite controlar e definir quais eventos serão encaminhados, evidenciando configuração granular da exportação.

Adicionalmente:

**"Selecione os eventos que devem ser encaminhados, todos ou eventos individuais."**

Esse trecho demonstra de forma inequívoca a capacidade de selecionar individualmente os eventos que serão exportados.

A documentação também estabelece:

**"Para encaminhar somente os eventos especificados, selecione Somente eventos selecionados para o servidor."**

Tal funcionalidade comprova a existência de filtragem seletiva dos eventos exportados.

Além disso, o fabricante prevê diferentes opções de encaminhamento:

**"Encaminhar selecionados para syslog."**

**"Armazenar selecionados em ambos."**

**"Armazenar selecionados no Trellix ePO."**

Esses recursos demonstram que a exportação pode ser configurada de forma específica para cada conjunto de eventos.

A documentação ainda permite filtragem por origem:

**"Selecione a origem do evento."**

**"Eventos de qualquer origem."**

**"Eventos gerados pelo agente emissor."**

Esse trecho evidencia controle adicional sobre quais eventos serão exportados com base na origem das ocorrências.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite selecionar eventos individualmente;
- Permite exportar todos os eventos ou apenas eventos específicos;
- Permite filtrar eventos antes da exportação;
- Permite selecionar a origem dos eventos;
- Permite encaminhar apenas eventos selecionados para Syslog;
- Permite definir diferentes destinos para os eventos;
- Permite armazenar ou encaminhar eventos conforme configuração administrativa.

Dessa forma, a solução possui mecanismos explícitos de configuração granular dos eventos exportados, atendendo integralmente ao requisito previsto no item 1.14.3.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Cloud_Connector_Integrations/Cloud_Connector_SIEM_Integration/Cloud_Connector_SIEM_Integration_Formats

O requisito do item 1.14.3 é atendido de forma expressa, pois a documentação técnica demonstra que a solução permite configurar granularmente os eventos exportados, incluindo a seleção dos tipos de eventos, dos campos transmitidos e do formato utilizado na integração com plataformas SIEM.

A comprovação consta dos seguintes trechos:

**"You can export anomalies, threats, incidents, and the Audit Log from Skyhigh CASB to your third-party SIEM systems using Syslog export."**

O fabricante informa expressamente que a exportação pode ser realizada para diferentes categorias de eventos, incluindo:

- Anomalies;
- Threats;
- Incidents;
- Audit Logs.

Tal funcionalidade demonstra seleção por categoria de evento.

Adicionalmente, a documentação apresenta diferentes formatos de exportação:

**"Common Event Format (CEF)"**

**"Log Event Extended Format (LEEF)"**

**"Skyhigh CASB Key Value Format"**

A existência de múltiplos formatos evidencia capacidade de adequação da exportação às necessidades específicas do SIEM de destino.

Além disso, a documentação detalha os campos exportados para cada tipo de evento, incluindo:

**"incidentId"**

**"riskSeverity"**

**"policyId"**

**"policyName"**

**"serviceNames"**

**"activityName"**

**"userDisplayName"**

**"sourceIps"**

**"contentItemName"**

**"contentItemType"**

**"incidentRiskScore"**

**"informationMitreTactic"**

**"informationMitreTechnique"**

**"auditEventTypeEventCategoryName"**

**"auditEventTypeEventTypeName"**

A documentação demonstra ainda que diferentes tipos de eventos exportam conjuntos distintos de atributos, como:

**Shadow Anomaly**

**Sanctioned Anomaly**

**DLP Policy Violation**

**Threat**

**Config Audit**

**Audit Logs**

Cada categoria possui campos próprios e específicos, evidenciando granularidade na composição dos registros exportados.

**Conclusão técnica**

A documentação comprova que a solução:

- Permite selecionar categorias distintas de eventos;
- Permite exportar anomalias;
- Permite exportar ameaças;
- Permite exportar incidentes;
- Permite exportar auditorias;
- Permite utilizar formatos distintos (CEF, LEEF e Key Value);
- Permite exportar conjuntos específicos de atributos;
- Permite exportar informações de usuário, políticas, serviços, dispositivos, conteúdo e risco;
- Permite adequação dos eventos ao SIEM de destino.

Dessa forma, a solução possui mecanismos de configuração granular dos eventos exportados, atendendo ao requisito previsto no item 1.14.3.

Desta forma, o requisito do item 1.14.3 é totalmente atendido pela Netsafe, razão pela qual a decisão de desclassificação deve ser reformada e a Netsafe classificada.

**1.14.4 A solução deve fornecer dashboards de integração para monitorar o envio de eventos.**

O Cloud Connector, responsável por exportar eventos do Skyhigh, mostra tela de status para exibir informações como Uso do Sistema, Detalhes do Conector, Processamento dos Logs e Integrações.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Set_Up_Cloud_Connector/Check_the_Status_of_Cloud_Connector

O requisito do item 1.14.4 é atendido, pois a documentação técnica demonstra expressamente que a solução disponibiliza painéis e indicadores específicos para monitoramento do

processamento, encaminhamento e integração dos eventos exportados, incluindo status de conexão, processamento de logs e integração com SIEMs.

A comprovação consta dos seguintes trechos:

**"The Status and Configuration page provides the current connection status between the Skyhigh Cloud Connector and Skyhigh CASB. It also provides the status for Log Processing and Enterprise Integration."**

O fabricante informa expressamente que a solução disponibiliza uma página dedicada ao monitoramento do estado das integrações, do processamento de logs e dos componentes responsáveis pelo envio dos eventos.

Adicionalmente:

**"Cloud Connection – Displays a green dot when Cloud Connector is successfully connected Skyhigh CASB, and a red dot when the cloud connection is not active."**

Esse trecho demonstra monitoramento visual do estado da integração responsável pela transmissão dos dados.

A documentação também estabelece:

**"Log Processing – Displays a green dot when the Log Processor is actively ingesting logs from your egress device and a red dot when Log Processor is not functioning."**

Tal funcionalidade comprova a existência de monitoramento operacional do fluxo de ingestão e processamento dos eventos.

Além disso:

**"Processing Queue: This line displays the next log file that will be processed."**

E:

**"You can use this line to determine if Log Processor is picking up the files you need it to and to track progress as Log Processor works through a backlog."**

Esses recursos permitem acompanhar em tempo real o processamento dos logs e identificar eventuais filas ou atrasos na exportação dos eventos.

Particularmente relevante para o requisito é a funcionalidade:

**"SIEM Integration: Confirms if Enterprise Connector is successfully connected to a third-party SIEM program with a green checkmark."**

Esse trecho demonstra de forma expressa que a solução possui indicador específico para monitoramento da integração com SIEMs.

A documentação também prevê:

**"Last Updated: Enterprise Connector checks the Skyhigh CASB Cloud for configuration updates every five minutes."**

Permitindo verificar a atualização e sincronização das configurações relacionadas ao processamento e encaminhamento dos eventos.

Além disso:

**"Configuration: Displays the current configuration controlling the behavior of Enterprise Connector for log sources, log processing and more."**

Esse recurso demonstra que o painel também permite acompanhar as configurações atualmente aplicadas ao fluxo de eventos.

**Conclusão técnica**

A documentação comprova que a solução:

- Possui painel de Status e Configuração;
- Monitora o estado das integrações;
- Monitora o processamento de logs;
- Monitora filas de processamento;
- Monitora a conectividade com SIEMs;
- Exibe status operacional em tempo real;
- Permite acompanhar a sincronização das configurações;

- Permite verificar a saúde dos componentes responsáveis pela exportação de eventos.

Dessa forma, a solução fornece dashboards e painéis específicos para monitoramento do envio, processamento e integração dos eventos exportados, atendendo integralmente ao requisito previsto no item 1.14.4.

Pelo exposto, a Netsafe atende literalmente ao requisito, razão pela qual a decisão de desclassificação deve ser reformada e a Netsafe classificada.

**1.14.5 A solução deve permitir exportação em tempo real e agendada.**

O Cloud Connector permite a exportação dos logs enquanto o Trellix DLP disponibiliza via API a coleta dos eventos de DLP e outros tipos de logs utilizando um conector ou scripts customizado, a depender da solução para onde está sendo exportada ou um Syslog.

https://success.skyhighsecurity.com/Skyhigh_Cloud_Connector/Cloud_Connector_Integrations/Cloud_Connector_SIEM_Integration/Exporting_Anomalies_and_Threats_to_a_SIEM

O requisito do item 1.14.5 é atendido, pois a documentação técnica demonstra que a solução permite tanto a exportação periódica e agendada de eventos quanto a configuração de intervalos personalizados para envio dos dados aos sistemas externos.

A comprovação consta dos seguintes trechos:

**"You can export anomalies, threats, incidents, and the Audit Log from Skyhigh CASB to your third-party SIEM systems using Syslog export."**

O fabricante informa expressamente que a solução permite exportar eventos de segurança para sistemas externos.

Adicionalmente:

**"By default, Cloud Connector fetches incidents from Skyhigh CASB every four hours."**

Esse trecho demonstra a existência de mecanismo nativo de exportação periódica e automática dos eventos.

A documentação também estabelece:

**"You can customize this interval in the logprocessor.local.properties file using the property siem.frequency=."**

Tal funcionalidade comprova que o intervalo de exportação pode ser configurado pelo administrador conforme a necessidade operacional.

Além disso:

**"The value is in milliseconds."**

Esse trecho demonstra que a periodicidade de exportação pode ser ajustada de forma granular, permitindo intervalos significativamente menores que o padrão.

**Conclusão técnica**

A documentação comprova que a solução:

- Exporta eventos automaticamente;
- Exporta anomalias;
- Exporta ameaças;
- Exporta incidentes;
- Exporta logs de auditoria;
- Possui execução periódica automática;
- Permite configuração do intervalo de exportação;
- Permite ajuste da frequência de envio dos eventos;
- Permite integração contínua com sistemas externos.

Dessa forma, a solução possui mecanismos de exportação agendada e configurável, atendendo ao requisito previsto no item 1.14.5.

A solução possui exportação automática e contínua de eventos para plataformas SIEM, com frequência configurável pelo administrador, inclusive por meio de integrações Syslog e mecanismos Inline de envio de eventos. A exportação periódica é expressamente documentada e sua frequência pode ser ajustada conforme a necessidade operacional do ambiente, atendendo ao requisito de exportação agendada. Ademais, a arquitetura de integração SIEM baseada em Log Collector, Syslog e processamento contínuo de eventos evidencia suporte à exportação em fluxo contínuo para sistemas de monitoramento corporativo.

https://developer.manage.trellix.com/public/mvision/apis/incident

O requisito do item 1.14.5 é atendido, pois a documentação técnica demonstra que a solução disponibiliza mecanismos de exportação automatizada por API, permitindo recuperação contínua de incidentes, consultas periódicas e integração programática com sistemas externos para consumo em tempo real ou sob agendamento.

A comprovação consta dos seguintes trechos:

**"The following API allows for the retrieval of these incidents in bulk."**

O fabricante informa expressamente que a solução disponibiliza API para recuperação automatizada de incidentes em larga escala, possibilitando integração contínua com plataformas externas.

Adicionalmente:

**"with the ability to constrain the results to a specific time period."**

Esse trecho demonstra que a exportação pode ser realizada de forma agendada e incremental, mediante consultas parametrizadas por período.

A documentação também estabelece os endpoints:

**"GET /dpim/v2/incident"**

**"GET /dpim/v2/incident/{incidentId}"**

Tais recursos comprovam que os incidentes podem ser consultados de forma automatizada por sistemas externos, permitindo sincronização contínua ou periódica conforme a necessidade operacional.

Além disso, a documentação disponibiliza infraestrutura dedicada de integração:

"**https://api.manage.trellix.com**"

Demonstrando que a solução fornece interface própria para consumo automatizado dos eventos e incidentes de segurança.

**Conclusão técnica**

A documentação comprova que a solução:

- Disponibiliza APIs para exportação de incidentes;
- Permite recuperação automatizada de eventos;
- Permite integração contínua com sistemas externos;
- Permite consultas periódicas e agendadas;
- Permite filtragem temporal dos dados exportados;
- Permite recuperação incremental de incidentes;
- Disponibiliza endpoints específicos para integração programática.

Dessa forma, a solução possui mecanismos que suportam exportação automatizada de eventos tanto por consultas periódicas quanto por integrações contínuas baseadas em API, atendendo ao requisito previsto no item 1.14.5, devendo a decisão que desclassificou a Netsafe ser reformada e a Netsafe classificada.

**Subitem 4.20.1 do Termo de Referência:**

4.20.1. Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure que a LICITANTE é autorizada e capacitada a comercializar seus produtos e serviços.

**O item requer carta de solidariedade do fabricante.** O TR exige, em caso de fornecedor revendedor ou distribuidor, carta do fabricante assegurando que a licitante é autorizada e capacitada a comercializar seus produtos e serviços.

A Netsafe enviou dois arquivos Carta do Fabricante - SKYHIGH.pdf

O requisito do item 4.20.1 é atendido substancialmente pela documentação apresentada, uma vez que o fabricante reconhece formalmente a Netsafe como parceira autorizada, certificada e apta a comercializar, implementar e suportar os produtos ofertados.

A comprovação consta dos seguintes trechos da carta do fabricante:

**"NetSafe Corp Ltda (...) é um membro do nosso Programa de Parceiros e atualmente tem um nível Advanced até o 31 de dezembro de 2026."**

O fabricante confirma expressamente que a Netsafe integra seu programa oficial de parceiros, em categoria ativa e vigente durante o período do certame.

Adicionalmente:

**"sujeito à relação revendedor/fabricante em curso entre Netsafe Corp Ltda e nós."**

Esse trecho demonstra a existência de vínculo comercial formal e vigente entre fabricante e revendedora.

A carta também estabelece:

**"Confirmamos também que a Netsafe possui as certificações técnicas necessárias para prestar serviços de instalação, suporte e treinamento."**

Tal declaração comprova expressamente a capacitação técnica da licitante para comercialização, implementação e suporte dos produtos ofertados.

**Argumento central**

O item 4.20.1 exige que o fabricante assegure que a licitante:

1. É autorizada a comercializar os produtos;
2. É capacitada a comercializar e prestar os serviços relacionados.

A carta apresentada faz exatamente isso ao declarar que:

- a Netsafe é parceira oficial do fabricante;
- possui nível Advanced no programa de canais;
- mantém relação comercial ativa com o fabricante;
- possui certificações técnicas para instalação, suporte e treinamento.

Tais declarações atendem diretamente à finalidade da exigência editalícia, qual seja comprovar a legitimidade comercial e a capacidade técnica da revendedora.

Carta do Fabricante – Trellix.pdf

O requisito do item 4.20.1 é atendido, pois a carta emitida pela Skyhigh Security comprova expressamente que a Netsafe é parceira autorizada do fabricante, mantém relacionamento comercial vigente e possui capacitação técnica para comercialização, implantação e suporte dos produtos ofertados.

A comprovação consta dos seguintes trechos da carta do fabricante:

**"NetSafe Corp Ltda (...) é um membro do nosso Programa de Parceiros e atualmente tem um nível Advanced até o 31 de dezembro de 2026"**

O fabricante reconhece formalmente a Netsafe como integrante de seu programa oficial de parceiros, em categoria ativa e vigente durante o período do certame.

Adicionalmente:

**"sujeito à relação revendedor/fabricante em curso entre Netsafe Corp Ltda e nós."**

Esse trecho demonstra a existência de vínculo comercial formal e vigente entre fabricante e revendedora autorizada.

A carta também estabelece:

**"Confirmamos também que a Netsafe possui as certificações técnicas necessárias para prestar serviços de instalação, suporte e treinamento."**

Tal declaração comprova expressamente a qualificação técnica da licitante para executar os serviços relacionados aos produtos ofertados.

## Conclusão técnica

A documentação comprova que:

- A Netsafe é parceira oficial do fabricante;
- A Netsafe possui credenciamento ativo no programa de canais;
- Existe relação comercial vigente entre fabricante e revendedora;
- A Netsafe possui certificações técnicas emitidas ou reconhecidas pelo fabricante;
- A Netsafe está apta a prestar instalação, suporte e treinamento;
- A Netsafe está autorizada a comercializar as soluções do fabricante.

Dessa forma, a carta apresentada atende integralmente à finalidade da exigência editalícia, qual seja demonstrar que a licitante é autorizada e capacitada pelo fabricante para comercializar e suportar os produtos ofertados.

## Nulidade de eventual interpretação excessivamente formalista

Ainda que a Administração sustente que a carta não utiliza literalmente a expressão **"carta de solidariedade"**, a documentação apresentada comprova todos os elementos materiais buscados pelo item 4.20.1:

- autorização do fabricante;
- vínculo comercial formal;
- capacitação técnica;
- reconhecimento oficial da condição de parceira.

A interpretação do requisito deve observar o princípio do formalismo moderado, da razoabilidade e da busca da proposta mais vantajosa, sendo vedada a desclassificação baseada exclusivamente na ausência de determinada expressão literal quando a documentação comprova substancialmente a condição exigida.

O fabricante reconheceu formalmente a Netsafe como parceira autorizada, certificada e habilitada para instalação, suporte e treinamento, circunstância que atende à finalidade prática e jurídica da exigência editalícia.

## Da vedação ao formalismo excessivo

Eventual interpretação tendente a desconsiderar a carta apresentada, apesar da inequívoca comprovação da autorização comercial e da capacidade técnica da licitante, configuraria afronta aos princípios da razoabilidade, proporcionalidade, competitividade, busca da proposta mais vantajosa e formalismo moderado consagrados pela Lei nº 14.133/2021.

A jurisprudência do TCU é pacífica no sentido de que a Administração deve privilegiar a análise material da documentação apresentada, especialmente quando o documento comprova substancialmente a condição exigida pelo edital e inexiste qualquer prejuízo à competitividade, à isonomia ou à segurança da contratação.

O procedimento licitatório não pode ser convertido em mecanismo de eliminação de propostas por apego a formalidades

destituídas de relevância material, sobretudo quando o próprio fabricante reconhece formalmente a condição da licitante como parceira autorizada e tecnicamente habilitada para fornecimento da solução.

**Da necessidade de diligência e do tratamento isonômico**

Ainda que, por hipótese, a Administração entendesse existir qualquer necessidade de esclarecimento adicional acerca do conteúdo da declaração emitida pelo fabricante, a medida juridicamente adequada seria a realização de diligência, nos termos da Lei nº 14.133/2021, destinada ao esclarecimento ou complementação da instrução processual.

A diligência, nesse contexto, não implicaria apresentação de documento novo nem modificação da proposta ou das condições de habilitação, mas apenas confirmação de circunstâncias já comprovadas documentalmente pelo próprio fabricante.

Além disso, a observância do princípio da isonomia impõe que a Netsafe receba o mesmo tratamento conferido aos demais licitantes. Caso tenham sido admitidos esclarecimentos, complementações documentais, saneamentos ou diligências em favor da licitante ESYWORLD ou de qualquer outro participante do certame, não pode a Administração adotar critério mais rigoroso exclusivamente em relação à Netsafe.

A adoção de pesos e medidas distintos para situações equivalentes viola os princípios da isonomia, da impessoalidade e da igualdade entre os licitantes, comprometendo a validade do julgamento e impondo a revisão do ato administrativo.

Diante da documentação apresentada, deve ser reconhecido o atendimento ao item 4.20.1 do Termo de Referência.

Subsidiariamente, caso persista qualquer dúvida interpretativa acerca do alcance da declaração emitida pela fabricante, requer-se a realização de diligência para esclarecimento formal da informação, em observância aos princípios da verdade material, do formalismo moderado, da competitividade e da isonomia entre os licitantes.

## 5. Irregularidades na aceitação da ESYWORLD

A aceitação da proposta da ESYWORLD demanda reavaliação pela autoridade competente, pois os autos registram inconsistências documentais relevantes que não foram suficientemente enfrentadas no relatório da sessão nem no ato de classificação da licitante.

Conforme registrado em 01/06/2026, a própria ESYWORLD comunicou a ocorrência de suposto erro material, informando ter anexado matriz PAP diversa daquela que pretendia apresentar, requerendo sua substituição por outra versão. Na mesma manifestação, reconheceu que o cabeçalho da proposta técnica continha dados pertencentes à licitante NCT, circunstância que igualmente motivou pedido de reabertura para substituição dos arquivos e juntada de documentos considerados corretos.

Posteriormente, em 02/06/2026, a Administração consignou expressamente que a ESYWORLD havia apresentado proposta contendo características idênticas às da empresa NCT, já desclassificada no certame. Além disso, identificou divergência objetiva entre a proposta comercial e técnica, que indicava a solução SAFETICA, e a matriz PAP então apresentada, a qual continha composição técnica, part numbers e referências associadas à solução FORCEPOINT.

Diante dessas inconsistências, a Administração passou a exigir da licitante declaração formal contendo fabricante, nome comercial da solução, modelo de licenciamento e respectivos part numbers, bem como nova matriz PAP assinada, contemplando os requisitos técnicos, os códigos dos produtos ofertados e a documentação comprobatória correspondente.

Embora tais fatos, por si sós, não permitam concluir pela existência de fraude, conluio ou má-fé, constituem indícios objetivos de irregularidade documental e de possível alteração substancial dos elementos técnicos que compõem a proposta originalmente submetida ao certame, circunstância que exige exame aprofundado e motivação específica.

Em manifestação datada de 08/06/2026, a ESYWORLD sustentou que a matriz PAP inicialmente apresentada continha informações remanescentes e não relacionadas à solução efetivamente ofertada, afirmando que sua proposta comercial

sempre esteve vinculada à plataforma SAFETICA. Todavia, tal declaração possui natureza unilateral e não afasta a necessidade de verificação objetiva dos documentos efetivamente existentes nos autos antes da realização da diligência.

Nesse contexto, permanecem sem resposta duas questões essenciais para a aferição da regularidade da classificação da licitante.

A primeira consiste em verificar se a ESYWORLD já havia apresentado, dentro do prazo originalmente estabelecido para apresentação da proposta, documentação técnica suficiente, válida e coerente para demonstrar o atendimento dos requisitos por meio da solução SAFETICA.

A segunda consiste em verificar se a denominada “nova matriz PAP” limitou-se a esclarecer informações já constantes dos documentos originalmente apresentados ou se, ao contrário, substituiu documento técnico essencial à comprovação do atendimento das exigências do edital e do Termo de Referência.

Tal distinção é juridicamente relevante porque o art. 64 da Lei nº 14.133/2021 autoriza diligências apenas para complementar informações relativas a documentos já apresentados ou para esclarecer fatos preexistentes à abertura do certame, não constituindo mecanismo apto a permitir a substituição de documentos essenciais, a reformulação da proposta técnica ou a apresentação tardia de elementos indispensáveis à comprovação da habilitação ou da conformidade da solução ofertada.

Caso a nova documentação tenha sido necessária para corrigir a identificação da solução, alterar fabricante, substituir part numbers, redefinir a composição técnica da oferta ou suprir comprovação originalmente inexistente, estar-se-á diante de situação que ultrapassa os limites legais da diligência e configura verdadeira modificação substancial da proposta após sua apresentação, em afronta aos princípios da isonomia, da vinculação ao instrumento convocatório, do julgamento objetivo e da igualdade de tratamento entre os licitantes, previstos nos arts. 5º e 11 da Lei nº 14.133/2021.

A situação torna-se ainda mais sensível diante do fato de que a NETSAFE foi desclassificada por supostas insuficiências documentais e técnicas, circunstância que impõe à Administração o dever de demonstrar, de forma clara e motivada, que o tratamento conferido à ESYWORLD observou os mesmos critérios de rigor aplicados aos demais participantes do certame.

Assim, mostra-se necessária a reavaliação da classificação da ESYWORLD, com análise detalhada dos documentos originalmente apresentados, da extensão das diligências realizadas e dos elementos efetivamente introduzidos após a abertura da fase de julgamento, a fim de verificar se houve mero esclarecimento de informações preexistentes ou verdadeira substituição de documentos e reformulação substancial da proposta originalmente ofertada.

## 6. Limites da diligência

A Lei nº 14.133/2021 e o edital autorizam diligência para **complementar** informações sobre documentos já apresentados e sanar falhas **que não alterem substância e validade jurídica dos documentos** (art. 64 da Lei 14.133)

Contudo, essa orientação não autoriza que licitante substitua matriz técnica essencial, altere produto, modifique part numbers, corrija documentação que indicava solução diversa ou passe a comprovar atendimento técnico apenas após provocação do pregoeiro.

Assim, se a ESYWORLD somente demonstrou atendimento técnico por meio de PAP_Safetica, proposta técnica revisada ou declaração posterior, sem que a comprovação já existisse tempestivamente, sua aceitação viola o edital, o julgamento objetivo e a isonomia.

## 7. Itens não comprovados na planilha ponto a ponto da ESYWORLD

De acordo com a documentação constante no processo, a ESYWORLD **deixou de apresentar** (ou seja, é **inexistente no processo**) a comprovação dos seguintes itens:

1.5 A solução deve suportar OCR para identifi cação de dados confi denciais em imagens ePDFs.

1.9.2 A solução deve permitir auditoria de mensagens instantâneas (Teams, Slack,WhatsApp, etc.).

1.11.2 A solução deve oferecer Shadow Copy para análise de arquivos envolvidos emincidentes de segurança.

1.11.4 A solução deve permitir integração com Azure Information Protection (AIP) e outrasmarcas de proteção de informações como google Cloud.

1.12.4 A solução deve permitir integração com rótulos de classifi cação e criptografi a doAzure Information Protection (AIP)

1.13.4 A solução deve utilizar métodos estatísticos e machine learning para identificar desvios de comportamento.

1.13.5 A solução deve atribuir pontuação de risco (risk score) por usuário/entidade.

1.13.6 A solução deve correlacionar eventos de comportamento com incidentes de segurança (DLP, auditoria, rede).

1.13.11 A solução deve manter histórico de comportamento de usuários por pelo menos 12meses.

1.13.12 A solução deve permitir classificação automática ou manual de criticidade deincidentes (alto, médio, baixo).

1.13.14 A solução deve oferecer mecanismos de redução de falsos positivos (ajuste desensibilidade e validação contextual).

1.14.2 A integração deve utilizar protocolos padrão (Syslog, CEF).

## 8. Pedidos

Diante do exposto, requer a NETSAFE:

1. **O recebimento do presente recurso**, com efeito suspensivo até decisão final, nos termos do art. 168 da Lei nº 14.133/2021, conforme sistematização do TCU sobre a fase recursal.

2. **Preliminarmente a nulidade do ato administrativo que desclassificou a Netsafe por falta de motivo, em vista da falta de disponibilização e juntada do parecer assinado técnico integral da STI** que teria fundamentado a desclassificação da NETSAFE, com todos os anexos, notas técnicas, planilhas e documentos de suporte.

3. **A reforma da decisão que desclassificou a NETSAFE**, reconhecendo-se o atendimento aos subitens 1.1, 1.9.2, 1.9.3, 1.11.2, 1.11.3, 1.12.1, 1.13.4, 1.13.11, 1.13.17, 1.14.1, 1.14.2, 1.14.3, 1.14.4 e 1.14.5 do Caderno de Especificações Técnicas, bem como ao item 4.20.1 do Termo de Referência, caso comprovada a apresentação da carta do fabricante.

4. **A classificação da proposta da NETSAFE**, com o regular prosseguimento do certame a partir de sua proposta, por ser tecnicamente aderente e economicamente mais vantajosa.

5. **A anulação ou revisão da aceitação da proposta da ESYWORLD**, por afronta ao artigo 64 da Lei 14.133, diante dos indícios relevantes de inconsistência documental, divergência entre solução SAFETICA e referências/part numbers FORCEPOINT, possível documentação idêntica/equivalente à NCT e possível substituição de matriz técnica essencial, **o que é alteração substancial da proposta, não erro material.**

6. **A desclassificação da ESYWORLD**, caso se confirme que a conformidade técnica da solução foi demonstrada apenas por documentos substitutivos ou complementares apresentados após a fase própria, especialmente nova matriz PAP, PAP_Safetica, proposta técnica revisada ou declaração técnica que tenha suprido requisito essencial não comprovado tempestivamente.

7. **A desclassificação da ESYWORLD**, pois não se encontra em nenhum documento no processo indicações e comprovações dos itens técnicosb 1.5, 1.9.2, 1.11.2, 1.11.4, 1.12.4, 1.13.4, 1.13.5, 1.13.6, 1.13.11, 1.13.12, 1.13.14, 1.14.2.

8. **A apuração formal da identidade documental ou equivalência de conteúdo entre ESYWORLD e NCT**, sem prejulgamento de fraude, conluio ou má-fé, assegurado o contraditório, mas com decisão motivada sobre a independência das propostas.

Termos em que,

Pede deferimento.

Brasília, 12 de junho de 2026

WALDO BAPTISTA GOMES:09182971846

Assinado de forma digital por WALDO BAPTISTA GOMES:09182971846
Dados: 2026.06.12 18:01:28 -03'00'

**NETSAFE CORP LTDA**

CNPJ nº 03.476.184/0002-30