Simplicidade para o dia-a-dia das Empresas

Nossa tecnologia facilita os desafios do SPED para as áreas fiscal, contábil e trabalhista-previdenciária.

KOLOSSUS

CERTIFICAÇÕES DE SEGURANÇA

ASIS Desafios Solucionados!

Google Cloud: Conformidade e Proteção dos Dados

As soluções ASIS utilizam a Google Cloud Plataform como Provedor dos Serviços de Cloud, portanto todos os Relatórios de Segurança, Auditoria e Certificados, foram replicados para nossos Produtos.

O modelo de segurança, a infraestrutura em escala global e a capacidade de inovação inigualável do Google Cloud mantem a ASIS segura e dentro dos padrões de conformidade. Como parte do nosso compromisso com a transparência e a privacidade, fornecemos uma visualização de pessoa com informações privilegiadas das práticas de conformidade, risco e segurança do Google Cloud.

Google Cloud: Conformidade e Proteção dos Dados

Criptografia em repouso

Criptografia em repouso se refere à criptografia de dados armazenados em um disco ou backup. O Google Cloud é o primeiro grande provedor de nuvem a oferecer criptografia em repouso por padrão, usando uma abordagem multicamadas que inclui criptografia no nível do dispositivo ou do sistema de armazenamento.

Por que isso é importante

A criptografia em repouso protege os dados de serem divulgados para indivíduos e sistemas sem autorização quando forem armazenados em uma nuvem pública. Muitos provedores de nuvem têm criptografia no nível do dispositivo de armazenamento, o que protege os dados em casos de comprometimento físico. Indo além, o Google Cloud também oferece criptografia no nível do sistema de armazenamento. Isso permite que o Google Cloud desempenhe tarefas operacionais, como fazer o backup de dados sem que as equipes de suporte ou os engenheiros do Google Cloud tenham acesso ao conteúdo.

Google Cloud: Conformidade e Proteção dos Dados

Como o Google Cloud realiza a implementação

O Google usa diversas camadas de criptografia para proteger os dados em repouso do cliente nos produtos do Google Cloud.

Os dados para armazenamento são divididos em blocos, e cada um deles é criptografado com uma chave de criptografia de dados exclusiva. Essas chaves de criptografia de dados são armazenadas com os dados e criptografadas (encapsuladas) por meio de chaves de criptografia de chaves, que são armazenadas e utilizadas exclusivamente dentro do serviço de gerenciamento de chaves central do Google. O serviço de gerenciamento de chaves do Google é redundante e distribuído no mundo inteiro. Os dados armazenados no Google Cloud são criptografados no nível de armazenamento usando AES256 ou AES128.

O Google usa a Tink, uma biblioteca criptográfica comum, para implementar a criptografia de maneira consistente em quase todos os produtos do Google Cloud. Como essa biblioteca comum é amplamente acessível, basta apenas uma pequena equipe de criptógrafos para implementar e manter adequadamente esse código rigorosamente controlado e revisado.

Google Cloud: Conformidade e Proteção dos Dados

Acesso privilegiado

O gerenciamento adequado do acesso privilegiado em uma organização ajuda a evitar a divulgação acidental de dados confidenciais e a reduzir o risco de um usuário não autorizado acessar esses dados.

Por que isso é importante

Ao armazenar dados em uma nuvem pública, é importante não só implementar um gerenciamento de acesso adequado para a equipe, como também entender como o provedor de nuvem garante que esses dados serão acessados pelos funcionários somente para fins comerciais legítimos. O provedor de nuvem deve acessar esses dados apenas para seguir instruções do cliente, garantir a operação do serviço ou obedecer às obrigações legais.

Como o Google Cloud realiza a implementação

Além da criptografia, o Google Cloud usa uma combinação de identidades fortes para contas de serviço e individuais, sistemas ACL e um controle interno semelhante à autorização binária para garantir que o acesso aos dados do cliente seja válido. Em relação ao acesso a dados armazenados nos serviços integrados à transparência no acesso, controles técnicos adicionais estão à disposição para assegurar que um registro de justificativa comercial seja gerado para cada acesso. Esses acessos são monitorados e auditados regularmente.

Google Cloud: Conformidade e Proteção dos Dados

Integridade da implantação

A integridade da implantação se refere à capacidade do Google Cloud de garantir que as configurações e os códigos implantados no ambiente de produção que interagirem com os dados de clientes serão devidamente revisados e autorizados. Autorização binária para Borg, ou BinAuthz, é uma verificação interna de aplicação no momento da implantação que avalia se as configurações e o software de produção implantados no Google Cloud estão devidamente revisados e autorizados, especialmente se o código puder acessar dados do usuário.

Por que isso é importante

A BinAuthz garante que as implantações de código e de configuração atendam a determinados padrões mínimos. Ela também pode ser usada em um modo de auditoria não obrigatório para avisar quando determinados requisitos não forem atendidos. Com a BinAuthz, o Google Cloud reduz o risco de pessoas com informações privilegiadas, evita possíveis ataques e dá suporte à uniformidade dos próprios sistemas de produção. O gerenciamento de acesso privilegiado se concentra em garantir que todos os acessos aos dados por indivíduos sejam autorizados. Já a integridade da implantação garante que o acesso programático aos dados seja autorizado. Essa verificação assegura que todo acesso programático aos dados do cliente, bem como as mudanças no ambiente de produção, gerem uma trilha de auditoria.

Google Cloud: Conformidade e Proteção dos Dados

Como o Google Cloud realiza a implementação

Nossa infraestrutura é projetada para sistemas altamente escalonáveis usando um sistema de gerenciamento de clusters chamado Borg (em inglês). Executamos centenas de milhares de jobs de vários aplicativos diferentes e em vários clusters, cada um com até dezenas de milhares de máquinas. Como resultado, nosso ambiente de produção é razoavelmente homogêneo, permitindo que os pontos de contato para acessar dados do usuário sejam controlados e auditados com mais facilidade. A BinAuthz oferece um serviço de aplicação no momento da implantação para evitar a inicialização de jobs não autorizados, bem como de trilhas de auditoria da configuração e do código usados em jobs com a BinAuthz ativada.

Google Cloud: Conformidade e Proteção dos Dados

Ofertas de conformidade

Migrar para a nuvem significa proteger cargas de trabalho confidenciais e, ao mesmo tempo, alcançar e manter a conformidade com diretrizes, frameworks e requisitos de regulamentação complexos. Regiões e setores diferentes têm requisitos variados. Esses requisitos podem ser autorizados por uma autoridade reguladora ou podem ser criados por organizações com padrões confiáveis, entre outras opções. O Google Cloud oferece suporte aos clientes no mundo inteiro, em vários setores, e entende a importância de atender às necessidades de conformidade para garantir que os clientes continuem com suas práticas comerciais. O Google Cloud é submetido, regularmente, a verificações independentes de controles de conformidade, privacidade e segurança, e tem certificações, atestados de conformidade e relatórios de auditoria de acordo com os padrões estabelecidos ao redor do mundo. Também criamos documentações e mapeamentos de recursos referentes aos frameworks e às legislações em países onde certificações ou atestados formais não são exigidos ou aplicados.

Por que isso é importante

Entendemos que você precisa de verificações independentes de controles de conformidade, privacidade e segurança dos nossos produtos. Por isso, nossas certificações, atestados de conformidade e relatórios de auditoria de acordo com padrões globais inspiram confiança. Isso significa que um auditor independente examinou os controles disponíveis nos data centers, na infraestrutura e nas operações. Essas certificações incluem os padrões de segurança independentes mais amplamente reconhecidos e aceitos internacionalmente, como a norma ISO/IEC 27001 para controles de segurança e a norma ISO/IEC 27017 para segurança na nuvem, além da SOC 1, 2 e 3 do AICPA. Essas certificações nos ajudam a atender às demandas dos padrões do setor, como CSA STAR e PCI-DSS, além de muitos outros padrões regionais. Continuamos a expandir nossa lista de ofertas de conformidade globalmente para ajudar nossos clientes a atender às obrigações de conformidade.

Google Cloud: Conformidade e Proteção dos Dados

Como o Google Cloud realiza a implementação

Nossos serviços são submetidos regularmente a verificações independentes de controles de segurança, privacidade e conformidade, e têm certificações, atestados de conformidade e relatórios de auditoria de acordo com padrões do mundo todo. A cada ano avaliamos os serviços que se aproximam da disponibilidade geral (GA, na sigla em inglês) para incluí-los no escopo dos nossos grandes ciclos de auditoria.

Além dos pontos citados, os principais recursos incluem os mais recentes Certificados ISO / IEC, Relatórios SOC e Autoavaliações.

A seguir apresentamos o resumo de cada um dos Certificados mencionados.

CSA STAR

A Cloud Security Alliance é uma organização sem fins lucrativos. A missão da empresa é “promover o uso de práticas recomendadas para fornecer garantias de segurança na computação em nuvem. Além disso, queremos ensinar aos usuários sobre as funcionalidades da computação em nuvem para proteger todas as outras formas de computação”.

O programa Registro de segurança, confiança e garantia (CSA STAR, na sigla em inglês) foi desenvolvido para ajudar os clientes a avaliarem e escolherem um provedor de serviços de nuvem por meio de três etapas: autoavaliação, auditoria por terceiros e monitoramento contínuo.

O Google Cloud conquistou a certificação baseada na avaliação de terceiros (CSA STAR nível 2: credenciamento) sobre os produtos Google Cloud Platform (GCP) e G Suite. Por isso, um relatório CSA STAR SOC2+ foi emitido.

O Google também patrocina a CSA, que faz parte do International Standardization Council (ISC), e é uma das empresas fundadoras do GDPR Center of Excellence da CSA.

ISO/IEC 27001

A Organização Internacional de Normalização (ISO, na sigla em inglês) é uma entidade internacional, não governamental e independente que tem a associação de 163 órgãos de normalização nacionais. A família de normas ISO/IEC 27000 (em inglês) ajuda as organizações a proteger os próprios dados.

A norma ISO/IEC 27001 descreve e informa os requisitos de um Sistema de Gestão de Segurança da Informação (SGSI), especifica um conjunto de práticas recomendadas e mostra detalhes sobre os controles de segurança que podem ajudar a gerenciar os riscos relacionados às informações.

O Google Cloud Platform, nossa infraestrutura compartilhada, o G Suite, o Chrome e a Apigee (links em inglês) têm um certificado de *compliance* com a ISO/IEC 27001. Embora essa norma não exija controles de segurança da informação específicos, o sistema e a lista de verificação dos controles definidos pela norma permitem que o Google garanta um modelo abrangente e em constante aprimoramento para o gerenciamento da segurança.

ISO/IEC 27017

A Organização Internacional de Normalização (ISO, na sigla em inglês) é uma entidade não governamental e independente com a associação de 163 órgãos de normalização nacionais.

A norma ISO/IEC 27017:2015 (em inglês) define diretrizes para os controles de segurança da informação aplicáveis ao provisionamento e uso de serviços de nuvem por meio de:

- orientações adicionais relacionadas à implementação dos controles pertinentes especificados na norma ISO/IEC 27002 nuvem, como o Google, e para os clientes dessas emp (em inglês);
- controles adicionais com diretrizes de implementação relacionadas especificamente a serviços de nuvem.

Essa norma fornece controles e orientações de implementação para provedores de serviços de resas.

A norma ISO/IEC 27017 proporciona diretrizes referentes à nuvem para 37 controles descritos na norma ISO/IEC 27002, além de sete novos controles relacionados aos serviços de nuvem que abordam:

ISO/IEC 27017

- quem é responsável por qual ação entre o provedor de serviços de nuvem e o cliente;
- a remoção/devolução de recursos quando um contrato é rescindido;
- a proteção e separação do ambiente virtual do cliente;
- a configuração da máquina virtual;
- os procedimentos e as operações administrativas associados ao ambiente de nuvem;
- o monitoramento das atividades do cliente realizadas na nuvem;
- o alinhamento dos ambientes virtual e de rede de nuvem.

O Google Cloud Platform, o G Suite, o Chrome, e a Apigee (links em inglês) têm um certificado de compliance com a norma ISO/IEC 27017.

ISO/IEC 27018

A Organização Internacional de Normalização (ISO, na sigla em inglês) é uma entidade internacional, não governamental e independente com a associação de 163 órgãos de normalização nacionais.

A ISO/IEC 27018 (em inglês) se refere a um dos elementos mais importantes da privacidade na nuvem: a proteção de informações de identificação pessoal (PII). Essa norma se concentra em duas formas de controles de segurança para os provedores de serviços de nuvem pública que processam PII:

Usa como base os controles existentes da ISO/IEC 27002 para se desenvolver ao adicionar itens específicos à privacidade na nuvem.

Fornece controles de segurança totalmente novos para dados pessoais.

O Google Cloud Platform, o G Suite, o Chrome e a Apigee (links em inglês) têm um certificado de compliance com a norma ISO/IEC 27018.

PCI DSS

O Conselho de Normas de Segurança da Indústria de Cartões de Pagamento (PCI, na sigla em inglês) é um fórum global para o desenvolvimento, o aprimoramento, o armazenamento, a divulgação e a implementação de padrões de segurança para a proteção de dados financeiros. Criado pelas maiores empresas de cartão de crédito (Visa, MasterCard, American Express, Discover, JCB) como uma organização independente, o conselho tem como finalidade definir práticas adequadas a comerciantes e provedores de serviços para a proteção dos dados de pagamento dos titulares de cartões. Com isso, foi criada a Norma de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS, na sigla em inglês).

A PCI DSS é um conjunto de diretrizes de práticas recomendadas empresariais e de segurança de rede adotadas pelo Conselho de Normas de Segurança do PCI. O intuito é estabelecer um padrão mínimo de segurança para proteger as informações dos cartões dos clientes. O escopo da PCI DSS inclui todos os sistemas, redes e aplicativos que processam, armazenam ou transmitem dados dos titulares de cartões, além de sistemas usados para proteger e registrar o acesso aos sistemas dentro do escopo.

O Google Cloud é submetido a uma auditoria anual conduzida por terceiros para certificar produtos individuais de acordo com a PCI DSS. Isso significa que esses serviços oferecem uma infraestrutura em que os clientes podem criar o próprio serviço ou aplicativo com capacidade para armazenar, processar ou transmitir dados de titulares de cartões.

PCI DSS

É importante observar que os clientes ainda são responsáveis por garantir que os respectivos aplicativos estejam em conformidade com a PCI DSS. Para saber como usar o Google Cloud Platform a fim de implementar a PCI DSS no seu aplicativo, veja o artigo Como criar um ambiente compatível com a PCI-DSS.

Os serviços do Google Cloud a seguir foram analisados por um avaliador de segurança qualificado independente e estão em conformidade com a PCI DSS 3.2.1. Isso significa que esses serviços oferecem uma infraestrutura em que os clientes podem criar os próprios serviços ou aplicativos com capacidade para armazenar, processar ou transmitir dados de titulares de cartões de pagamentos. Criamos esta matriz para esclarecer melhor a responsabilidade compartilhada entre o Google e os clientes.

SOC 1

Controles sobre relatórios financeiros.

Um relatório SOC 1 documenta os controles de uma organização de serviços que podem ser relevantes para os relatórios financeiros. O Google Cloud Platform é submetido a uma auditoria regular conduzida por terceiros para certificar produtos individuais de acordo com esse padrão.

SSAE 16/ISAE 3402 Tipo II

O Comitê de Padrões de Auditoria do Instituto Americano de Contadores Públicos Certificados (AICPA, na sigla em inglês) criou a Declaração sobre Padrões para Compromissos de Atestado (SSAE 16, na sigla em inglês) nº 16 para acompanhar os padrões de contabilidade internacionais reconhecidos mundialmente.

O SSAE 16 está rigorosamente alinhado com a International Standard on Assurance Engagements 3402 (ISAE 3402).

O SSAE 16 e o ISAE 3402 são usados para gerar um relatório por um terceiro objetivo que atesta um conjunto de afirmações que uma organização confirma sobre seus controles. A estrutura do Service Organization Controls (SOC) é o método pelo qual o controle de informações financeiras é medido.

SOC 2

Controles sobre segurança, disponibilidade e confidencialidade.

O SOC 2 é um relatório baseado nos princípios e critérios do Trust Services existentes do AICPA. O objetivo do relatório do SOC 2 é avaliar os sistemas de informação de uma organização relevantes para segurança, disponibilidade, integridade de processamento e confidencialidade ou privacidade. O Google Cloud é submetido a uma auditoria regular conduzida por terceiros para certificar produtos individuais de acordo com esse padrão.

SSAE 16/ISAE 3402 Tipo II

O Comitê de Padrões de Auditoria do Instituto Americano de Contadores Públicos Certificados (AICPA, na sigla em inglês) criou a Declaração sobre padrões para compromissos de atestado nº 16 (SSAE, na sigla em inglês) para acompanhar os padrões de contabilidade internacionais reconhecidos mundialmente.

O SSAE 16 está rigorosamente alinhado com a International Standard on Assurance Engagements 3402 (ISAE 3402). Ambos são usados para gerar um relatório por um terceiro objetivo que atesta um conjunto de afirmações que uma organização confirma sobre seus controles. A estrutura do Service Organization Controls (SOC) é o método pelo qual o controle de informações financeiras é medido.

SOC 3

Relatório público de controles sobre segurança, disponibilidade e confidencialidade.

O SOC 3 é baseado nos princípios existentes do SysTrust e do WebTrust. Ao contrário do SOC 1 e do 2, os relatórios do SOC 3 referentes ao Google Cloud Platform e ao G Suite podem ser distribuídos publicamente para uso geral. O Google Cloud é submetido a uma auditoria regular conduzida por terceiros para certificar produtos individuais de acordo com esse padrão.

SSAE 16/ISAE 3402 Tipo II

O Comitê de Padrões de Auditoria do Instituto Americano de Contadores Públicos Certificados (AICPA, na sigla em inglês) criou a Declaração sobre padrões para compromissos de atestado nº 16 (SSAE 16, na sigla em inglês) para acompanhar os padrões de contabilidade internacionais reconhecidos mundialmente.

O SSAE 16 está rigorosamente alinhado com a International Standard on Assurance Engagements 3402 (ISAE 3402).

O SSAE 16 e o ISAE 3402 são usados para gerar um relatório por um terceiro objetivo que atesta um conjunto de afirmações que uma organização confirma sobre seus controles. A estrutura do Service Organization Controls (SOC) é o método pelo qual o controle de informações financeiras é medido.

Security

Comercial São Paulo/SP
Rua Gomes de Carvalho, 1356 - 2º andar
Vila Olímpia

Comercial Belo Horizonte/MG
Av. Francisco Sales, 1614 - sala 505
Funcionários

Laboratório de Inovação Barueri/SP
Al. Rio Negro, 503 - sala 1311
Alphaville

Administrativo São Paulo/SP
R. Padre João Manuel, 222 - sala 132
Jardins

ASIS
Desafios Solucionados!