SUMÁRIO

1. INTRODUÇÃO

A presente Política de Segurança da Informação para Parceiros tem como objetivo principal direcionar um programa efetivo de proteção dos ativos de informação, com vistas a assegurar a confidencialidade, a integridade e a disponibilidade das informações, sendo a base para o estabelecimento dos padrões e procedimentos de Segurança da Informação no Grupo WEG.

2. ABRANGÊNCIA

Todos os Parceiros (qualquer pessoa que possua relação jurídica com o Grupo WEG na qualidade de fornecedor de produtos, licenças ou serviços) devem cumprir os requisitos de Segurança da Informação aqui definidos.
O cumprimento das diretrizes estabelecidas é fundamental para a efetiva relação de parceria firmada e o atingimento de níveis adequados de proteção à informação.
As diretrizes e os requisitos aqui estabelecidos se aplicam a todos os Parceiros que tenham acesso aos dados, informações e sistemas do Grupo WEG. Os Parceiros serão responsáveis por si e por seus colaboradores, fornecedores e prestadores de serviços.

3. DEFINIÇÕES

- **DPIA:** é a sigla em inglês para Data Protection Impact Assessment, que significa Relatório de Impacto à Proteção de Dados Pessoais (RIPD) na Lei Geral de Proteção de Dados (LGPD) brasileira. Este processo que identifica, avalia e reduz os riscos de privacidade em projetos de dados antes de serem implementados. É uma responsabilidade legal e obrigatória quando o tratamento de dados pode colocar em risco os direitos e liberdades dos titulares de dados.
- **Opt-in:** é um termo em inglês que significa a autorização de um usuário para receber informações de uma empresa.
- **Opt-out:** é um termo que significa "optar por sair", é um movimento em que o indivíduo tem a autonomia de deixar de fazer parte de algo que está inserido.
- **Segregação de Funções (SOD):** SOD é a sigla para *Segregation of Duties*, é um princípio de controle interno que visa evitar riscos, como fraudes, erros e ataques cibernéticos, em organizações. A Segregação de Funções é baseada na delegação de tarefas entre diferentes pessoas ou grupos, de forma a evitar que uma mesma pessoa tenha controle total sobre sistemas, processos ou atividades confidenciais.
- **Política de privilégio mínimo:** é um conceito de segurança cibernética que consiste em dar aos usuários apenas o mínimo de privilégios necessários para desempenhar suas funções.
- **Runbooks:** guias detalhados que descrevem os procedimentos e processos de uma organização, com o objetivo de garantir que as atividades sejam executadas de forma consistente, segura e eficiente.
- **Hardening:** processo que visa fortalecer a segurança de sistemas, redes, softwares, hardwares, firmwares e infraestruturas de TI, tornando-os mais resistentes a ciberataques.
- **Patches de segurança:** atualizações corretivas que visam corrigir vulnerabilidades, falhas e bugs em softwares e plataformas. A palavra "patch" é um termo inglês que significa "correção" ou "remendo".

- **OWASP:** Open Worldwide Application Security Project(OWASP) é uma organização internacional sem fins lucrativos que trabalha para melhorar a segurança de aplicativos web e móveis. O OWASP é uma das principais iniciativas de combate a crimes cibernéticos.
- **Privacy and Security by Design:** conceitos que se referem à proteção de dados e segurança de sistemas de forma proativa, desde a concepção de um projeto ou serviço.
- **Phishing:** tipo de ciberataque que tem como objetivo roubar informações pessoais ou acessar contas online. Os golpistas usam mensagens fraudulentas que parecem legítimas para enganar as vítimas e fazer com que revelem dados confidenciais.
- **Ethical hacking:** Ethical hacking ou hacking ético, é uma prática de segurança digital que consiste em simular um ataque cibernético para identificar e corrigir vulnerabilidades em sistemas, redes ou aplicativos.
- **Teste de intrusão:** teste de intrusão (ou pentest) é um ataque simulado autorizado que as organizações fazem nos próprios sistemas ou redes de computadores para avaliar sua segurança. O objetivo é descobrir vulnerabilidades usando as mesmas ferramentas, técnicas e processos que os hackers usam. Ao expor os pontos fracos da segurança cibernética, os pentests ajudam a reduzir os riscos de ataques cibernéticos maliciosos.

4. RESPONSABILIDADES

4.1. Área contratante de serviços de fornecedores

- Durante o processo de contratação de Parceiros (inclusos aqui os colaboradores, os fornecedores e os prestadores de serviços vinculados ao Parceiro) que necessitem acessar a rede interna, os sistemas, as informações ou os dados do Grupo WEG, a área contratante deverá assegurar que todos os envolvidos estejam cientes dessa política de segurança da informação.
- A área contratante deve assegurar que os contratos com Parceiros incluam cláusulas específicas sobre segurança da informação e proteção de dados, inclusive com referência expressa à presente Política de Segurança da Informação.

4.2. Parceiros

- É de responsabilidade dos Parceiros observar e seguir as orientações estabelecidas na presente Política de Segurança da Informação; e
- As atividades executadas devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras com relação à Segurança da Informação aplicáveis ao objeto do contrato.

5. DIRETRIZES

5.1. Geral

Os Parceiros, sejam eles fornecedores de produtos, licenças ou serviços, devem comprometer-se a seguir integralmente os itens a seguir:

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade;

- Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Grupo WEG;
- Assegurar que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos de acordo com os padrões do Grupo WEG;
- Assegurar a continuidade do processamento das informações críticas de negócios;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Implementar e manter controles de segurança da informação, conforme as melhores práticas de mercado e regulamentações aplicáveis;
- Comunicar imediatamente ao Grupo WEG qualquer descumprimento da Política de Segurança da Informação para Parceiros, por si ou por outras pessoas, sejam elas vinculadas ou não ao Parceiro.
- Cumprir as Condições Gerais para Compra de Bens, Materiais e/ou Serviços do Grupo WEG (“CGC”) – disponível em: https://www.weg.net/ -> Isto é WEG -> Condições GERAIS DE COMPRAS PARA FORNECEDORES – e o Código de Ética para Fornecedores do Grupo WEG (“Código de Ética”) – disponível em: https://www.weg.net/ -> Isto é WEG -> CÓDIGO DE ÉTICA PARA FORNECEDORES. O Parceiro deverá cumprir rigorosamente os parâmetros a si aplicáveis sobre proteção e privacidade de dados estabelecidos em qualquer legislação aplicável, bem como seguir as melhores práticas de mercado sobre o tema.
- Parceiros que realizem atividades críticas em favor do Grupo WEG, devem passar por processo de avaliação de Segurança da Informação (“SI”). No processo de avaliação em SI será realizado um Self Assessment de SI durante as fases de qualificação de fornecedores e negociação do contrato. A depender do resultado do Self Assessment, o Grupo WEG poderá requisitar procedimentos adicionais para averiguação da adequação do Parceiro aos parâmetros de SI estabelecidos nesta Política de Segurança da Informação para Parceiros.

6. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

6.1. CONDUTA DE PARCEIROS NO AMBIENTE DO GRUPO WEG

6.1.1. Acesso lógico e uso aceitável

- Para Parceiros que precisem acessar o ambiente do Grupo WEG remotamente, o gestor WEG responsável pelo contrato deve providenciar acesso através de usuário único e individual, no qual somente poderá ter acesso aos recursos de trabalho e ambientes necessários para o desempenho de suas funções;
- Os computadores de Parceiros não podem ser conectados na rede interna do Grupo WEG sem a aprovação prévia da área responsável pela segurança da informação, os softwares dos equipamentos de Parceiros devem obrigatoriamente estarem devidamente licenciados;
- É proibido o acesso, download ou distribuição de qualquer conteúdo que viole direitos autorais ou de propriedade do Grupo WEG. Da mesma forma, não é permitido acesso ou distribuição de conteúdo ilegal, pornográfico de qualquer natureza ou que viole o Estatuto da Criança e Adolescente;
- As credenciais de acesso disponibilizados para o parceiro são de uso exclusivo e não podem ser divulgados ou compartilhados com outras pessoas;

- O parceiro deve manter suas credenciais de acesso seguras, sendo de sua inteira e exclusiva responsabilidade qualquer utilização realizada com suas credenciais de acesso, inclusive o eventual uso indevido;
- É responsabilidade do Parceiro comunicar qualquer desligamento de seus colaboradores, fornecedores ou prestadores de serviços.

6.1.2. Notificação de incidentes de segurança da informação

O Parceiro deve, quando descobrir um incidente ou suspeitar razoavelmente que um incidente está ocorrendo ou ocorreu:

- Iniciar imediatamente o tratamento de incidentes para investigar, conter prontamente e proteger quaisquer sistemas de TI e dados da empresa em risco, minimizar e mitigar o impacto do incidente nos sistemas de TI;
- Notificar imediatamente o Grupo WEG por meio do e-mail soc@weg.net.

O Parceiro deve notificar o incidente incluindo as seguintes informações:

- A natureza e o escopo suspeito do incidente;
- A data suspeita em que o incidente começou;
- A data e hora da descoberta do incidente;
- Ações tomadas pelo Parceiro para assegurar o fornecimento contínuo do escopo e para proteger e recuperar os dados da empresa, quando relevante; e
- Detalhes de contato de um representante do Parceiro para responder às solicitações do Grupo WEG para tais informações.

O Parceiro deve fornecer ao Grupo WEG as seguintes informações o mais rápido possível:

- A(s) causa(s) suspeita(s) do incidente e do(s) ator(es) envolvido(s);
- O impacto estimado do incidente;
- Ações corretivas propostas e tempo estimado para recuperação total do impacto do incidente; e
- Ações corretivas propostas, inclusive para garantir o fornecimento contínuo do escopo e para proteger e recuperar os dados da empresa, quando relevante.

O Parceiro deverá fornecer ao Grupo WEG atualizações regulares das informações fornecidas nos termos dos parágrafos anteriores, juntamente com quaisquer outras informações que o Grupo WEG possa razoavelmente solicitar em conexão com o incidente (incluindo registros de todo o acesso aos sistemas de TI relevantes em conexão com o incidente e evidências para demonstrar a proteção e recuperação efetivas dos dados da empresa).

O Parceiro deve fornecer imediatamente ao Grupo WEG toda a assistência que o Grupo WEG possa precisar para permitir que ele investigue, responda, mitigue o impacto e corrija os incidentes (incluindo a proteção e recuperação de dados da empresa) e se comunique e responda a indivíduos ou autoridades públicas, incluindo as autoridades reguladoras relevantes.

O Parceiro deve fornecer ao Grupo WEG um relatório final do incidente, incluindo uma análise de causa raiz, assim que estiver disponível.

Não obstante qualquer disposição em contrário no contrato, um incidente não será considerado um evento de força maior na medida em que tenha sido contribuído por qualquer violação deste anexo ou negligência de um membro do Parceiro.

6.1.3. Segurança de equipamentos

- Cada Parceiro é responsável pela proteção dos dispositivos físicos contendo informação do Grupo WEG que estão sob sua guarda; e
- Os Parceiros estão cientes de que o acesso a qualquer ambiente do Grupo WEG ou o uso de qualquer recurso de TI no ambiente do Grupo WEG, mesmo nas situações em que o parceiro utilizar um equipamento de propriedade pessoal, estão sujeitos ao monitoramento e à vistoria, excetuadas as situações em que a lei local aplicável expressamente vetar tal conduta.

6.1.4. Violação de conduta

São consideradas violações à esta Política de Segurança da Informação para Parceiros as seguintes situações, não se limitando a:

- Quaisquer ações, omissões ou demais situações que possam expor o Grupo WEG à perda financeira ou de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- Uso indevido ou divulgação de qualquer informação sem a permissão expressa do Grupo WEG, tais como: dados corporativos, segredos comerciais ou outras informações;
- O descumprimento comissivo ou omissivo de qualquer orientação, regra, parâmetro ou obrigação estabelecidos na presente Política de Segurança da Informação para Parceiros;
- Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do Grupo WEG; e
- A não-comunicação imediata ao Grupo WEG de quaisquer incidentes de Segurança da Informação ou descumprimentos da presente Política de Segurança da Informação para Parceiros.

6.2. CONTROLES DE SEGURANÇA E PRIVACIDADE NO AMBIENTE DO PARCEIRO

Ao ser requisitado pela área de negócio do Grupo WEG, o Parceiro em questão será cadastrado pelo time de Governança em Segurança da Informação em uma ferramenta de verificação de sua cyber-saúde. Essa plataforma provê score de pontuação.

O score geral do Parceiro deverá atingir no mínimo 80% ou a média de score do seu segmento de mercado fornecido pela própria ferramenta, o que for maior.

Os Parceiros que não atingirem o score desejado receberão do Grupo WEG um relatório de adequação e compliance a fim de que o Parceiro tome medidas para atingir o score desejado em até 180 dias.

Além do procedimento de cadastro acima descrito, o Parceiro deverá seguir as seguintes diretrizes de segurança da informação, dispostas também no documento de Self Assessment enviado e mantido pela área de Segurança da Informação.

6.2.1. Privacidade

- Apresentar por meio de documentação o fluxo dos dados da WEG no ambiente do Parceiro, contendo todo o seu ciclo de vida (coleta, processamento, armazenamento, compartilhamento e exclusão).

- Informar ao Grupo WEG quais informações são coletadas, para qual finalidade, qual a base legal que embasa o tratamento do dado, onde são armazenadas e por quanto tempo, sempre buscando minimizar o período de armazenamento e a quantidade de informação coletada.
- Possuir uma avaliação de impacto relacionada aos dados pessoais de um titular (DPIA), assim como possuir um processo que conceda acesso irrestrito ao Grupo WEG às suas informações processadas e armazenadas, previstas no escopo do contrato.
- Possuir um processo de *opt-in* e de *opt-out* para expressão prévia e livre do Grupo WEG e dos titulares de dados pessoais acerca do compartilhamento por meio de uma parceria. Destaca-se, ainda, que o padrão deve ser o não compartilhamento. Somente após o *opt-in* do interessado o Parceiro poderá compartilhar dados com parceiros.

6.2.2. Controle de acesso

- Possuir um processo de Gerenciamento de Acessos devidamente documentado;
- Dar acesso irrestrito ao Grupo WEG sobre os dados e informações armazenados ou a serem processados, conforme os serviços específicos definidos, prezando pela confidencialidade, integridade, disponibilidade e pela capacidade de recuperação destes dados e informações;
- Dar visibilidade ao Grupo WEG dos procedimentos e controles utilizados para cumprimento do contrato, como descrito no item acima, em especial, para a identificação e a segregação dos dados de clientes do Grupo WEG, por meio de controles físicos ou lógicos;
- Não permitir o uso de contas compartilhadas ou usuários genéricos para sistemas críticos, bem como manter controles relacionados a login, a exemplo de (sem se limitar a): forçar alteração no primeiro acesso, bloquear o usuário após um número de determinadas tentativas inválidas, exigir padrão de senha complexa e demais práticas de segurança da informação conforme os melhores padrões de mercado;
- Possuir um processo formalizado e documentado de concessão, alteração e revogação de acessos, principalmente àqueles com ações privilegiadas;
- Possuir um processo para controle de ausência de segregação de função (SOD);
- Adotar política de privilégio mínimo;
- Possuir métodos para controle de acesso físico e lógico de visitantes; e
- Possuir controles de acesso remoto dos colaboradores/prestadores de serviço em período de *teletrabalho*.

6.2.3. Monitoramento dos serviços e gestão da operação de segurança da informação

- Assegurar que dispõe do mais alto nível de capacidade no provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados, bem como garantir o cumprimento da legislação e da regulamentação em vigor;
- Informar e dar acesso ao Grupo WEG, quando solicitado, sobre os recursos de gestão adequados ao monitoramento dos serviços contratados;
- Possuir recursos e ferramentas para o monitoramento de capacidade e disponibilidade dos seus ativos, correlacionando alertas e gerando tickets de incidentes de forma automatizada;
- Possuir um processo estruturado de Resposta a Incidentes, contemplando a categorização dos incidentes e *runbooks* para tratamento e resolução de incidentes já conhecidos.

- Prevenir, detectar e reduzir incidentes relacionados com o ambiente cibernético, evidenciando procedimentos e controles que abranjam, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de dados, a realização periódica de testes e varreduras para detecção de vulnerabilidade, a aplicação de *patches* de segurança, a aplicação de *hardening* em seus servidores e estações de trabalho, a proteção contra softwares maliciosos e bloqueio de softwares não homologados, o estabelecimento de mecanismos de rastreabilidade e de segmentação da rede de computadores, a manutenção de cópias de segurança dos dados e das informações;
- A WEG se reserva o direito de imediata e unilateralmente, revogar qualquer acesso em caso de incidente de segurança ou comportamento anormal/inadequado no ambiente WEG envolvendo o Parceiro, seja ele confirmado, sob suspeita ou em investigação;
- Fornecer, quando solicitado, informações relacionadas a quantidade de incidentes ocorridos nos últimos 24 meses, classificando-os pela sua relevância. Todos os dados sobre incidentes de severidade “média”, “alta” ou “muito alta” devem ser armazenados pelo Parceiro por ao menos 5 anos; e
- Manter o Grupo WEG permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

6.2.4. Gerenciamento de ameaças

O Parceiro deverá assegurar que as vulnerabilidades nos sistemas de TI sejam corrigidas por meio de patches ou atualizações em tempos adequados. Em qualquer hipótese, o Parceiro deverá:

a) No prazo de 24 horas a partir da descoberta de qualquer vulnerabilidade crítica (CVSS ou CVE 9.0 ou superior) nos sistemas informáticos relevantes do grupo contratante que não seja fornecida por terceiros:

- Iniciar o processo de desenvolvimento e implementação uma atualização ou patch para corrigir a vulnerabilidade;
- Notificar o Grupo WEG em soc@weg.net e fornecer detalhes sobre a vulnerabilidade e a ameaça relacionada, e quais medidas o Parceiro implementou para mitigar a ameaça ou vulnerabilidade.
- Assegurar que todos os sistemas de TI relevantes do Parceiro tenham os patches mais recentes fornecidos por terceiros instalados e implementados; e
- Instalar e implementar atualizações ou patches para vulnerabilidades incluídas no catálogo de vulnerabilidades exploradas conhecidas da Agência de Segurança Cibernética e de Infraestrutura dos EUA (*US Cyber & Infrastructure Security Agency*) dentro de 24 horas a partir do lançamento da atualização ou patch. Se qualquer atualização ou patch não puder ser aplicado por qualquer motivo dentro de 24 horas, o Parceiro deverá notificar imediatamente o Grupo WEG em soc@weg.net.

b) O Parceiro deverá:

- Assegurar que os sistemas de TI relevantes sejam continuamente monitorados para garantir sua segurança, autenticidade, confidencialidade, integridade e disponibilidade; e
- Gerar continuamente os registros de sistemas de TI relevantes necessários para: (A) habilitar a resposta a incidentes; (B) identificar a origem de um incidente; e (C) recriar a sequência de eventos que levam a um incidente. O Parceiro deve manter de maneira segura esses registros por pelo menos 180 dias a

partir da data de geração, de modo que esses registros só possam ser acessados por usuários autorizados.

6.2.5. Segurança no desenvolvimento de sistemas

- Adotar as práticas de *Privacy and Security by Design* em seus processos de desenvolvimento de software;
- Descrever os recursos de segurança e os dados acessados pelas aplicações, os quais devem ser avaliados pela área de Segurança de Informação durante a fase de homologação (Ex: Especificação técnica e/ou Diagrama Funcional);
- Utilizar rotinas de validação de integridade para prevenir erros, seja involuntário ou intencional, utilizando de dados fictícios ou anonimizações em ambiente não produtivo;
- Adotar as práticas de análise de segurança no código-fonte;
- Adotar as práticas de análise de segurança em suas aplicações (Ethical Hacking Tests e testes de intrusão);
- Prever as validações de segurança no processo de qualidade e verificação de código. No mínimo, devem ser consideradas aquelas que constam no OWASP TOP 10.

6.2.6. Continuidade dos negócios, gestão, retenção e armazenamento de dados.

- Definir um programa de continuidade de negócios, para assegurar que possíveis incidentes não afetem os serviços prestados ao Grupo WEG, contemplando especialmente o plano de recuperação de desastres, testando regularmente os controles de asseguração a fim de se verificar o quão preparada a empresa está para casos reais;
- Informar e dar acesso ao Grupo WEG, quando solicitado, sobre as medidas de segurança para a transmissão e armazenamento dos dados e informações, bem como o seu descarte, utilizando procedimentos seguros de exclusão (digital e/ou físico);
- Possuir um processo de execução de backups que seja realizado periodicamente nos ativos que armazenam informações do Grupo WEG, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

6.2.7. Treinamento e conscientização

- Assegurar da existência de um programa de treinamento e conscientização em Segurança da Informação e Privacidade de Dados, com periodicidade mínima anual, para todos os seus colaboradores, fornecedores e prestadores de serviço, sendo que o treinamento deve ser contemplado com a aplicação obrigatória do Código de Conduta do Parceiro para colaboradores, fornecedores e prestadores de serviço recém-contratados.
- Contemplar em seu programa de treinamento e conscientização de Segurança da Informação e Privacidade de Dados campanhas de prevenção contra o *phishing* e de orientação sobre engenharia social, bem como a realização de palestras, a emissão de boletins informativos de SI e Privacidade de Dados etc.

- Os colaboradores, fornecedores ou prestadores de serviço do Parceiro que tiverem acesso ou processarem dados pessoais e/ou informações sensíveis devem ter ciência desta Política e do que diz respeito a treinamento de segurança da informação proveniente.

6.2.8. Serviços e certificações

O Parceiro deve:

- Notificar, previa e formalmente, a subcontratação de serviços relevantes para o objeto de contrato com o Grupo WEG;
- Possuir reconhecimentos de segurança da informação ou continuidade dos negócios, comprovados por relatórios de auditorias externas independentes;
- Informar e dar acesso ao Grupo WEG, quando solicitado, sobre as certificações necessárias para a prestação dos serviços, bem como aos relatórios relacionados aos controles utilizados na prestação dos serviços contratados, elaborados por empresa de auditoria independente especializada; e
- Possuir mecanismos para comunicar anomalias ou incidente de segurança ao Grupo WEG, aos Indivíduos envolvidos e à Autoridade Nacional de Proteção de Dados.

7. AVALIAÇÕES PERIÓDICAS

O Grupo WEG poderá realizar, sempre que achar necessário, avaliações para atestar sobre a efetividade da implementação dos controles apresentados neste documento, devendo para isso, comunicar o parceiro com 30 dias de antecedência. Avaliações poderão ocorrer também caso ocorra algum incidente de segurança ou alteração nas condições de mercado aplicáveis ao segmento do Parceiro ou do Grupo WEG.

8. SANÇÕES

A violação a um controle ou a não-aderência à Política de Segurança da Informação para Parceiros e suas definições são consideradas faltas graves ou violações, podendo ser aplicadas penalidades ou sanções cabíveis de acordo com as Políticas internas do Grupo WEG e/ou previstas em contrato.

Em caso de violação de qualquer obrigação ou disposição da presente Política pelo Parceiro, seus colaboradores, fornecedores, prestadores de serviço e/ou quaisquer pessoas vinculadas ao Parceiro, o Parceiro se obriga a indenizar, manter indene, defender e isentar o Grupo WEG de todas e quaisquer perdas ou danos, sem prejuízo das demais cominações, sanções e/ou penalidades previstas em contrato ou em lei.

O Parceiro reconhece e concorda que a mera indenização pode não ser a forma adequada para sanar eventuais violações da presente Política, podendo o Grupo WEG valer-se de qualquer forma e/ou meio de execução específica de obrigações que seja cabível no caso de ameaça ou violação efetiva desta Parceria.