1. Objetivo do documento

A Política de Segurança da Informação para Terceiros tem como objetivo principal direcionar um programa efetivo de proteção dos ativos de informação, sendo a base para o estabelecimento de todos os padrões e procedimentos de segurança.

2. Abrangência da aplicação do documento

Todas as empresas que estabelecem contratos formais com o Grupo Greca se obrigam a cumprir os requisitos de Segurança da Informação aqui definidos.

O cumprimento das diretrizes estabelecidas é fundamental para a efetiva relação de parceria firmada para atingir níveis adequados de proteção à informação.

O Grupo Greca é composto pelas empresas AJG PARTICIPACOES SOCIETARIAS LTDA., ARTHUR GRECA SCHMUCK CONSULTORIA EMPRESARIAL, ATRIA S/A - CREDITO, FINANCIAMENTO E INVESTIMENTO, BRASIL MINERACAO E TRANSPORTES LTDA., GRCA PARTICIPACOES LTDA, GREGOR PARTICIPACOES LTDA, MAJIC PARTICIPACOES S/A, MAJIC II PARTICIPACOES S/A, GRECA DISTRIBUIDORA DE ASFALTOS LTDA., GRECA TRANSPORTES DE CARGAS LTDA.

3. Responsabilidades

3.1 Área Contratante de Serviços e Fornecedores

Quando da contratação de fornecedores que tenham colaboradores que venham a acessar a rede interna e os dados do Grupo Greca, a área contratante deverá garantir que todos estejam cientes dessa política de segurança da informação.

3.2 Prestador de Serviços/Fornecedores

É de responsabilidade dos prestadores de serviços/fornecedores do Grupo Greca observar e seguir as orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação, devendo cumprir com todos os requisitos da legislação brasileira aplicáveis, comprometendo-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;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis que regulamentam as atividades do Grupo e seu mercado de atuação;

- Selecionar os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- Comunicar imediatamente ao Grupo qualquer descumprimento da Política de Segurança da Informação para Terceiros.

4. Distribuição e vigência

Este documento consiste na Política de Segurança da Informação para Terceiros (prestadores de serviço e/ou fornecedores) do Grupo Greca, e deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a prevenção e proteção de ativos do Grupo, bem como definição de responsabilidades. Destaca-se que a mesma deve ser adotada, cumprida e aplicada por todos os prestadores de serviço e/ou fornecedores.

Esta versão pode ser alterada a qualquer momento, uma vez que os pontos identificados para mudanças sejam informados e discutidos com os membros do Comitê de Segurança da Informação do Grupo. Contudo, a versão da Política de Segurança da Informação para Terceiros deve ser revisada a cada ano, considerando a data de sua aprovação.

Em havendo atualizações, essas serão divulgadas a todos os prestadores de serviço e/ou terceiros.

5. Glossário

- Ativo: Algo que tenha valor para a organização;
- Incidente: Ocorrência que traz prejuízos à empresa;
- Internet: Rede mundial de computadores interligados entre si por meio do protocolo TCP/IP (Transmission Control Protocol/Internet Protocol);
- Malwares: Qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador;
- Ponto de Acesso ou AP: Equipamentos que permitem acesso às redes Wi-Fi e, consequentemente, à Internet;
- Risco: Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos;
- Site: Página ou sequência de páginas que uma pessoa jurídica ou física mantém na Internet;
- Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos à organização;
- Wi-Fi (Wireless Fidelity): Tecnologia de rede sem fio, baseada na especificação IEEE 802.11b/g/n, que define o método de acesso, velocidade e faixa de frequência, usada por essa rede;
- SSID (Service Set IDentifier): Conjunto único de caracteres que identifica uma rede sem fio.

6. Descrição da Política

6.1 Introdução

A presente Política de Segurança da Informação para Terceiros está baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente com um código de prática para a gestão da segurança da informação, e também em conformidade com a Resolução nº 4.893 de 26 de fevereiro de 2021 do Banco Central do Brasil, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

A informação é um ativo de grande valor para o Grupo Greca, por isso necessita ser adequadamente protegida.

Por princípio, a Segurança da Informação deve abranger três propriedades básicas:

- Confidencialidade: Informações devem estar acessíveis apenas para pessoas autorizadas;
- Integridade: Informações não devem sofrer alterações durante o seu processamento;
- Disponibilidade: Informações devem estar sempre acessíveis, a qualquer momento, para uso legítimo de pessoas autorizadas.

6.2 Conduta de Terceiros no Ambiente do Grupo Greca

6.2.1 Acesso Lógico e Uso Aceitável

O acesso lógico ao ambiente da rede interna, wi-fi e internet do Grupo Greca deverá ser solicitado pelo gestor responsável pela contratação, por meio da ferramenta de chamados da TI. A solicitação será avaliada e aprovada de acordo com a necessidade, seguindo as diretrizes corporativas de Segurança da Informação. O acesso só deve ser concedido após ciência do Termo de Responsabilidade, conforme ANEXO I.

Para prestadores de serviço/fornecedores que precisam acessar o ambiente do Grupo remotamente, o gestor responsável pelo contrato deve solicitar acesso à VPN através de chamado para TI, no qual somente poderá ter acesso aos recursos de trabalho e ambientes necessários para o desempenho de suas funções.

É dever do gestor responsável pelo terceiro informar a validade do contrato de prestação de serviços no momento da solicitação do acesso, bem como solicitar a exclusão do acesso quando não houver mais necessidade.

Os computadores de terceiros não podem ser conectados na rede interna do Grupo sem a aprovação prévia da TI, sendo que estes deverão estar protegidos por software antivírus/anti-malware e demais softwares devidamente licenciados.

Quando aplicável, o usuário e senha disponibilizado para o terceiro são de uso exclusivo e não podem ser divulgados ou compartilhados.

O terceiro deve manter suas credenciais de acesso seguras, sendo de sua responsabilidade qualquer utilização indevida.

É responsabilidade da empresa terceira comunicar qualquer desligamento de seus colaboradores para que os mesmos tenham seus acessos devidamente cancelados no ambiente do Grupo.

É proibido o compartilhamento de usuários e senhas entre os prestadores de serviços.

6.2.1.1 Orientações para utilização da Internet

É proibida a utilização do link de internet do Grupo Greca para acessar, propagar ou manter Portal ou Site(s) na Internet com conteúdo que:

1. Viole a lei ou que não seja autorizado;
2. Infrinja a propriedade intelectual, os direitos à honra, à imagem, à vida privada, à intimidade pessoal e familiar;
3. Estimule a prática de condutas contrárias à moral e aos bons costumes;
4. Induza à prática de atos discriminatórios, seja em razão de sexo, raça, religião, crenças, idade ou qualquer outra condição;
5. Coloque à disposição ou possibilite o acesso a mensagens, produtos ou serviços ilícitos, inapropriados, difamatório, violentos, obsceno e pornográfico;
6. Incite práticas perigosas, de risco ou nocivas para a saúde e para o equilíbrio psíquico;
7. Viole o sigilo das comunicações;
8. Constitua publicidade ilícita, enganosa ou desleal, em geral, que configure concorrência desleal e/ou denominado "spam-mails";
9. Acesso ou distribuição de conteúdo pornográfico de qualquer natureza ou conteúdo que viole o Estatuto da Criança e Adolescente;
10. Incorpore vírus ou outros elementos físicos ou eletrônicos que possam danificar ou impedir o normal funcionamento da rede, do sistema ou dos equipamentos informáticos (hardware e software) de terceiros ou que possam danificar os documentos eletrônicos e arquivos armazenados nestes equipamentos informáticos.

O Grupo Greca não se responsabiliza, direta ou indiretamente, por quaisquer despesas, danos ou perdas que sejam efetiva ou alegadamente causados por quaisquer conteúdos, produtos ou serviços disponíveis em referidos sites de terceiros ou recursos externos, não garantindo a perfeição, qualidade, veracidade, adequação, utilidade ou segurança do conteúdo ou de qualquer serviço oferecido, inclusive, mas não se limitando a, serviços envolvendo investimentos, seguros, aplicações, transferências de valores, e demais operações financeiras, ou pela utilização ou confiança depositada pelo usuário em tais conteúdos, produtos ou serviços.

Embora o Grupo Greca utilize as melhores tecnologias e empenhe seus maiores esforços, não possui a função nem as condições de controlar e garantir a ausência de vírus nos conteúdos transmitidos, difundidos, armazenados, recebidos, obtidos, colocados à disposição, ou acessíveis por meio da utilização da rede de dados e internet, nem a ausência de outros elementos que possam produzir alterações no equipamento informático do usuário ou nos documentos eletrônicos e pastas armazenadas ou transmitidas desde o equipamento informático do usuário.

Tendo em vista o disposto no item anterior, O GRUPO GRECA SE EXIME DE QUALQUER RESPONSABILIDADE PELOS DANOS E PREJUÍZOS DE QUALQUER NATUREZA QUE POSSAM DECORRER DA PRESENÇA DE VÍRUS OU DE OUTROS ELEMENTOS NOCIVOS NOS CONTEÚDOS E QUE, DESTA FORMA, POSSAM PRODUZIR ALTERAÇÕES E/ OU DANOS NO SISTEMA FÍSICO E/ OU ELETRÔNICO DOS EQUIPAMENTOS DO USUÁRIO. O GRUPO GRECA RESERVA-SE AO DIREITO DE REVISAR, A QUALQUER MOMENTO E SEM AVISO PRÉVIO, POR PRÓPRIA INICIATIVA OU A PEDIDO DE TERCEIRO, OS CONTEÚDOS TRANSMITIDOS, DIFUNDIDOS OU POSTOS À DISPOSIÇÃO DE TERCEIROS PELOS USUÁRIOS ATRAVÉS DO SERVIÇO E A IMPEDIR A SUA TRANSMISSÃO, DIFUSÃO OU COLOCAÇÃO A DISPOSIÇÃO DE TERCEIROS NO CASO DE QUE, NO SEU ENTENDIMENTO, RESULTAREM CONTRÁRIOS AO DISPOSTO NESTE TERMO DE USO.

6.2.2 Notificação de Incidentes de Segurança da Informação

Incidentes e não-conformidades de Segurança da Informação que sejam de conhecimento do terceiro devem ser imediatamente comunicados ao gestor do contrato para que este realize o processo de notificação de incidente à TI pelos meios formais.

Uma vez aberto, o processo de triagem, análise, tratamento e resposta seguem o mesmo fluxo dos incidentes internos do Grupo Greca.

6.2.3 Segurança de Equipamentos

Cada usuário é responsável pela proteção dos dispositivos físicos contendo informação do Grupo Greca que estão sob sua guarda, e devem estar cientes que o uso de qualquer recurso de TI no ambiente do Grupo, ainda que de propriedade pessoal, está sujeito a vistoria.

6.2.4 Violação de Conduta

São consideradas violações à esta Política as seguintes situações, não se limitando a:

- Quaisquer ações ou situações que possam expor o Grupo à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- Uso indevido de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Grupo;
- 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;
- A não-comunicação imediata de quaisquer descumprimentos da Política.

6.3 Controles de Segurança no Ambiente do Terceiro

O fornecedor que venha a oferecer serviços em nuvem, processar ou armazenar dados do Grupo em seu ambiente, deve seguir as seguintes diretrizes de segurança da informação:

6.3.1 Controle de Acesso

- Dar acesso irrestrito aos dados e informações armazenadas ou a serem processadas, conforme os serviços específicos definidos, prezando pela confidencialidade, integridade, disponibilidade e pela capacidade de recuperação destes dados e informações.

6.3.2 Gestão de Vulnerabilidade

- Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

6.3.3 Monitoramento dos Serviços

- 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.

6.3.4 Gestão de Incidentes

- Fornecer, quando solicitado, informações sobre incidentes relevantes ocorridos no fornecedor, bem como as ações tomadas;
- Manter o Grupo permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

6.3.5 Segurança no Desenvolvimento de Sistemas

- Desenvolver levando em consideração os padrões de segurança e privacidade aceitos pelo mercado;
- Descrever os recursos de segurança e os dados acessados pelas aplicações, os quais devem ser avaliados pela área de TI do Grupo durante a fase de homologação (Ex: Especificação técnica);
- Utilizar rotinas de validação de integridade para prevenir erros, seja involuntário ou intencional;
- Realizar análise de segurança no código-fonte.

6.3.6 Armazenamento de Dados

- Informar e dar acesso ao Grupo, quando solicitado, sobre as medidas de segurança para a transmissão e armazenamento dos dados e informações;
- Toda informação processada e/ou armazenada pelo fornecedor deve prever segregação de dados e dos controles de acesso, lógico e físico, de outras empresas;
- Deve prever a indicação dos países e da região em que cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados.

6.3.7 Gestão de Retenção de Dados

- Possuir um processo de execução de backups, o qual seja realizado periodicamente nos ativos que armazenam informações do Grupo, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes;
- Garantir que os dados serão totalmente excluídos quando solicitado.

6.3.8 Treinamento e Conscientização

- Assegurar a existência de um programa anual de treinamento e conscientização em Segurança da Informação para todos os colaboradores.

6.3.9 Subcontratação de Serviços

- Notificar antecipadamente sobre a subcontratação de serviços relevantes para o Grupo.

6.4 Avaliações periódicas

O Grupo 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.

6.5 Sanções

A violação a um controle ou a não-aderência à Política de Segurança da Informação para Terceiros e suas definições serão consideradas como descumprimento contratual, sujeitas às penalidades previstas em contrato, indenização e ressarcimento por prejuízos causados ao Grupo Greca e rescisão contratual motivada.

7. Considerações Finais

As dúvidas decorrentes nesta Política de Segurança da Informação para Terceiros deverão ser encaminhadas ao contato no Grupo, que dará o devido encaminhamento interno.

Esta PSI entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

8. Histórico de aprovação e revisão do documento

Número da revisão	Data	Descrição da revisão
1.0	14/08/2020	Elaboração da política.
2.0	26/11/2021	Atualização de resolução 4.658 para 4.893 do Banco Central do Brasil (BACEN), que dispõe sobre política de segurança cibernética e a contratação de serviços de processamento e armazenamento de dados em nuvem, no tópico 6.1

ANEXO I

TERMO DE CIÊNCIA E RESPONSABILIDADE SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA TERCEIROS NO GRUPO GRECA

Comprometo-me a:

1. Executar as atividades objeto de contratação de forma a cumprir com as orientações da Política de Segurança da Informação para Terceiros e com as Normas e Padrões vigentes;

2. Utilizar adequadamente os recursos do Grupo Greca, assegurando que sejam utilizados apenas para as finalidades aprovadas;

3. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a confidencialidade, integridade e disponibilidade;

4. Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;

5. Garantir a continuidade do processamento das informações críticas de negócios;

6. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade dos acessos à infraestrutura do Grupo, responsabilizando-se por si e também neste sentido em relação aos seus empregados, representantes, profissionais ou prepostos, ficando-lhe assegurado o direito de regresso;

7. Comunicar imediatamente ao Grupo qualquer descumprimento da Política de Segurança da Informação para Terceiros.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar rescisão contratual motivada, bem como na aplicação das penalidades previstas em contrato e indenização e ressarcimento por prejuízos causados ao Grupo Greca.

Data: __/__/____

Empresa:_____ CNPJ: _____

Nome: _____ Assinatura: _____