Grupo Eagle Gestão de Negócios

Política de Gestão de Prestadores de Serviço

Versão 1.0 - 15 de Agosto de 2020

Conteúdo

1. Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança para gerenciamento de prestadores de serviços contrato pelo Grupo Eagle Gestão de Negócios. A administração do Grupo Eagle Gestão de Negócios adotou esta política de segurança para assegurar que todos os colabores, prestadores de serviço, fornecedores e outros parceiros estejam cientes dos seus papéis e responsabilidades para os quais eles foram selecionados e assim garantir o uso correto dos privilégios concedidos e garantir a segurança de todas as suas operações.

2. Classificação do documento e alvo

Esta política se aplica a todos os colaboradores que gerenciam prestadores de serviço e parceiros do Grupo Eagle Gestão de Negócios. Exceções da política serão permitidas somente quando aprovadas antecipadamente por escrito pelo Chief Security Officer.

3. Seções da política e responsabilidades

3.1. Requisitos para o Gerenciamento de Prestadores de Serviço

a. Deve haver um acordo de confidencialidade por escrito entre as partes que inclua o reconhecimento da responsabilidade e confidencialidade pela segurança dos dados do Grupo Eagle Gestão de Negócios por parte do prestador de serviços.

b. O acordo de confidencialidade e responsabilidade deve se estender não somente às informações da Grupo Eagle Gestão de Negócios como dados de terceiros que estejam sob responsabilidade do Grupo Eagle Gestão de Negócios, onde deve possuir definições claras sobre os tipos de informações acessadas e seu propósito.

c. É de responsabilidade do Jurídico revisar todos os contratos com prestadores de serviço do Grupo Eagle Gestão de Negócios.

d. Os contratos devem declarar as responsabilidades de cada parte, data de efetividade, tipo de serviço sendo prestado, níveis de serviço e se necessário restrição jurídica ou comercial, assim como definição de ações para caso ocorra descumprimento dessas reponsabilidades.

e. É de responsabilidade da área de contratos manter uma lista de todos os prestadores com os quais a Grupo Eagle Gestão de Negócios, possui contrato. Além disso, esta lista deve revisada pelo menos uma (1) vez ao ano.

f. É de responsabilidade do gestor do serviço estabelecer critérios para escolha do prestador de serviço que inclusive leve em conta:

Critérios
Histórico e reputação do prestador de serviço
Qualidade de serviços prestados para outros clientes
Quantidade e competência de seus funcionários
Estabilidade financeira e comercial
Procedimentos e processos de Segurança da Informação de acordo com o mínimo aceitável pelo serviço sendo contratado

g. É de responsabilidade do gestor do serviço, em caso de encerramento de contrato, revisar o acordo de confidencialidade para determinar se este deve ser prorrogado para garantir a confidencialidade das informações

3.2. Gestão de Prestadores de Serviço

a. Os prestadores de serviço devem ser orientados sobre o sigilo e proteção das informações do Grupo Eagle Gestão de Negócios de acordo com a Política de Segurança da Classificação da Informação.

b. Os prestadores de serviço devem possuir um gestor de serviço atribuído que seja um funcionário do Grupo Eagle Gestão de Negócios.

c. Os prestadores devem ser notificados sobre as políticas, padrões e procedimentos de do Grupo Eagle Gestão de Negócios assim como qual o papel e responsabilidades em todo o ciclo.

d. Os prestadores de serviço que atuarem internamente no Grupo Eagle Gestão de Negócios devem dar o aceite na política de segurança da informação e no código de conduta definido pelo Grupo Eagle Gestão de Negócios. Esse aceite deve ser renovado a cada ano.

e. É de responsabilidade do gestor do serviço monitorar os prestadores de serviço quanto ao nível de seu serviço para garantir que estes estejam dentro do nível de serviço contratado.

f. É de responsabilidade do gestor do serviço realizar reuniões regulares para revisar relatórios dos serviços prestados.

3.3. Controles do Gerenciamento de Prestadores de Serviço

a. De acordo com a análise do departamento de Segurança da Informação podem ser atribuídos controles adicionais, como exemplo, mas não se limitando a:

Controle adicionais
Adoção de políticas, padrões e procedimentos de segurança da informação de acordo com os padrões estabelecidos pelo departamento de Segurança do Grupo Eagle Gestão de Negócios.
Checagem de indivíduos contratados para prestação de serviços no ambiente do Grupo Eagle Gestão de Negócios (A checagem deve respeitar a legislação brasileira).
Estabelecimento de procedimento de resposta a incidente em conjunto do prestador de serviço.
Revogação de acesso a informação ou destruição da informação quando do encerramento das atividades.

b. É de responsabilidade da Área de Tecnologia implementar e manter processo de monitoramento de trilha de auditoria de acordo com a Política de Segurança de Gerenciamento de Operações e Comunicações.

c. É de responsabilidade da Área de Tecnologia implementar e manter um processo de concessão de acesso a prestadores de serviço de acordo com a Política de Segurança de Gerenciamento de Acesso Lógico.

d. É de responsabilidade do gestor do serviço notificar e orientar os prestadores de serviço sobre alterações nas Políticas, Padrões e Processos de segurança da informação do Grupo Eagle Gestão de Negócios.

3.4. Responsabilidades

3.4.1. Segurança da Informação

a. O Chief Security Officer é responsável por coordenar e supervisionar o cumprimento das políticas e procedimentos em toda o Grupo Eagle Gestão de Negócios no tocante à confidencialidade, integridade e segurança de seus ativos de informação.

b. Garantir que os contratos com os prestadores de serviço possuam controles de segurança definidos de acordo com níveis aceitáveis.

c. Garantir que todos os prestadores de serviços recebam treinamentos apropriados das condições e requisitos de uso dos ativos de informação e políticas de segurança da informação do Grupo Eagle Gestão de Negócios

3.4.2. Gestão do Prestador de Serviço

a. Garantir que todos os prestadores de serviço conheçam as políticas de segurança da informação pertinentes para cumprimento de suas atividades.

3.4.3. Departamento Jurídico

a. Revisar e se necessário elaborar os contratos de acordo com as Políticas de Segurança da Informação Grupo Eagle Gestão de Negócios.

3.4.4. Prestadores de Serviço

a. Comunicar qualquer violação ou suspeita de violação das Políticas de Segurança da Informação.

b. Cumprir com os requisitos das Políticas de Segurança da Informação do Grupo Eagle Gestão de Negócios.

c. Garantir que requisitos mínimos de segurança da informação estejam implementados nos ativos de informação em sua custódia.

3.5. Aderência a norma PCI-DSS

3.5.1. Abrangência

Os tópicos abaixo foram criados a partir da mais recente norma PCI-DSS disponível no site do PCI Council (https://www.pcisecuritystandards.org). Uma completa referência está disponível no anexo "*Matriz de Normas e Requerimentos*".

3.5.2. Compartilhamento de Informações de Portadores de Cartão

Para todos os terceiros com os quais as informações de portadores de cartão são compartilhadas (ex. instalações de armazenamento de fitas de back-up, prestadores de serviço gerenciados tais como empresas de *web hosting* ou de serviços de segurança, ou aqueles que recebem informações para fins de modelagem de fraude), o seguinte deve ser feito:

a. Deve ser documentada uma lista de todos os terceiros com os quais as informações de portadores de cartão são compartilhadas.

b. Deve haver um acordo por escrito entre as partes (prestador de serviços e o Grupo Eagle Gestão de Negócios) que inclua o reconhecimento da responsabilidade pela segurança dos dados de portador de cartão de pagamento.

c. Ao contratar um prestador de serviços ou terceiro deve-se ter documentado as responsabilidades de ambas as partes com relação aos dados de portador de cartão de pagamento, essas responsabilidades devem ir de encontro com todos os requerimentos do PCI DSS aplicáveis aos serviços prestados. Isso pode ser efetuado da seguinte maneira:

- Caso o prestador de serviço ou terceiro esteja listado no website de Prestadores de Serviço Validados da Visa, é necessário validar que os serviços sendo prestados encontram-se no ambiente validado.

- Caso o prestador de serviço ou terceiro não esteja relacionado no website da Visa, uma lista com todas as normas PCI pelas quais a empresa será responsável deverá ser criada. Após a lista ser disponibilizada, evidência deve ser obtida do terceiro para demonstrar que ele atende a todas as normas PCI em questão, e que seu serviço não vai impactar o status geral de conformidade PCI DSS da empresa.

d. Ao menos uma vez por ano, a lista de terceiros deve ser revista. O acompanhamento dos terceiros que lidam com informações de portadores de cartão deve ser realizado para certificar que o status de conformidade PCI DSS ainda é atual.

e. Ao menos uma vez por ano, a Área de Segurança da Informação deve realizar um processo de diligência ("due diligence") nas instalações do prestador de serviço a fim de garantir a qualidade e conformidade dos serviços prestados e também para detectar possíveis problemas que impactem no ambiente do Grupo Eagle Gestão de Negócios (mais informações ver Formulario de DueDiligence).

3.6. Da Responsabilidade dos Prestadores de Serviço

3.6.1. Gerenciamento de Contas e Usuários/Clientes

a. Todas as contas de usuários/clientes devem ser protegidas e seus parâmetros devem seguir a *Política de Controle de Acesso*.

b. É de responsabilidade do prestadores de serviços prover documentação, orientação ou treinamento sobre os métodos disponíveis para troca de senha e em quais circunstância estas devem ser conduzidas.

3.6.2. Chaves Criptográficas Compartilhadas

a. Caso chaves criptográficas sejam compartilhadas com clientes/prestadores de serviço para transmissão de informações de portadores de cartão, documentação deve ser fornecida com orientações sobre como armazenar e modificar as chaves criptográficas (utilizadas para transmissão de informações com o Grupo Eagle Gestão de Negócios.)

3.6.3. Ambientes de Hospedagem compartilhada

a. Todas as informações das empresas ou clientes mantidas em ambientes de hospedagem compartilhada devem ser protegidas. Os pontos abaixo deve ser observados (mas não limitado à):

- Assegurar que cada empresa tenha acesso somente a seu próprio ambiente de informações de portadores de cartão.

- Caso as empresas sejam autorizadas a utilizar seus próprios aplicativos, os processos destes aplicativos devem utilizar o ID exclusivo da empresa. Por exemplo:

  ➔ Nenhuma empresa no sistema pode utilizar um ID de servidor web compartilhado.

  ➔ Todos scripts CGI utilizados por uma empresa devem ser criados e utilizados como a ID exclusiva de usuário da empresa.

- A ID de usuário de serviços não deve ser um usuário privilegiado (root/admin).

- Cada empresa deve ter permissões de *read, write* ou *execute* somente para arquivos e diretórios próprios ou para arquivos de sistemas necessários (restritos por meio de permissões de sistemas de arquivos, listas de controle de acesso, *chroot*, *jailshell*, etc.). Adicionalmente, os arquivos de uma empresa não podem ser compartilhados pelo grupo.

- Os usuários da empresa não devem tem acesso *write* a sistemas binários compartilhados.

- Para assegurar que cada empresa não possa monopolizar os recursos do servidor para explorar as vulnerabilidades (condições de *error*, *race* and *restart*, que resultem em, por exemplo, *buffer overflows*), restrições devem estar disponíveis para utilização de recursos do sistema, tais como *Disk space*, *Bandwidth, Memory* e *CPU*.

- As trilhas de *logging* e auditoria devem estar habilitadas e ser exclusivas ao ambiente de informações de portadores de cartão de cada empresa. Os registros devem estar ativos por "default" e devem estar habilitados para aplicativos de terceiros.

- Os registros devem estar disponíveis para revisão pela empresa titular e os locais dos registros devem ser claramente comunicados à empresa titular.

- A visualização dos registros deve ser restrita à empresa titular.

- No evento de um comprometimento, uma investigação por peritos especializados deve ser conduzida, de acordo com a *Política de Resposta a Incidentes.*

3.6.4. Armazenamento de Dados Sensíveis de Autenticação

a. Caso dados sensíveis de autenticação sejam armazenados para fins de emissão de cartões de pagamento, uma justificativa de negócio deve ser documentada e tais dados devem ser protegidos por criptografia forte conforme a *Política de Criptografia.*

4. Regulamentos externos

- PCI-DSS v3.0

5. Anexos

- Política de Controle de Acesso
- Política de Criptografia
- Política de Respostas a Incidentes
- Formulario de DueDiligence-v1_ptBR

6. Glossário

Ativos de informação
Qualquer informação de propriedade do Grupo Eagle Gestão de Negócios

Terceiro ou Prestados de Serviços
Qualquer usuário que não pertence ao quadro de colaboradores do Grupo Eagle Gestão de Negócios, porém possui contrato estabelecido e necessita de acesso a ativos de informação para cumprimento de suas funções.

7. Histórico de versões

Abaixo encontra-se a tabela com o histórico de revisões deste documento.

Versão	Data	Alterações	Responsável
1.0	15/08/2020	Versão inicial oficial – Grupo Eagle	João Felipe Leal Cordeiro

