
# Eagle Gestão de Negócios

# Política de Segurança da Informação

Versão 0.1 - 21 de Julho de 2020

# Conteúdo

# 1. Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança da informação da Eagle Gestão de Negócios para todos os colaboradores, prestadores de serviços e parceiros. A administração da Eagle Gestão de Negócios adotou esta política de segurança para proteger a informação com o objetivo de atingir suas metas comerciais ou de conformidade com normas ou leis aplicáveis.

Todos os ativos de informação são de propriedade intelectual da Eagle Gestão de Negócios, não importando a sua forma ou meio de armazenamento (digital ou impresso). Portanto o uso deste ativo só deve acontecer dentro das atividades de negócio que a administração da Eagle Gestão de Negócios ation julgar pertinente.

# 2. Classificação do documento e alvo

Esta política se aplica a todos os colaboradores, prestadores de serviço fornecedores e parceiros que utilizam, mantêm ou lidam com ativos de informação da Eagle Gestão de Negócios devem seguir esta política. Exceções da política serão permitidas somente quando aprovadas antecipadamente por escrito.

# 3. Seções da política e responsabilidades

## 3.1. Organizando a segurança da informação

Constituí-se nesta política a Área de Segurança da Informação, que tem a missão de assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e proporcionar confiança ao negócio onde a Eagle Gestão de Negócios atua.

### 3.1.1. Papeis e responsabilidades da segurança da informação

- Chief Security Officer

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

O Chief Security Officer trabalha juntamente ao Chief Information Office e outros administradores e colaboradores da Eagle Gestão de Negócios envolvidos em proteger os ativos de informação da empresa para aplicar as políticas definidas, identificar áreas de preocupação e implantar as mudanças apropriadas de acordo com as necessidades. As responsabilidades especificas do Chief Security Officer incluem:

| Responsabilidades do Chief Security Officer |
| --- |
| – Tomar decisões de alto nível pertinentes às Políticas de Segurança da Informação e seu conteúdo. Aprovar, antecipadamente, exceções a estas políticas com base em análise caso-a-caso. |

- Coordenar, anualmente, uma verificação de risco formal para identificar novas ameaças e vulnerabilidades e identificar controles apropriados para minimizar qualquer novo risco.
- Rever anualmente as políticas e procedimentos de segurança da informação para manter a adequação face às emergentes necessidades de negócio ou ameaças à segurança.
- Certificar que terceiros, com os quais informações de portadores de cartão são compartilhadas, estejam contratualmente obrigados a adotar as normas PCI DSS e reconhecer que são responsáveis pela segurança dos dados dos portadores de cartão processados por eles.
- Manter atualizados e distribuir o Plano de Resposta e Procedimentos para todos os usuários.
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional.
- Consultar anualmente as demais áreas de negócios e verificar se novos métodos de aceitação de cartões de pagamento foram adotados e verificar a aplicabilidade do PCI DSS a esses novos métodos. Qualquer mudança no escopo do PCI DSS deve ser documentada na Descrição do Ambiente PCI.

## Área de Segurança da Informação

A proteção bem sucedida dos sistemas da Eagle Gestão de Negócios requer que vários departamentos e grupos sigam consistentemente uma visão compartilhada de segurança.

O Área de Segurança da Informação trabalha com os gerentes, administradores e usuários de sistemas dos departamentos no desenvolvimento de políticas, normas e procedimentos de segurança para ajudar na proteção dos ativos da Eagle Gestão de Negócios

O Área de Segurança da Informação é dedicada ao planejamento, educação e conscientização sobre segurança. As responsabilidades específicas do Área de Segurança da Informação incluem:

### Responsabilidades da Área de Segurança da Informação

- Criar novas políticas e procedimentos de segurança da informação quando necessário. Manter e atualizar Políticas e procedimentos de segurança da informação existentes. Rever anualmente as políticas e auxiliar a administração com o processo de aprovação.
- Agir como um departamento central de coordenação para implantação das políticas de Segurança da Informação.
- Criar, manter e distribuir procedimentos de resposta a incidentes e de encaminhamento.
- Monitorar e analisar alertas de segurança e distribuir informações ao pessoal apropriado de segurança, técnico e da administração da unidade de negócios.
- Fazer a revisão diária dos registros. Verificar qualquer exceção identificada.
- Restringir e monitorar o acesso a áreas restritas e informação confidencial. Assegurar que os controles adequados estejam disponíveis onde houver informações de portadores de cartão.
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional (Anexo N).

## Administrador de Sistemas

 

O Administrador de Sistemas da Eagle Gestão de Negócios são o elo direto entre as políticas de Segurança da Informação e a rede, os sistemas e os dados. As responsabilidades dos Administrador de Sistemas incluem:

Responsabilidades do Administrador de Sistemas

- Aplicação das políticas e procedimentos de segurança da informação de acordo com sua aplicabilidade a todos os ativos de informação.
- Administração das contas de usuários e gerenciamento de autenticação.
- Auxiliar o Área de Segurança da Informação com o monitoramento e controle de todos os acessos aos dados da Eagle Gestão de Negócios
- Manter um diagrama de rede atualizado incluindo as redes sem fio. O diagrama deve incluir a data em que se deu a última atualização .
- Restringir o acesso físico a pontos de rede acessíveis ao público, pontos de acesso sem fio, gateways e equipamentos portáteis (hand held).
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional (Anexo N).

## Recursos Humanos

Devido ao seu relacionamento direto e constante com os funcionários existentes, assim como sua posição única de ter a primeira e última interações com novos/ ex- funcionários, o Recursos Humanos tem um papel importante no que se refere à segurança das informações da Eagle Gestão de Negócios. Os seguintes itens são responsabilidade do Recursos Humanos:

Responsabilidades do Recursos Humanos

- Auxiliar o Área de Segurança da Informação com a publicação e disseminação das políticas de Segurança da Informação e orientação sobre o uso aceitável a todos os usuários de sistema relevantes incluindo prestadores de serviço, empreiteiros e parceiros de negócio.
- Realizar verificações de antecedentes de potenciais funcionários que terão acesso a dados de portador de cartão de pagamento ou ao ambiente PCI. Quando possível e, dentro das condições previstas pela legislação, as verificações devem incluir: histórico de empregos anteriores, verificação de antecedentes criminais, verificações de crédito e análise de referências pessoais. Para candidatos a vagas que lidam com apenas um número de cartão de pagamento por vez durante o processamento de uma transação (como operadores de caixa), as verificações descritas não são obrigatórias, porém sua execução é recomendada.
- Certificar–se de que o funcionário participe do treinamento de conscientização sobre segurança após a contratação e pelo menos uma vez por ano.
- Trabalhar com o Área de Segurança da Informação na disseminação de informações de conscientização sobre segurança, utilizando diversos métodos de comunicação de conscientização e educação dos funcionários (ex. pôsteres, cartas, memorandos, treinamento via web, reuniões, etc).
- Trabalhar com o Área de Segurança da Informação para administrar sanções e ações disciplinares referentes a violações da Política de segurança da informação.
- Notificar o Área de Tecnologia quando qualquer funcionário for desligado.
- Manter todos os Formulários de Conscientização sobre Segurança e Uso Aceitável (Anexo A) e de Solicitação de Autorização (Anexo G) nos arquivos dos funcionários.

- Usuários

Todo usuário de recursos computacionais e de informação da Eagle Gestão de Negócios devem estar cientes da importância fundamental de tais recursos e reconhecer sua responsabilidade pela manutenção segura dos mesmos. Os usuários devem protegê-los contra abusos que interrompam ou ameacem a viabilidade de todos os sistemas. As seguintes responsabilidades são especificas a todos os usuários de sistemas computacionais da Eagle Gestão de Negócios:

Responsabilidades do Usuários

- Entender as conseqüências de suas ações relacionadas às praticas de segurança computacional e agir de forma condizente. Aceitar que a filosofia de que "Segurança é responsabilidade de todos" para auxiliar a Eagle Gestao de Negócios no atingimento de seus objetivos comerciais.
- Manter a conscientização sobre o conteúdo das políticas de Segurança da Informação.
- Ler e assinar a Política de Conscientização sobre Segurança e Uso Aceitável (Anexo A) da Eagle Gestão de Negócios quando de sua contratação e ao menos uma vez ao ano.
- Classificar informações confidenciais e sensíveis que sejam recebidas sem classificação, de acordo com a Política de Classificação e Controle de Informaçao. Limitar a distribuição destas informações.

### 3.1.2. Segregação de funções

Para todos os ambientes da Eagle Gestão de Negócios, sejam eles de produção, homologação, desenvolvimento ou teste, é obrigatório a implementação de segregação de funções. A segregação de funções determina que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada, ou para coibir o mau uso dos ativos da organização intencional ou não intencional. Para casos de exceção, seja por limitação técnica ou de negócio, é obrigatório o uso de controles adicionais de segurança e aprovação do Chief Security Officer.

### 3.1.3. Contato com as autoridades externas

Como parte do plano de comunicação interno e externo e do plano de resposta a incidentes de segurança da informação da Eagle Gestão de Negócios, declara-se que qualquer comunicação relacionada a segurança da informação, junto à autoridades externas que incluem mas não se limitam a entidades reguladoras, entidades de conformidade e governo, devem ser previamente autorizadas pelo Chief Security Officer.

### 3.1.4. Segurança da informação no gerenciamento de projetos

Como parte da metologia de gerenciamento e projetos da Eagle Gestão de Negócios, todos os projetos devem incluir segurança da informação dentro do seu ciclo de vida. A inclusão tem como objetivo avaliar os riscos de segurança da informação, bem como propor controles adequados e acrescentar aos objetivos do projeto, os objetivos de segurança de informação.

## 3.2. Política de Segurança em Recursos Humanos

A área de Recursos Humanos deve criar e manter atualizado critérios de seleção para candidatos (funcionários ou prestadores de serviço) que tenham como objetivo, garantir a veracidade e honestidade das informações fornecidas, sendo que estes critérios devem respeitar e atender as regulamentações e leis vigentes.

Além disso os acordos de confidencialidade devem ser anexados ao contrato de trabalho ou prestação de serviço, aos quais devem ser assinados e devolvidos para os seus representantes legais. Para mais informações, consulte a Política de Segurança em Recursos Humanos.

## 3.3. Política de Gestão de Ativos

Todos os ativos de informação da Eagle Gestão de Negócios deverão ser classificados de acordo com o seu nível de confidencialidade, disponibilidade, integridade e controles legais. Uma vez classificados, devem ser respectivamente relacionados ao modo como são acessados, armazenados, movimentados e por fim descartados.

Todos os ativos de informação em forma de mídias removíveis ou impressos devem ter sua classificação de modo claro e visível para que se possa dar o devido grau de tratamento. Para mais informações, consulte a Política de Gestão de Ativos.

## 3.4. Política de Controle de Acesso

Todos os sistemas de informação da Eagle Gestão de Negócios devem estar integrados à um sistema de controle de acesso homologado pelos Área de Tecnologia e a Área de Segurança da Informação.

A concessão de acessos (recursos ou sistemas) devem ser aprovados pelo gestor da informação. Além disso deve ser instituido a segregação de função de acordo com nível funcional ou responsabilidade assim como uma revisão periódica dos acessos concedidos, afim de se evitar acessos indevidos. Para mais informações, consulte a Política de Controle de Acesso.

## 3.5. Política de Criptografia

Toda informação da Eagle Gestão de Negócios, que precise ser protegida contra acesso não autorizado ou estabelecido por normas externas ou internas de conformidade, deve utilizar criptografia robusta conforme os padrões aceitos pelo mercado, de modo a garantir a confidencialidade, autenticidade e integridade da informação.

Além disso todas as chaves de criptografia utilizadas, devem ser gerenciadas por um processo que determine as diretrizes do ciclo de vida da chave e outros aspectos relevantes. Para mais informações, consulte a Política de Criptografia.

## 3.6. Política de Segurança Física e do Ambiente

É de responsabilidade dos seus respectivos proprietários proteger os ativos de informação contra danos, roubo ou qualquer evento que possa gerar indisponibilidade.

É necessário estabelecer o perímetro de segurança física de modo a preservar o acesso somente a pessoas autorizadas. Além disso deve ser instituído de modo obrigatório o uso de identificação funcional (crachá), para que seja possivel monitorar os mais diversos níveis de acesso para colaboradores, prestadores de serviço, parceiros de negócios e visitantes. Para mais informações, consulte a Política de Segurança Física e do Ambiente.

## 3.7. Política de Segurança nas Operações

A Área de Tecnologia com apoio da Área de Segurança da Informação, deve estabelecer as diretrizes para garantir a operação segura e correta dos recursos de processamento da informação. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis ao usuários necessários.

Este procedimentos operacionais devem incluir e não se limitar a, procedimentos de instalação e configuração de sistemas, procedimentos para manipulação de informação, procedimentos de cópias de segurança (backup), procedimentos para gerenciamento de trilhas de auditoria e procedimentos de monitoramento de eventos.

Além disso deve ser estabelecido um processo único de gestão de mudanças com o objetivo de controlar e garantir a autorização e documentação de toda mudança no ambiente. Para mais informações, consulte a Política de Segurança nas Operações.

## 3.8. Política de Segurança nas Comunicações

A Área de Tecnologia com apoio da Área de Segurança da Informação, deve estabelecer as diretrizes para garantir a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis ao usuários necessários e que estabelecam as responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede. Para mais informações, consulte a Política de Segurança nas Comunicações.

## 3.9. Política de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação

Todos os processos que envolvam aquisição, desenvolvimento ou manutenção de sistemas de informação, somente devem ser feitos a partir das áreas custodiantes mediante autorização da Área de Tecnologia e a Área de Segurança da Informação. Além disso deve ser contemplado em cada processo a execução de testes de segurança para garantir que os riscos relacionados sejam conhecidos e tratados. Para mais informações, consulte a Política de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação.

## 3.10. Política de Gestão de Prestadores de Serviço

Todo relacionamento com prestadores de serviço deve seguir as diretrizes estabelecidas, de modo a garantir a proteção dos ativos da Eagle Gestão de Negócios acessados por estes fornecedores. Além disso todo relacionamento acordado deve ser formalizado e estabelecido entre as partes cláusulas de confidencialidade e de responsabilidade na manipulação de informações e prestação de serviços. Para mais informações, consulte a Política de Gestão de Prestadores de Serviço.

## 3.11. Política de Gestão de Incidentes de Segurança da Informação

O processo de gestão de incidentes de segurança da informação tem como objetivo garantir que eventos de segurança da informação associados a ativos de informação da Eagle Gestão de Negócios sejam comunicados a Área de Segurança da Informação.

É de responsabilidade da Área de Segurança da Informação coordenar todas as atividades pertinentes ao processo de gestão de incidentes de segurança da informação. É dever de todos os usuários de informação comunicar um incidente de segurança da informação para área responsável. Para mais informações, consulte a Política de Gestão de Incidentes de Segurança da Informação.

## 3.12. Política de Continuidade de Negócios

O processo de gestão de continuidade do negócio deve ser implementado com o objetivo de reduzir os impactos sobre os negócio da Eagle Gestão de Negócios. É responsabilidade do gestor da unidade de negócio em solicitar a Área de Tecnologia a condução e suporte dos planos de continuidade. Para mais informações, consulte a Política de Continuidade de Negócios.

## 3.13. Política de Dispositivos Móveis

A Área de Tecnologia e a área de Recursos Humanos com apoio da Área de Segurança da Informação, devem estabelecer as diretrizes para garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis da Eagle Gestão de Negócios. Para isso devem estabelecer uma política formal e acessível com as condições e restrições.

Esta política deve incluir e não se limitar a, procedimentos de registro dos dispositivos móveis, proteção física, instalação de software, acesso a informações classificadas, controle de acesso, desativação ou bloqueio remoto e cópias de segurança (backup). Para mais informações, consulte a Política de Dispositivos Móveis.

### 3.14. Conformidade

Todos os ativos e sistemas de informação da Eagle Gestão de Negócios, assim como os seus funcionários e prestadores de serviço devem estar em conformidade com as obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação estabelecidos pela Eagle Gestão de Negócios.

Com objetivo de prevenir violações, todas as informações armazenadas ou que trafeguem dentro dos perímetros físicos e lógicos da Eagle Gestão de Negócios podem ser monitoradas, mediante a processo de aprovação instituído, revisado pela Área de Segurança da Informação. Violações não serão toleradas e as sanções apropriadas serão aplicadas.

Para fins específicos da norma PCI-DSS (Payment Card Industry), a Eagle Gestão de Negócios estabeleceu uma política específica que complementa as demais políticas existentes e estabelece as diretrizes a serem seguidas por seus funcionários e prestadores de serviço. Para mais informações, consulte a Política de Manutenção do PCI-DSS.

## 4. Regulamentos externos

- PCI-DSS v3.1

## 5. Anexos

- Política de Segurança em Recursos Humanos
- Política de Gestão de Ativos
- Política de Controle de Acesso
- Política de Criptografia
- Política de Segurança Física e do Ambiente
- Política de Segurança nas Operações
- Política de Segurança nas Comunicações
- Política de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação
- Política de Gestão de Prestadores de Serviço
- Política de Gestão de Incidentes de Segurança da Informação
- Política de Continuidade de Negócios
- Política de Dispositivos Móveis

- Política de Manutenção do PCI-DSS

## 6. Glossário

## 7. Histórico de versões

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

| Versão | Data | Alterações | Responsável |
|---|---|---|---|
| 0.1 | 21/07/2020 | Versão inicial | João Felipe Cordeiro |
| | | | |
| | | | |