Getnet

# Política do Sistema de Gestão da Getnet



**ÍNDICE**


1. OBJETIVO ..... 3
2. ABRANGÊNCIA ..... 3
3. APLICAÇÃO NORMAS E CERTIFICAÇÕES ..... 3
4. TERMOS E DEFINIÇÕES ..... 3
5. DISPOSIÇÕES GERAIS ..... 5
6. DIRETRIZES ..... 6
7. RESPOSABILIDADES ..... 8
7.1. ALTA DIREÇÃO ..... 8
7.2. COLABORADORES ..... 8
7.3. QUALIDADE PARA CLIENTES ..... 8
7.4. REENGENHARIA DE PROCESSOS ..... 8
7.5. SEGURANÇA DA INFORMAÇÃO ..... 9
7.6. COE LEARNING (RH) ..... 9
7.7. COE TALENT ACQUISITION (RH) ..... 9
7.8. GESTÃO DE ACESSOS (SDS) ..... 9
8. CONTROLE E INDICADORES ..... 10
9. ANEXOS ..... 10
10. REFERÊNCIAS ..... 10
11. HISTÓRICO DE REVISÕES ..... 11


*As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.*

## 1. OBJETIVO

Direcionar e orientar as ações dos colaboradores e processos de negócio da organização a fim de garantir e preservar a confidencialidade, integridade e disponibilidade das informações, além de orientar os colabores quanto as diretrizes de qualidade e atendimento ao cliente.

## 2. ABRANGÊNCIA

(x) Getnet (x) Auttar (x) SCD (x) GetAtende ( ) Eyemobile (x) Mobyan

## 3. APLICAÇÃO NORMAS E CERTIFICAÇÕES

(x) Auditoria (x) BACEN (x) ISO ( ) PCI ( ) SOx ( ) Outros

Outros, especificar: Pulse

## 4. TERMOS E DEFINIÇÕES

**Alta Direção:** pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível, abrangendo Vice-presidência e Presidência.

**Análise crítica:** Atividade realizada para verificar se os controles e medidas traçadas para alcançar os objetivos de uma determinada meta estão pertinentes, adequados e eficazes.

**Análise de causa raiz:** É um processo que identifica os eventos responsáveis pelas falhas e que utiliza essas informações para definir as ações certas para evitar reincidência do problema.

**Benchmark:** O processo de comparação do desempenho entre dois ou mais sistemas.

**COMEX:** Comitê Executivo formado pela presidência, vice-presidências e demais gestores convidados, e que tem como funções principais o planejamento e decisões estratégicas para a Gestão da empresa.

**Comitê de Satisfação de Clientes:** Reunião periódica de Qualidade que tem por objetivo assessorar o Comitê Executivo (COMEX) na monitoria da jornada do cliente com geração de planos de melhoria de processos e projetos para maximizar a satisfação total dos clientes da Getnet Adquirência e Serviços para Meios de Pagamentos S.A e de suas controladas. A reunião é gerenciada pelo gerente da área de Ouvidoria.

*As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.*

**Gestão das Reclamações:** Engloba todo o processo de Gestão das Reclamações, entrada, tratamento e saída da reclamação.

**KPIs:** Sigla de 'Key Process Indicators', indicadores estratégicos da organização

**NPS:** Net Promoter Score é uma métrica que tem como objetivo medir a satisfação e lealdade dos clientes com as empresas.

**Reclamação:** Expressão de insatisfação, relativa a seus produtos/serviços ou ao próprio processo de tratamento de reclamações, para a qual explícita ou implicitamente espera-se uma resposta ou resolução.

**SLA**: Service Level Agreement ou Acordo de Nível de Serviço é parte do contrato de serviços entre duas ou mais entidades. Na prática, o termo é usado no contexto de tempo de entregas de um serviço ou de um desempenho específico.

**Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano um sistema ou para a Getnet.

**Ativo:** tudo o que a Getnet considera valioso é um ativo. Exemplos de ativos são os serviços e processos tecnológicos, como softwares e hardwares (computadores, servidores, equipamentos de rede etc.), além da própria informação (dados de cartão e do portador de cartão, documentos internos etc.) e seus colaboradores.

**Colaborador:** Nome utilizado para referir-se a funcionários da Getnet, Controladas e Coligadas.

**Confidencialidade:** Propriedade que define que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

**Disponibilidade:** propriedade de estar acessível e utilizável sob demanda por uma entidade autorizadora.

**Firewall:** Tecnologia de hardware e/ou software que protege recursos de rede de acesso não autorizado. O firewall permite ou nega tráfego de computador entre redes com diferentes níveis de segurança com base em um conjunto de regras e outros critérios**.**

**Integridade:** Propriedade de salvaguarda da exatidão e completude de ativos**.**

**Informação sensível:** Toda informação classificada com rotulação **Secreto, Confidencial Restrito ou Confidencial**. Exemplos de informações sensíveis são dados do portador do cartão, relatórios de auditoria, informações de clientes e colaboradores, contratos.

***Malwares*:** Softwares maliciosos que se propagam nas redes corporativas com o intuito de causar algum dano ou coletar informações do sistema ou rede em que se encontra instalado. Normalmente o *malware* é conhecido como vírus.

**Política:** Intensões e diretrizes globais formalmente expressas pela alta direção.

**Segurança da Informação:** preservação e garantia das propriedades de confidencialidade, integridade e disponibilidade.

**Vulnerabilidade:** Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

## 5. DISPOSIÇÕES GERAIS

Todo documento sem tarja (obsoleto/em revisão) é considerado vigente desde que disponível na Plataforma de Documentos.

Os colaboradores envolvidos no processo em questão estão cientes de que as diretrizes definidas neste documento poderão ser auditadas e devem auxiliar o Auditor na obtenção de dados que subsidiem seu trabalho com informações suficientes, fidedignas, relevantes e úteis, como base sólida para emissão de seu relatório final.

***Portanto, recomenda-se não salvar cópias dos normativos na área de trabalho/diretórios da rede ou imprimi-los.*** O colaborador deve sempre acessar a Plataforma de Documentos.

Este documento encontra-se no padrão de formatação definido pela ABNT NBR 14724:2011, portanto, o redator deve garantir que a formatação e estrutura do documento siga os padrões já definidos.

## 6. DIRETRIZES

A Getnet, empresa fornecedora de serviços de meios de pagamentos e tecnologia, define diretrizes para monitorar e promover a melhoria contínua dos seus Sistemas de Gestão buscando superar positivamente as expectativas de seus stakeholders, além de garantir a segurança das informações.

São compromissos da empresa:

- Trabalhar com paixão e colaboração para atingir a Satisfação de seus Clientes, estabelecendo processos que propiciem um tratamento justo, uma comunicação clara e empática, de forma que se sintam únicos;
- Atender aos requisitos legais, estatutários, organizacionais, regulatórios, financeiros e outros pertinentes, associados aos seus produtos e serviços, a fim de entregar resultados no curto e longo prazo, sempre de forma ética e transparente.
- Buscar o comprometimento de todos os colaboradores, para construir a cultura da excelência Getnet, incentivando-os para a busca da melhoria contínua dos Sistemas de Gestão atualizado e compromisso com resultados, através de treinamento contínuo;
- Proporcionar meios e recursos para o atingimento dos objetivos e metas dos Sistemas de Gestão, mensurando o seu progresso regularmente;
- Adotar princípios, para tomada de decisões, que pautem pelo imaginar, cuidar e simplificar;
- Trabalhar com transparência e ética em todas as relações com os stakeholders, assim como considerar e tratar de forma adequada as informações fornecidas por esses, garantindo confidencialidade, integridade e disponibilidade delas;
- Garantir a confidencialidade, integridade e disponibilidade das informações dos seus clientes e da própria Getnet, protegendo os dados e os sistemas de informação contra acessos indevidos e modificações não autorizadas;
- Garantir e proteger os processos críticos de negócio contra falhas ou desastres significativos.
- Disponibilizar um serviço de atendimento para recepção, gestão e resolução de reclamações, assegurando priorização e imparcialidade, colocando seu cliente na essência desse processo.
- Estabelecer critérios e métodos para avaliação de riscos e oportunidades dos seus processos, a fim de ter uma operação segura e eficiente;

- Assegurar que somente pessoas autorizadas tenham acesso às instalações da Getnet, às informações e aos sistemas de informação.
- Atribuir identificações únicas a cada colaborador que necessite acessar sistemas computacionais.
- Registrar, analisar, investigar e tratar os incidentes de segurança da informação, criando mecanismos de prevenção para evitar a sua ocorrência.
- Assegurar o treinamento contínuo e atualizado nas políticas e nos procedimentos do Sistema de Gestão Getnet, enfatizando as obrigações das pessoas pela segurança da informação e qualidade.
- Garantir que todas as responsabilidades pela segurança da informação e qualidade estão claramente definidas e que as pessoas indicadas são competentes e capazes de cumprir com as atribuições pela segurança da informação.
- Monitorar e atuar sobre o desempenho dos seus processos e produtos a fim de fornecer aos seus clientes soluções inovadoras, seguras e eficientes em todo ecossistema de pagamento.
- Monitorar e atuar sobre o desempenho dos fornecedores considerados críticos para o Sistema de Gestão da Getnet;
- Instalar e manter configuradas as ferramentas e os mecanismos de segurança para proteger as informações sensíveis do negócio da Getnet.
- Alterar os padrões de configuração disponibilizados pelos fabricantes de todos os sistemas e componentes de segurança, visando à conformidade com as políticas da Getnet.
- Criptografar todas as informações sensíveis que trafeguem em redes públicas e abertas.
- Desenvolver sistemas e aplicativos de forma segura.
- Restringir o acesso às informações sensíveis de acordo com a necessidade de conhecimento para o negócio.
- Monitorar, controlar e acompanhar todos os recursos da rede e às informações sensíveis.
- Testar regularmente os processos e sistemas de segurança da informação.
- Seguir procedimentos operacionais diários de segurança da informação.
- Classificar todas as informações de acordo com o respectivo nível de confidencialidade.

*As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.*

- Garantir que os colaboradores e prestadores de serviço assinem um contrato de confidencialidade para garantir que as informações da Getnet não serão divulgadas.

## 7. RESPOSABILIDADES

### 7.1. ALTA DIREÇÃO

- Assegurar que as metas de Qualidade e Segurança da Informação estejam de acordo com os requisitos da Getnet e que estejam claramente identificadas;
- Aprovar e analisar criticamente as políticas de Relacionamento com Clientes e de Segurança da Informação;
- Apoiar as iniciativas relacionadas a Qualidade e a Segurança da Informação;
- Fornecer os recursos necessários para que os objetivos de Qualidade e Segurança da Informação sejam atingidos;
- Analisar e aprovar as atribuições de responsabilidade e de tarefas relacionadas a Qualidade e Segurança da Informação;
- Nortear as ações do sistema de gestão com foco na satisfação dos clientes e partes interessadas;

### 7.2. COLABORADORES

- Conhecer e seguir as diretrizes e normas vigentes relacionadas a Qualidade e Segurança da Informação.

### 7.3. QUALIDADE PARA CLIENTES

- Gerir as ações relacionadas a Qualidade da organização;
- Monitorar e analisar as informações e indicadores relacionados a Qualidade;
- Disseminar a Política de Relacionamento Com Clientes na companhia;
- Realizar, organizar, gerir e orientar as empresas quanto as auditorias relacionadas à norma ISO 9001, sendo elas de primeira, segunda ou terceira parte.

### 7.4. REENGENHARIA DE PROCESSOS

- Padronizar e gerenciar os normativos da companhia;

*As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.*

### 7.5. SEGURANÇA DA INFORMAÇÃO

- Gerir a segurança das informações da Getnet.
- Definir e documentar as políticas e procedimentos de Segurança da Informação.
- Definir e comunicar os procedimentos de gestão de incidentes de Segurança da Informação.
- Avaliar os riscos de Segurança da Informação;
- Relatar o desempenho do Sistema de Gestão de Segurança da Informação (SGSI) através de indicadores para a alta direção;
- Gerir o programa de conscientização em Segurança da Informação.
- Analisar e tomar decisões de resposta aos alertas de segurança relacionados ao ambiente cibernético da Getnet monitorados pela equipe de Gestão de Incidentes corporativa.
- Realizar, organizar, gerir e orientar as empresas quanto as auditorias relacionadas à norma ISO 27001, sendo elas de primeira, segunda ou terceira parte.

### 7.6. COE LEARNING (RH)

- Mediante acionamento das áreas responsáveis dos processos do Sistema de Gestão, fomentar e conscientizar os colaboradores em relação a importância da qualidade, excelência operacional e segurança da informação na companhia, enfatizando o Sistema de Gestão;
- Disponibilizar meios para que os colaboradores sejam capacitados em relação a qualidade quando cabível e necessário;

### 7.7. COE TALENT ACQUISITION (RH)

- Analisar os potenciais colaboradores antes de serem contratados e garantir que estes tenham as competências necessárias para realizarem suas atividades;
- Garantir a ciência do termo de confidencialidade de todos os novos colaboradores.

### 7.8. GESTÃO DE ACESSOS (SDS)

- Administrar as solicitações de criação, alteração, revisão e deleção de contas de usuários.

*As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.*

## 8. CONTROLE E INDICADORES

Os indicadores monitorados são:

a) volume de constatações de cada auditoria, sendo elas:

- Ponto forte: Boas práticas;
- Oportunidade de Melhoria: Oportunidade identificada pela equipe auditora que não representa o não atendimento de um requisito;
- Não Conformidade: O não atendimento de um requisito pré-estabelecido
- Não Conformidade Maior: O não atendimento de um requisito pré-estabelecido de forma sistêmica na empresa ou a reincidência de apontamentos (não conformidade mesmo requisito / processo da auditoria anterior)

b) percentual de ações entregues no prazo (SLA).

## 9. ANEXOS

N/A

## 10. REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2022

ABNT NBR ISO/IEC 27002:2022

ABNT NBR ISO 9001:2015

PCI-DSS Requirements and Security Assessment Procedures - Versão 3.2.1

PL000499 - Política Corporativa de Relacionamento com Clientes

PR000187 - Procedimento de Gestão de Reclamação

PL000103 - Política de Reclamações

PR000189 - Procedimento de Tratamento de Não Conformidades e Melhorias

PL000362 - Política Corporativa de Privacidade de Dados

Código de conduta

*As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.*

## 11. HISTÓRICO DE REVISÕES

| Versão | Data | Descrição alteração | Responsável |
|---|---|---|---|
| 1 | 23/12/2020 | Criação do documento, baseado nas políticas PL 248, PL 103 e PL 023. | Bruna Omizzolo Lazzarotto |
| 1 | 04/02/2022 | Atualização do documento (responsabilidades áreas) | Priscila Morais |
| 2 | 29/12/2022 | Atualização do documento (documentos de referência) | Priscila Morais e Indiara da Silva |
| 3 | 15/12/2023 | Adequação de modelo e revisão do documento | Bruna Camargo e Raquel Oliveira |
| 4 | 09/12/2024 | Atualização do documento (documentos de referência); Ajuste cadeia de valor (título); Inclusão do segundo tópico do item 7.7; Inclusão da SX Negócios como abrangência; Inclusão do terceiro tópico no item 7.3; exclusão do item 7.9 Representa da Direção no Tratamento de Reclamações; Inclusão de indicadores de monitoramento; Inclusão no tópico de compromissos a necessidade de atuar sobre os fornecedores críticos para o sistema de gestão ; Inclusão da política de reclamações nos documentos de referência | Priscila Morais, Bruna Camrgo e Raquel Oliveira |
| 5 | 03/12/2025 | Adequação de modelo e revisão do documento. Atualização do responsável pelo Comitê de Satisfação de Clientes, Nome das áreas de RH (COE's); Item 3, alterado nome SX para pulse, item 10, atualizado nome dos documentos; | Priscila Morais, Bruna Camargo e Raquel Oliveira |

*As informações contidas neste documento são classificadas de acordo com seu conteúdo e protegidas por sigilo profissional.*