Classificação da Informação: (x) Pública ( ) Interno ( ) Restrita ( ) Confidencial

1. OBJETIVO

Publicar para fornecedores, clientes, parceiros de negócio e entidades externas interessadas as diretrizes definidas pela Getnet para garantir a confidencialidade, a disponibilidade e a integridade dos dados, informações e sistemas de informação utilizados, através de controles tecnológicos e de recursos humanos capacitados para prevenir, detectar e reduzir vulnerabilidades que possam gerar incidentes de segurança da informação.

Tornar pública as diretrizes definidas pela Getnet para identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações.

2. DOCUMENTOS DE REFERENCIA

Artigos 9º, 10º e 15º da Lei 12.865, de 9 de outubro de 2013.

Artigo 14º da Resolução 4.282, de 4 de novembro de 2013.

Resolução 4.658 do Banco Central, de 26 de abril de 2018.

Circular 3.909 do Banco Central, de 16 de agosto de 2018.

Lei 13.709 de 14 de agosto de 2018.

Política de Segurança da Informação da Getnet

ABNT NBR ISO/IEC 27001:2013

ABNT NBR ISO/IEC 27002:2013

PCI-DSS Requirements and Security Assessment Procedures - Versão 3.2.1

Política de Privacidade da Getnet

3. DEFINIÇÕES

Hardening: processo para configuração segura de ativos tecnológicos.

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

Classificação da Informação: (x) Pública ( ) Interno ( ) Restrita ( ) Confidencial

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.

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.

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

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

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

4. DIRETRIZES

4.1. A Getnet possui procedimentos internos para mapear, gerenciar e controlar os riscos de segurança da informação onde precisam ser realizados no ambiente de responsabilidade do fornecedor / parceiro de negócio.

4.2. Garantir que todas as responsabilidades pela segurança da informação nos ambientes de terceiros estejam claramente definidas e que as pessoas indicadas são competentes e capazes de cumprir com as atribuições pela segurança da informação.

4.3. 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.

4.4. A Getnet implementa diretrizes específicas para a proteção das informações e espera que seus clientes e parceiros tenham o mesmo cuidado e responsabilidade ao assunto tais como:

a) Políticas e procedimentos internos para a implementação de *hardening* em todos os seus ativos tecnológicos.
b) Procedimento para identificar vulnerabilidades técnicas, bem como definições para a implementação de correções dentro de prazos definidos.
c) Políticas e procedimentos para o uso de controles tecnológicos para a proteção da rede e de seus ativos.
d) Políticas e procedimentos que definem o uso de tecnologias críticas.
e) Políticas para a definição de controle dos acessos físicos e lógicos.
f) Políticas e procedimentos que definem o manuseio e proteção das cópias de segurança.
g) Garantir e proteger os processos críticos de negócio contra falhas ou desastres significativos.
h) Registrar, analisar, investigar e tratar os incidentes de segurança da informação, criando mecanismos de prevenção para evitar a sua ocorrência.

4.5. Os Clientes, terceiros ou fornecedores da Getnet precisam garantir que, pelo menos anualmente, testes de continuidade dos serviços de pagamento, prevendo indisponibilidade destes serviços por incidentes.

4.6. Seguir procedimentos operacionais diários de segurança da informação.

4.7. Obter definições específicas para o gerenciamento de incidentes de segurança da informação.

a) As notificações de incidentes de segurança da informação por fornecedores, clientes e público externo devem ser realizadas através do e-mail público csirt@getnet.com.br.

b) Os incidentes que são notificados para a Getnet são investigados e classificados. Uma vez que confirmados pela Getnet os incidentes são tratados de acordo com procedimentos internos de tratamento e gerenciamento de incidentes de segurança da informação.

c) O procedimento de gestão de incidentes de segurança da informação é aprovado pelo Comitê de Segurança da Informação da Getnet.

4.8. A Getnet possui política que definem diretrizes para o desenvolvimento seguro de suas aplicações e seus parceiros e clientes devem seguir de acordo com a necessidade e escopo de suas atividades.

4.9. Os fornecedores, clientes e terceiros que a Getnet julgar necessário, devem possuir uma política para classificar as suas informações de acordo com a sua criticidade ao negócio.

4.10. Os terceiros ou qualquer tipo de entidade externa a Getnet precisam implementar mecanismos para a prevenção da perda de informações.

4.11. A partir a sua data de publicação a Política de Segurança Cibernética é revisada pelo menos anualmente.

4.12. Fornecedores e entidades externas a Getnet precisam possuir políticas e procedimentos específicos para a execução e avaliação de riscos quanto necessário e aplicável pela Getnet.

4.13. Fornecedores precisam possuir políticas e procedimentos que definem a implementação de controles criptográficos em dados considerados sensíveis pela Getnet.

4.14. Fábricas de Software e/ou qualquer tipo de entidade externa a Getnet precisam atender aos requisitos de desenvolvimento de sistemas baseando-se nas melhores práticas do mercado de forma segura

4.15. Qualquer fornecedor ou entidade que seja responsável por algum escopo que contenha informações consideradas sensíveis pela Getnet precisarão criar, manter e aprovar procedimentos para gerenciar os acessos de terceiros a essas informações.

4.16. Garantir que qualquer fornecedor, cliente, terceiro ou entidade externa, assinem um contrato de confidencialidade para garantir que as informações que serão acessadas não serão divulgadas.

Classificação da Informação: (x) Pública ( ) Interno ( ) Restrita ( ) Confidencial

5. CONTROLE DE REVISÕES

Revisão nº	Data da Revisão	Descrição da Revisão
1	02/10/2019	Criação do Documento.
2	24/08/2020	Revisão e atualização da documentação.
3	12/11/2020	Revisão e inserção de novos requisitos