GUIDANCE
SEGURANÇA CIBERNÉTICA E RESPOSTA À INCIDENTES CIBERNÉTICOS

EXTRATO A SER ENCAMINHADO AOS FORNECEDORES E PRESTADORES DE SERVIÇOS DO CITI BRASIL

PROPRIETÁRIO:
DIRETOR ESTATUTÁRIO DE SEGURANÇA CIBERNÉTICA – EDSON PEREIRA

CONTATO(S):
ROLF HENRIQUE NEUBARTH

DATA DE PUBLICAÇÃO:
FEVEREIRO /2020

DATA DE REVISÃO:
SETEMBRO /2023

VERSÃO: 2.0

ÍNDICE

1 VISÃO GERAL

1.1 OBJETIVO

Este documento tem por objetivo estabelecer os padrões necessários para segurança cibernética e o plano de resposta à incidentes cibernéticos a serem observados pelo conglomerado Prudencial Citibank Brasil (Citi Brasil).

A segurança da informação é uma questão de gestão de risco do negócio. A falha em proteger as informações do Citi Brasil poderia resultar em prejuízo financeiro e ter um impacto negativo na marca. As normas de segurança da informação do Citi Brasil identificam requisitos de proteção para garantir que as informações sejam protegidas de acordo com os requisitos legais e regulatórios.

1.2 ALCANCE

Este documento destina-se ao Citi Brasil.

1.3 PÚBLICO-ALVO

Este documento destina-se a todos os colaboradores do Citi Brasil.

1.4 RESPONSÁVEL

Este documento é de responsabilidade do Diretor de Segurança Cibernética do Citi Brasil. Qualquer alteração no mesmo, deve ser aprovada pelo Diretor de Segurança Cibernética do Citi Brasil.

1.5 DATA DE EFETIVIDADE / PERÍODO DE TRANSIÇÃO

Esta Política tem efeito imediato.

1.6 PROCESSO DE EXCEÇÃO

É de responsabilidade da Diretoria do Citi Brasil autorizar, quando necessário, exceções à política presente.

2 PROCEDIMENTOS E CONTROLES VOLTADOS A SEGURANÇA DA INFORMAÇÃO

Os programas de segurança da informação do Citi Brasil oferecem uma visão holística do risco de Segurança da Informação em toda a organização e, trabalhando em estreita parceria com as áreas de negócios, com foco na redução ativa deste risco.

Os programas de SI também estabelecem padrões e políticas para avaliar, gerenciar e mitigar os riscos associados a informações, sistemas, redes e desenvolvimento de aplicativos do Citi Brasil, incluindo o estabelecimento de controles em torno da transferência, armazenamento e acesso à dados do cliente.

Com este objetivo, o Citi Brasil estabeleceu os seguintes procedimentos e controles:

a) Programa de Avaliação de Vulnerabilidades
b) Gestão de Vulnerabilidades Técnicas
c) Proteção de Dados
d) Classificação das Informações
e) Controles Contra Malwares (Softwares Maliciosos)
f) Registro de Eventos – Registro de Trilhas de Auditoria
g) Segregação de Redes
h) Controle de Acesso Físico
i) Registro do Usuário e Cancelamento do Registro
j) Provisionamento de Acesso ao Usuário
k) Gestão de Direitos de Acesso Privilegiados
l) Revisão dos Direitos de Acesso aos Usuários
m) Retirada ou Ajuste dos Direitos de Acesso
n) Uso de Informações Secretas de Autenticação?
o) Procedimentos de Logon Seguro
p) Sistema de Gestão de Senhas
q) Dados em Repouso
r) Monitoramento de E-mail
s) Transferência de Arquivos e Dados, incluindo:
    a. Tratamento de Ativos
    b. Gestão de Mídia Removível
t) Criptografia, Gerenciamento de Chaves e Certificados Digitais

u) Gestão de Dados Sensíveis
v) Avaliação de Riscos de Segurança da Informação
w) Autenticação Multifator / Detecção de Atividade Suspeita
x) Ambiente de Desenvolvimento Seguro (quando aplicável)
y) Procedimentos e Controles voltados à empresas prestadoras de serviço

3.1 AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO EM TERCEIROS

O processo de avaliação de riscos de terceiros (TP-RAP) fornece uma metodologia estruturada e objetiva para identificar os riscos inerentes a um relacionamento com terceiros e determinar os controles necessários.

Para todos os terceiros dentro do escopo da Avaliação de Segurança em Fornecedores (TPISA), a avaliação deve ser concluída no prazo determinado de acordo com o nível de classificação de risco de segurança da informação do terceiro, da forma definida pelo processo em questão.

Para o Citi manter a segurança apropriada das informações e dos sistemas que são acessados, processados, armazenados ou gerenciados por terceiros, as categorias mínimas que o terceiro deverá ser avaliado, de acordo com a natureza do serviço prestado, são:

1. Políticas e normas de segurança da informação
2. Identificação e autenticação
3. Autorização e controles de acesso
4. Confidencialidade e integridade
5. Detecção e resposta a incidentes
6. Administração
7. Treinamento e conscientização
8. Infraestrutura e plataformas do processo principal
9. Desenvolvimento de Software
10. Gestão da continuidade do negócio
11. Segurança física
12. Quarteirizados / subcontratatados
13. Aspectos Legais e Conformidade
14. Midias Eletronica Transportaveis - ETM
15. Web Hosting
16. Cloud Computing

3.2 Prevenção e Tratamento dos Incidentes por Empresas Prestadoras de Serviços

Os requisitos especificados no processo de TPISA são aplicáveis a todos os terceiros externos que armazenam, processam, gerenciam ou acessam informações do Citi Brasil classificadas como confidenciais ou com classificação superior e/ou que hospedam um aplicativo da internet com a marca Citibank, independentemente de seu escopo de serviços, nível de classificação de risco de terceiros, infraestrutura ou gasto anual.

Este processo permite que o Citi Brasil identifique, avalie e reporte os níveis de risco e controles de segurança da informação, continuidade de negócios, segurança física e resposta a incidentes de um prestador de serviços.

3.3 Plano de Ação e Resposta a Incidentes e Definição de um Incidente de Segurança

Um incidente de Segurança da Informação é um evento que compromete ou ameaça a confidencialidade, integridade ou disponibilidade de informações confidenciais ou de classificação superior, pertencentes ou gerenciados pelo Citi Brasil, ou dados que o Citi Brasil tem obrigação de proteger, ou sistemas de informação armazenando tais dados; independentemente de como, quem (funcionário/provedor de serviço ou parceiro do Citi Brasil), ou onde (dentro e fora de um prédio do Citi Brasil) em que o incidente ocorreu. Isso inclui, não limitado a, alteração, destruição, divulgação, perda, roubo, ou mal-uso destes dados ou sistemas, dispositivos, ou mídia física ou eletrônica. Isso pode também incluir ativos expostos ao público, assim como qualquer vazamento de dados PII (informação de identificação pessoal/dado pessoal), que provavelmente irá resultar em alto risco aos direitos e liberdade de pessoas naturais, onde tais direitos e liberdade são definidos pelas leis e regulamentações locais.

3.4 Responsabilidades e Procedimentos

Sempre que um evento de segurança atender à definição acima, o mesmo deverá ser informado ao Citi Brasil.

3.5 ETAPAS DO PROCESSO DE RESPOSTA A INCIDENTES

Os incidentes devem ter, no mínimo, as seguintes etapas:

a) Identificação do incidente;

b) Registro do incidente;

c) Time para tratamento de incidentes;

d) Revisão (Triagem);

e) Processo de Investigação;

f) Processo de Notificação ao Citi Brasil;

g) Processo de Encerramento;

h) Revisão Pós-Fato;

i) Fechamento;

j) Revisão de Qualidade (QA).

4 Conscientização de Segurança da Informação, Instrução e Treinamento

O Citi Brasil anualmente distribui materiais de conscientização de Segurança da Informação para todas as áreas internas, que abrangem temas específicos da política de segurança, tais como catalogação das informações, mensagens eletrônicas, controles contra malware, entre outros.

Adicionalmente por política global são requeridos a realização dos seguintes treinamentos aos novos funcionários, bem como periodicamente para renovação:

- Segurança da Informação e Segurança Cibernética.
- Atualização Anual em Segurança da Informação.

5 CONTINUIDADE DE NEGÓCIOS

O Citi Brasil mantém planos de continuidade de negócios para minimizar perdas financeiras e responder às necessidades do mercado e dos clientes no evento de qualquer desastre, crise, interrupção ou emergência natural ou provocada pelo homem. O Citi Brasil deve estar preparado para responder a qualquer evento que possa afetar operações normais de negócios. Se aplicável, os planos de continuidade devem conter os seguintes elementos ou, senão, indicar que o elemento não é aplicável: Tempo de recuperação (Recovery Time Objectives, RTO) e ponto de recuperação (Recovery Point Objectives, RPO), procedimentos de recuperação, soluções alternativas manuais a serem empregadas quando a tecnologia não estiver disponível, requisitos de locais e recursos de recuperação, plano de alocação de pessoal para os locais de recuperação (incluindo equipe de recuperação de negócios e tecnologia), informações de contato do Citi Brasil (p. ex., contatos, níveis de serviço contratado), informações do subcontratado, informações do aplicativo, procedimentos para voltar ao local de trabalho primário, listas de chamada, procedimentos de chamada e listas de armazenamento fora do local.

6 GESTÃO DE FORNECEDORES

O Citi possui política de gerenciamento de terceiros (TPM) que envolve o monitoramento e gerenciamento de riscos associados com o uso de terceiros internos e externos que fornecem produtos e serviços para o Citi. O processo é realizado através da formalização do ciclo de vida de gestão de terceiros, são eles:

i) Planejamento

ii) Due Diligence

iii) Contratação

iv) Monitoramento

v) Encerramento.

Cada fase apresenta requisitos diferentes para identificar, mitigar e / ou escalar os riscos associados ao relacionamento com terceiros, dependendo do tipo e do nível de risco envolvido. As normas estabelecem os requisitos para cada uma das fases do ciclo de vida.

APÊNDICE A: GLOSSÁRIO

CoB: Continuity of Business

CTO: Chief Technology Officer

DoA: Denial of Access

DoS: Denial of Service

PII: Personally Identifiable Information

TPISA: Third Party Information Security Assessment

TPM: Third Party Management

TP-RAP: Third-Party Risk Assessment Process

RTO: Recovery Time Objectives

RPO: Recovery Point Objectives