Política

Segurança Cibernética

Definição:

A Finalidade dessa política é a de municiar a CHG_MERIDIAN de procedimentos para preservação das propriedades da informação, sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Escopo:

Produto Afetado: Operação de Arrendamento Mercantil

Responsáveis:

Controladoria
Compliance
TI

ÍNDICE

Feito:	Aprovado:	Aprovado:	Data:
Moisés Moura Analista de Controladoria	Luiz Nali Diretor Financeiro	Roberto Mussalem Diretor Presidente	30 de abril de 2019

1. Introdução

A Resolução 4.658/18 do Banco Central do Brasil dispõe sobre a política de segurança cibernética e sobre requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, e contém especificações de como a segurança da informação e segurança cibernética devem ser observadas pela instituição. A CHG-MERIDIAN estabelece as diretrizes para compor um programa completo e consistente de segurança de informação e riscos cibernéticos, visando proteger o valor e a reputação da empresa, garantindo confidencialidade, integridade e disponibilidade das informações da companhia.

2. Objetivo

Definir critérios para orientar os colaboradores da CHG-MERIDIAN, clientes, fornecedores e parceiros de negócios sobre as diretrizes e políticas referentes às melhores práticas a serem adotadas para garantir a segurança da informação e segurança cibernética, em conformidade com a legislação e regulamentação vigentes e normas internas.

3. Conceitos

A segurança cibernética, constitui-se da preservação das propriedades da informação, sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

3.1 Confidencialidade: Garantia de que a informação é acessível somente pelas pessoas autorizadas.

3.2 Integridade: Salvaguarda de exatidão da informação e dos métodos de processamento.

3.3 Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3.4 Riscos cibernéticos: Riscos de ataques cibernéticos oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da companhia, causando danos financeiros e de reputação consideráveis.

3.4.1. Malwares:

- **Vírus:** Software que causa danos à máquina, rede, softwares e banco de dados;
- **Cavalo de troia:** Aparece dentro de outro software e cria uma porta para a invasão do computador;
- **Spyware:** Software malicioso para coletar e monitorar o uso de informações;
- **Ransomware:** Software malicioso de que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

3.4.2. Engenharia Social:

- **Pharming:** Direciona o usuário para um site fraudulento, sem o seu conhecimento;
- **Phising:** Links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- **Vishing:** Simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas tenta obter informações confidenciais;
- **Smishing:** Simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

3.4.3. Acesso pessoal: Pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

3.4.4. Fraudes externas e invasões: Realização de operações fraudulentas, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades especificas em uma ambiente cibernético.

3.4.5. Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso à serviços e sistemas da instituição. No caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar ou enviar SPAM ou Virus, ou inundar uma rede com mensagens resultando na negação dos serviços.

4. Princípios

A proteção e privacidade de dados dos clientes refletem os valores da CHG-MERIDIAN e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de proteção de dados:

- São coletadas de forma ética e legal, para os propósitos específicos e devidamente informados;
- Somente serão acessados por pessoas autorizadas e capacitadas para o seu uso adequado;
- Poderão ser disponibilizadas a empresas contratadas para a prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

5. Diretrizes corporativas

Conforme estipulado no Art. 15º da Resolução 4.658/18 do BACEN. Referente aos pontos a serem observados para a contratação de serviços relevantes de processamento de dados em nuvem, a CHG-MERIDIAN dispõe para o desenvolvimento de suas atividades um ambiente tecnológico desenvolvido e fornecido por sua matriz situada na Alemanha denominado CHG-Cloud®. Todo gerenciamento de risco cibernético desta estrutura é realizada pela própria matriz

e através de um contrato a nível de serviço, a solução é firmada entre filial e matriz, sem a possibilidade de rescisão contratual.

6. Estrutura de gerenciamento e medidas de segurança

O gerenciamento de procedimentos e controles de segurança cibernética são realizados pela matriz na Alemanha e objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela política de segurança cibernética.

Os seguintes pontos descrevem as medidas técnico-organizacionais implementadas pela CHG-MERIDIAN.

6.1 Gestão de acessos às informações

O controle de acesso inclui medidas desenvolvidas para prevenir que pessoas não autorizadas acessem as dependências de onde os dados pessoais estão sendo processados. Estes acessos são controlados, monitorados e restringidos à menor permissão e privilégios possíveis. Pessoas não autorizadas devem se dirigir a recepção e aguardar um funcionário da CHG-MERIDIAN para acompanha-lo às dependências da empresa.

O controle de acesso ao sistema de processamento de dados em nuvem estão protegidos contra o acesso não autorizado através de um domínio e diretório ativo correspondente a um nome de usuário e senha. A política de senhas está de acordo com protocolos de segurança bastante rigorosos incluindo complexidade, comprimento e mudança. Após um período definido sem acesso a senha é expirada e o usuário bloqueado automaticamente. O acesso ao CHG-cloud® se dá através do navegador de internet, com domínio especifico. Aqui a autenticação de dois fatores é utilizada, que consiste em um nome de usuário, uma senha de domínio e dispositivo RSA Token.

6.2 Proteção de dados

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança da infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações.

A CHG-MERIDIAN assegura que a autorização de usuários somente permite acessar dados cobertos por sua autorização de acesso. Essas autorizações de acessos são regulamentadas nos conceitos de autorização da CHG-MERIDIAN onde são revisadas regularmente. Adicionalmente o requerimento de proteção é determinado e reavaliado de forma regular, fazendo isso, a confidencialidade da informação é classificada como seguinte:

- C1: Informação publicamente acessível;
- C2: Informação interna;
- C3: Informação confidencial;
- C4: Informações estritamente confidenciais.

De acordo com os requisitos de proteção determinados, as medidas de proteção adequadas são implementada, como por exemplo:

- Registro de acesso de leitura;
- Registro de outros acessos;
- Armazenamento, retenção e descarte adequado de dados e portadores de dados;
- Três linhas de defesa: O monitoramento das autorizações pelo departamento competente é incorporado ao processo;
- Três linhas de defesa: Revisão das permissões por auditoria interna;

6.3 Pseudonimização

o processamento de dados pessoais é feito de tal forma que os dados não possam mais ser atribuídos a uma pessoa afetada específica sem o recurso a informações adicionais, desde que essas informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais apropriadas.

Na medida em que os dados pessoais não precisam ser processados em texto simples, eles são anonimizados ou pseudonimizados.

6.4 Medidas para assegurar que dados coletados para diferentes propósitos possam ser processados separadamente.

Dados coletados para propósitos diferentes são processados e armazenados separadamente. A CHG-MERIDIAN dispõe de ambientes diferentes para o processamento dos dados, sendo estes – desenvolvimento, teste e produção. Como sempre, nos ambientes de desenvolvimento e teste, trechos dos dados reais são processados exclusivamente para os propósitos do teste. As autorizações atribuídas podem ser rastreadas via conceito de autorização. O círculo de colaboradores que tem autorização para coletar dados para este propósito é limitado.

6.4.1.Integridade dos dados (Item VII e VIII, Art. 6º CAPÍTULO I Lei 13.709/18)

As atividades de tratamento de dados devem observar a boa-fé dos princípios de segurança e prevenção.

Medidas para garantir que os dados pessoais não possam ser lidos, copiados, modificados ou apagados quando estiverem sendo transferidos por sigilo ou quando estiverem sendo transportados ou salvos para transportadores de dados, e que os locais para os quais os dados pessoais serão transferidos por meio de equipamentos de transferência de dados possam ser verificados e determinados.

A princípio, todos os transportadores de dados podem ser encriptados. Dependendo do requerimento de proteção, e-mails também podem ser encriptados. Isto se aplica para ambas as informações internas e informações externas, além disso mídias de armazenamentos, como pen-drive, podem ser encriptados se caso for requerido a proteção para o transporte de dados.

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação São identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores da CHG-MERIDIAN são treinados periodicamente sobre os conceitos de segurança da informação, através de um programa efetivo de conscientização.

6.5 Continuidade de Negócios.

O processo de gestão de continuidade de negócios relativo à segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação. Após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os teste previstos para os cenários de ataques cibernéticos.

6.5.1. Plano de respostas à incidentes.

A fim de detectar e lidar com incidentes de segurança, um processo de gerenciamento de incidentes é implementado, o que garante o processamento estruturado e a derivação de medidas para melhoria contínua. Obrigações de relato em relação às autoridades e partes afetadas também são revisadas e, se necessário, comunicadas ao cliente. O agente de segurança da informação, o responsável pela proteção de dados e o gerente de segurança de TI estão envolvidos no processamento, a fim de derivar as medidas apropriadas de acordo com a CIP.

7. Processamento, armazenamento de dados e computação em nuvem

Conforme prevê a Resolução 4.658/18 do Banco Central do Brasil. Na contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, as instituições financeiras devem adotar procedimentos que contemplem a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e os riscos a que estejam expostos, assim como a verificação da capacidade do potencial prestador de serviço de assegurar tais pontos. Neste caso a CHG-MERIDIAN através de um contrato a nível de serviço utiliza computação em nuvem fornecida por sua Matriz na Alemanha, este contrato não é passível de rescisão, logo os riscos inerentes à gestão de contratos de serviços de computação em nuvem, é baixo.

Atendendo aos requisitos da Resolução 4.658, o serviço ofertado pela Matriz atende aos seguintes pontos:

- o cumprimento da legislação e da regulamentação em vigor, incluindo a Resolução 4658;
- o acesso da instituição contratante aos dados processados ou armazenados pelo prestador de serviço;
- a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados processados ou armazenados pelo prestador de serviço;
- o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados, incluindo relatórios de auditoria independente;
- a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;
- a qualidade dos controles de acesso voltados à proteção dos dados dos clientes da instituição

8. Conclusão

O gerenciamento de procedimentos e controles de segurança cibernética são realizados pela matriz na Alemanha e objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela política de segurança cibernética.

Com isso, a empresa preserva as informações, confidencialmente e integralmente disponibilizando e permitindo o uso e o compartilhamento da informação de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques em conformidade com a legislação e regulamentação vigentes de normas internas.

A CHG-MERIDIAN assegura que a autorização de usuários somente permite acessar dados cobertos por sua autorização de acesso. Todas as informações compartilhadas estão disponíveis ao Banco Central do Brasil.