GRUPO SINOSSERRA
DESDE 1947

Política de Segurança Cibernética

SUMÁRIO

1. OBJETIVO

Esta Política tem como objetivo formalizar as diretrizes de segurança cibernética do Grupo Sinosserra, visando à proteção dos ativos de informação de modo seguro e transparente e de forma compatível com o porte, o perfil de risco, o modelo de negócio e sensibilidade dos dados e das informações sob responsabilidade das empresas do Grupo Sinosserra.

2. ABRANGÊNCIA

A Política de Segurança Cibernética se aplica a todos os diretores, colaboradores, parceiros de negócios, fornecedores e prestadores de serviços relevantes das empresas do Grupo Sinosserra.

3. DEFINIÇÕES

3.1 Segurança Cibernética: conjunto de estratégias, políticas e padrões voltados à mitigação do risco cibernético.

3.2 Risco Cibernético: possibilidade de ocorrência de perdas resultantes do comprometimento da confidencialidade, integridade ou disponibilidade de dados e informações em suporte digital, em decorrência da sua manipulação indevida ou de danos a equipamentos e sistemas utilizados para seu armazenamento, processamento ou transmissão.

3.3 Serviços Relevantes de Processamento ou Armazenamento de Dados: São aqueles prestados no âmbito dos processos de negócio imprescindíveis para a geração de receita.

3.4 Incidentes Relevantes: eventos adversos, decorrentes ou não de atividade maliciosa, que, conforme parâmetros definidos pela supervisionada, comprometam substancialmente: (i) a confidencialidade, integridade ou disponibilidade de dados relevantes; ou (ii) serviços relevantes de processamento ou armazenamento de dados.

3.5 Computação em Nuvem: serviço que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação, provisionados com esforços mínimos de gestão ou de interação com o prestador de serviços.

3.6 Confidencialidade: limitação do acesso à informação, sendo permitido o acesso somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessário o acesso, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.

3.7 Disponibilidade: garantia de acesso das pessoas devidamente autorizadas à informação sempre que o acesso for necessário, prevenindo interrupções das operações da Instituição por meio de um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

3.8 Autenticidade: garante a veracidade da autoria da informação, porém, não garante a veracidade do conteúdo da informação. A autenticidade garante a veracidade do autor, de quem de fato produziu aquela informação, não importando se o conteúdo é verdadeiro ou falso. Não-Repúdio: A autenticidade garante também um subproduto, que é o não-repúdio. O Não-Repúdio está contido na autenticidade e significa que o autor da informação não tem como recusar que ele é o verdadeiro autor, ou seja, o não-repúdio é a incapacidade da negação da autoria da informação.

3.9 Integridade: garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por uma pessoa não autorizada e impedindo alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

3.10 Negação de serviço: Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

3.11 Fraudes Externas e Invasões: Realização de operações por fraudadores, com o uso de conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

4. DIRETRIZES

As diretrizes traçadas pela Diretoria que sintetizam os compromissos assumidos pelas empresas do Grupo Sinosserra, são:

As diretrizes traçadas pela Diretoria que sintetizam os compromissos assumidos pelas empresas do Grupo Sinosserra, são:

a) Tratar de forma ética e sigilosa, de acordo com as leis vigentes e normas internas, as informações das empresas do Grupo Sinosserra, dos colaboradores, dos clientes e dos parceiros de negócios, evitando-se o acesso indevido, modificações, destruição ou divulgação não autorizada;

b) Prover a adequada classificação da informação, considerando os critérios de confidencialidade, integridade e disponibilidade;

c) Garantir que as informações e os dados sejam utilizados de forma transparente e apenas para as finalidades para as quais foram coletadas;

d) Assegurar que os colaboradores tenham acesso somente as informações necessárias para o exercício de atividades;

e) Atender às leis que regulamentam as atividades do Grupo Sinosserra e seu mercado de atuação;

f) Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;

g) Garantir a continuidade do processamento das informações críticas de negócios;

h) Reportar à área de Segurança da Informação os riscos às informações, bem como eventuais fatos ou ocorrências que possam colocar em risco tais informações;

i) Manter estrutura organizacional adequada para garantir a qualidade e a efetividade da segurança da informação;

j) Prever que os procedimentos e os controles voltados a segurança cibernética devem abranger a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;

k) Estabelecer o uso de senhas fortes para acesso aos sistemas. As senhas devem ser pessoais e intransferíveis, sendo proibido seu compartilhamento.

5. PROCEDIMENTOS E CONTROLES ADOTADOS PARA REDUZIR A VULNERABILIDADE A INCIDENTES DE SEGURANÇA

O Grupo Sinosserra tem como objetivo principal garantir a segurança das informações confidenciais e sensíveis, evitando a exposição a incidentes de

segurança cibernética. Para alcançar esse objetivo devem ser adotados os seguintes procedimentos e controles:

a) Implementação de políticas de senha seguras, que incluem o uso de senhas fortes, alterações regulares de senha e autenticação de dois fatores, sempre que possível;

b) Atualização regular de softwares, sistemas operacionais, antivírus e firewalls, para evitar vulnerabilidades conhecidas e possíveis ataques de malware;

c) Implementação de restrições de acesso, com base nas funções e necessidades do trabalho de cada usuário, a fim de garantir que somente as pessoas autorizadas tenham acesso aos dados;

d) Realização de testes regulares de segurança e avaliações de vulnerabilidades para identificar e corrigir quaisquer vulnerabilidades encontradas.

6. CÓPIAS DE SEGURANÇA (BACKUP)

O Grupo Sinosserra deve manter cópias de segurança dos dados mantidos em sistema e na rede. Deve ser elaborada documentação apropriada sobre os procedimentos de restauração da informação.

7. CONTROLES VOLTADOS PARA A RASTREABILIDADE DA INFORMAÇÃO

Para garantir a rastreabilidade da informação, o Grupo Sinosserra adotará os seguintes controles:

a) Identificação e autenticação dos usuários;

b) Os logs de eventos devem ser ativados para registrar todas as atividades do sistema, permitindo o rastreamento de todas as atividades realizadas pelos usuários e administradores;

c) Controle de acesso a informações críticas.

8. PROCEDIMENTOS PARA REGISTRO, ANÁLISE DE CAUSA E IMPACTO DE INCIDENTES RELEVANTES

O Grupo Sinosserra entende que incidentes de segurança cibernética podem ocorrer, mesmo com a implementação de controles e procedimentos. Para lidar com incidentes relevantes serão adotados os seguintes procedimentos:

a) Registro imediato de incidentes, a fim de iniciar a análise e avaliação do impacto do incidente;

b) Análise de causa raiz para identificar como o incidente ocorreu e como evitar futuros incidentes semelhantes;

c) Avaliação do impacto do incidente, incluindo o impacto na confidencialidade, integridade e disponibilidade das informações;

d) Implementação de medidas corretivas para prevenir incidentes semelhantes no futuro;

e) Notificação às partes interessadas, conforme necessário.

9. DIRETRIZES PARA ELABORAÇÃO DE TESTES DE CONTINUIDADE DE NEGÓCIOS

O Grupo Sinosserra reconhece a importância da continuidade dos negócios em caso de incidentes de segurança cibernética. Para garantir a continuidade dos negócios devem ser adotadas as seguintes premissas:

a) Elaboração de planos de continuidade de negócios, que incluem a identificação de processos críticos, a definição de alternativas de trabalho e a recuperação de dados em caso de perda;

b) Realização de testes regulares de continuidade de negócios para identificar e corrigir possíveis vulnerabilidades;

c) Avaliação dos resultados do teste e implementação de melhorias, conforme necessário.

10. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES

As informações sobre incidentes relevantes devem ser compartilhadas com as partes interessadas incluindo quando aplicável, os titulares de dados pessoais, o Banco Central do Brasil (Bacen), a Superintendência de Seguros Privados (SUSEP), as demais instituições financeiras e do mercado segurador. O objetivo do compartilhamento de informações é melhorar a resposta a incidentes de segurança e reduzir a vulnerabilidade geral do setor financeiro.

11. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

As contratações de serviços de terceiros para o processamento e armazenamento de dados e de computação em nuvem devem seguir todos os requisitos de segurança, avaliando a relevância do serviço contratado, criticidade e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciados pelo serviço.

Todos os prestadores deste tipo de serviço contratados pelas empresas do Grupo Sinosserra devem ter avaliadas a sua capacidade e conformidade com a regulamentação em vigor: padrões mínimos de segurança, certificações (se aplicável), critérios de qualidade desejados, confidencialidade, integridade, disponibilidade e capacidade de recuperação. Estes prestadores devem garantir

o acesso do Grupo Sinosserra, sempre que solicitado, aos seus relatórios de auditoria e as evidências dos controles de identificação e segregação dos dados.

A contratação e alterações contratuais de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pela:

a) Sinosserra Financeira e Sinosserra Consórcios ao Banco Central do Brasil no prazo de até 10 dias após a formalização dos contratos. No caso da inexistência de um convênio entre o Banco Central e as autoridades supervisoras dos países onde os serviços poderão ser prestados deve ser solicitada a autorização para uso do serviço diretamente com o Banco Central com no mínimo 60 dias de antecedência;

b) Aplicap Capitalização à Susep, em até 30 dias após a formalização dos contratos.

12. ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A estrutura de gestão da segurança da informação está constituída em uma unidade única, que atende as empresas do Grupo Sinosserra e se reporta ao Diretor responsável pela Segurança Cibernética da Sinosserra Financeira e da Sinosserra Consórcios. O gerenciamento centralizado resulta em maior agilidade e assertividade na tomada de decisões.

13. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Os incidentes de segurança ou a suspeita deles devem ser informados no Formulário de relato de incidentes: https://sinosserra-privacy.my.onetrust.com/incident-portal/webforms/f4dcef9a-9072-4fcd-9a0c-a6e44720ffcf/671f20fc-87b9-427d-badb-7961c90a0f36

14. PENALIDADES

Qualquer violação as diretrizes e controles internos estabelecidos nesta Política e normas correlatas resultará na aplicação de medidas disciplinares apropriadas, podendo, inclusive, levar à aplicação de advertências, dispensa do colaborador por justa causa, rescisão contratual imediata do parceiro de negócios, sem prejuízo de providências legais cabíveis, tais como comunicação aos órgãos de polícia e de fiscalização, e tomada de medidas judiciais e administrativas para responsabilização e ressarcimento de todo e qualquer dano que possa ser causado.