zema | FINANCEIRA

POLÍTICA SEGURANÇA DA INFORMAÇÃO

VERSÃO 01

Data de Edição: Novembro/2019

1. OBJETIVO

A Política Corporativa de Segurança da Informação (PSI) é a incorporação lógica dos requisitos de negócio da empresa para segurança e controle. Objetiva estabelecer instruções e diretrizes para assegurar a integridade, confidencialidade e disponibilidade das informações e sistemas

2. ESCOPO

Esta política abrange todas as informações, os sistema e recursos de Tecnologia da Informação Zema Crédito, Financiamento e Investimento S/A, designada neste documento como Empresa, suas filiais e subsidiárias; incluindo também seus colaboradores, estagiários, terceirizados, temporários e fornecedores em quaisquer das dependências da Empresa ou locais onde estes se façam presentes através da utilização, manuseio ou processamento das informações.

3. RESPONSABILIDADES

3.1 Diretoria de Operações

Responsável pela Gestão de Segurança da Informação (SGSI – Sistema de Gestão de Segurança da Informação) bem como por estabelecer, manter, publicar e divulgar as políticas de segurança, padrões e procedimentos. A continuidade do negócio também é responsabilidade da Diretoria de Operações envolvendo a análise de riscos e definição de estratégias para mitigar os riscos.

3.2 Tecnologia da Informação (TI)

Responsável pela operação, manutenção dos serviços de segurança, a investigação de intrusão em sistemas e outros incidentes de segurança da informação.

3.3 Auditoria Interna

Responsável por garantir o bom andamento do processo de gestão de SI, bem como a aderência de todas as áreas da Empresa a esta Política, através da publicação mensal de indicadores, realização de auditorias internas e/ou externas anualmente.

3.4 Área de Negócios

Devem assegurar que contratos com clientes, fornecedores e parceiros de negócio possuam cláusulas de Segurança da Informação que assegurem a proteção das informações e recursos de TI. Um Termo de Confidencialidade deve ser assinado entre as partes antes do início de serviços e projetos que envolvam informações sensíveis, sendo responsabilidade da área contratante a garantia de que as cláusulas e termo de confidencialidade estão presentes durante e após a negociação.

3.5 Área de Riscos

Gerenciar os riscos relacionados à Segurança da Informação, comunicar possíveis alterações no cenário e impactos imediatos, bem como apresentá-los trimestralmente a Diretoria de Operações e manter registros das decisões aplicadas. Realização de análise de vulnerabilidades e testes de invasão periódicos deve ser prática de responsabilidade da área SI, informada e acompanhada pela área de Auditoria Interna.

3.6 Colaboradores da Empresa

Devem familiarizar-se, aderir e praticar as políticas contidas na PSI, bem como procedimentos e padrões relacionados à Segurança da Informação. Todos os colaboradores têm a obrigação de tratar estas informações como sigilosas, sob pena de sansões, punições, processos cíveis e criminais no rigor da lei.

3.7 Recursos Humanos

Responsável por informar sobre os requisitos de Segurança da Informação aos possíveis candidatos a vagas de emprego da Empresa mesmo antes de se concretizar a contratação, bem como apoiar e garantir os processos de educação e conscientização em Segurança da Informação durante o ciclo de vida do colaborador na Empresa.

3.8 Comitê de Gestão de Privacidade e Segurança da Informação

Deve avaliar e revisar o estado corrente da Gestão de Privacidade e Segurança da Informação na Empresa, aprovar novas ou modificar políticas de segurança, privacidade e deliberar sobre outras questões de alto-nível relacionadas às atividades de Gestão da Segurança da Informação.

3.9 Alta Direção da Empresa

Deve supervisionar e garantir recursos para a eficácia do Comitê de Gestão de Privacidade e Segurança da Informação.

4. CLASSIFICAÇÃO DA INFORMAÇÃO:

Para assegurar que a informação receba um nível adequado de proteção e de acordo com sua importância, a Empresa estabelece três categorias para responsabilidades associadas à informação e seu manuseio. Pelo menos uma das categorias aplica-se para cada colaborador, cliente, fornecedor e/ou parceiro enquanto durar a relação contratual ou trabalhista. A saber: Proprietário, Custodiante e Usuário da Informação.

5. RECURSOS DE TECNOLOGIA

5.1 Uso de Software

O uso de software é regulamentado por legislação específica e qualquer ato que a contrarie pode ser punido com os rigores da lei. É PROIBIDA a instalação de software não licenciado.

É responsabilidade da área de TI manter uma linha base com registro de software necessários ao desempenho das funções dos usuários.

É vedada ao colaborador, a instalação e/ ou remoção de softwares nos equipamentos da Empresa, salvo através de autorização formal da equipe de Tecnologia da Informação. Todos os programas e documentos criados ou providos pelos funcionários em benefício da empresa são considerados propriedade da mesma

5.2 Uso de Hardware

Todos os servidores e estações de trabalho devem ser obrigatoriamente associados aos domínios de controle definidos pela área de Tecnologia da Informação. É vedada a utilização de estações de trabalho que não estejam associadas a algum domínio de responsabilidade da Empresa; salvo em condições previamente aprovadas pela área de TI.

Os colaboradores/terceiros não devem utilizar computadores e periféricos pessoais, tais como discos externos, roteadores wireless, pendrive e impressoras, bem como software pessoal nas redes da Empresa, salvo com autorização prévia da equipe de Segurança da Informação.

É vedada a instalação de hardware sem prévia aprovação da área de Tecnologia da Informação e /ou projeto previamente aprovado.

5.3 Acesso Remoto

O acesso remoto para terceiros só pode ser feito por intermédio de projeto específico da área de Tecnologia da Informação, considerando que terão acesso controlado e apenas aos recursos e serviços de TI necessários para o exercício da atividade contratada.

O acesso remoto para colaboradores só pode ser realizado através de protocolos seguros e por meio de plataformas homologadas e validadas pela área de TI. É responsabilidade da área de TI disponibilizar, gerenciar e monitorar os acessos remotos

5.4 Internet, E-mail, Redes Sociais

- Internet
  - A *Empresa* reserva-se o direito de bloquear acesso a sites de conteúdo ilícito, sexo, atividades *hacker* e outros, sem aviso prévio e de forma automática.
  - A *Empresa* armazena os registros de navegação na Internet e poderá monitorá-los para avaliar atividades ilícitas, possíveis fraudes, comportamentos impróprios ao exercício da função definida em contrato de trabalho, bem como gerar estatísticas de uso e desempenho visando aprimorar seus serviços internos e externos

- E-mail
  - Colaboradores da *Empresa* que possuem contas de e-mail associadas ao desempenho de suas funções, devem utilizá-la somente para fins específicos desta função.
  - Contas de e-mail de uso pessoal não podem ser utilizadas para envio e recebimento de informações da *Empresa.*
  - Não é permitido o uso do sistema de e-mail, cujos domínios pertencem a *Empresa*, ou aqueles administrados pela mesma, para o repasse conteúdo inadequado ao ambiente corporativo e ou que possa trazer instabilidade de relacionamento pessoal e queda desempenho nos recursos de Tecnologia da Informação.

- Redes Sociais
  - ➢ É vedada aos colaboradores a publicação de informações em qualquer rede social, salvo por área devidamente autorizada pela Empresa. Mesmo as áreas autorizadas devem ter especial atenção ao conteúdo, bem como a classificação da informação a qual para ser divulgada deverá previamente ser classificada como PÚBLICO (rótulo). Um processo de revisão e aprovação da comunicação deve ser devidamente registrado pelas áreas autorizadas

6. CONTROLE DE ACESSO LÓGICO E FÍSICO

Todo colaborador, cliente, fornecedor e terceiros deve possuir uma única identificação de usuário (User IDs, ou logon) e senha(s) (password) relacionada às suas atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço.

É proibido o empréstimo e compartilhamento de identificação de usuários e senhas associadas a qualquer tipo acesso às informações, sistemas e equipamentos da Empresa.

7. MALWARE

Toda estação de trabalho e servidor deve possuir software antivírus instalado e atualizado automaticamente. É responsabilidade da área de Tecnologia da Informação assegurar o processo de controle de malware na Empresa.

O uso de dispositivos do tipo “mídia removível” (pendrives) deve ser previamente autorizado formalmente e controles de segurança da informação devem ser empregados pela área de TI coibindo o uso não autorizado

8. CRIPTOGRAFIA

As comunicações e transferências de informações entre a Empresa, clientes, instituições financeiras, parceiros e fornecedores estratégicos devem ser realizadas através de redes privadas (VPN) utilizando-se de esquemas criptográficos previamente avaliados e aprovados pela área de Tecnologia da Informação.

9. CÓPIAS DE SEGURANÇA E CONTIGÊNCIA

Todas as informações críticas de negócio da Empresa têm que possuir cópia de segurança (backup) realizada de acordo com planejamento associado a criticidade da informação para o negócio.

10. DESENVOLVIMENTO DE SOFTWARE

O processo de desenvolvimento e aquisição de novos sistemas deve considerar as melhores práticas de segurança da informação. Estas práticas devem ser atualizadas, discutidas e disseminadas na Empresa. É responsabilidade da área de Tecnologia da Informação garantir a disseminação e aplicação de melhores práticas para desenvolvimento seguro.

11. SEGURANÇA CIBERNÉTICA

É responsabilidade da área de TI em conjunto com a área de Risco determinar as possíveis ameaças, definir e adotar medidas de proteção tais como a contratação de links seguros, serviços de gestão de conteúdo e etc.

12. CONFORMIDADE

A conformidade com requisitos legais e contratuais é responsabilidade de todos os colaboradores da Empresa. Os gestores devem identificar e observar a legislação aplicável à Empresa, garantindo a adequação contratual e observância das diretrizes de Segurança da Informação desta Política.

Em especial os requisitos da Lei Geral de Proteção de Dados (LGPD 13709/2018) devem ser observados por todos os colaboradores visando preservar a privacidade do Titular dos Dados pessoais. A confidencialidade e sigilo de Dados Pessoais devem ser observados, preservados e garantidos por todos os colaboradores da Empresa. A área de TI é responsável por propiciar mecanismos de proteção condizentes com a criticidade da informação e requerer estes aspectos de provedores de serviços e sistemas. Suspeitas de violação de Dados Pessoais devem ser comunicadas ao superior imediato e/ou através de contato com a ouvidoria (0800 095 6702) e/ou envio de e-mail para privacy@zemafinanceira.com

A contratação de serviços de terceiros para tratamento de informações da Empresa que caracterizem processamento e armazenamento em nuvem, deve considerar os requisitos de adequação a legislação e regulação vigentes, em especial aos requisitos da Resolução 4658 BACEN (Banco Central do Brasil).

13. DISPOSIÇÕES GERAIS

O prazo de atualização desta Política é de 01 (um) ano ou em data anterior, caso necessário.

14. DIVULGAÇÃO

Esta versão deve ser utilizada para publicação nos veículos de comunicação externa da Zema Financeira, alinhada com a Política de Segurança da Informação oficial interna.

15. APROVAÇÃO

_____	_____
Juliano Antonio de Oliveira	José Joaquim de Oliveira Junior
Diretor de Riscos e Compliance	Diretor Adm. / Financeiro

_____

Maria Virginia Gomes Moreira

Diretora Comercial