ELABORAÇÃO	**Gestor de Compliance SINICON**	[Tatiane Ollé]	**DATA DE ELABORAÇÃO**	[08/09/2020]
APROVAÇÃO	Conselho de Ética	[Alexandre Olmacht, Eduardo Staino, Guilherme Luna, Luiz Felipe Seabra, Maria Ximena Rocha, Patrícia Moreira, Silvia Lacerda]	**DATA DE APROVAÇÃO**	

1. Introdução

A Política de Segurança da Informação é uma declaração formal do SINICON a respeito do seu compromisso com a proteção dos ativos de informação de sua propriedade ou sob sua guarda. Deve, portanto, ser cumprida pelo Conselho Diretor, Colaboradores e Terceiros que tenham acesso a dados ou informações do SINICON, de alguma forma.

Esta Política de Segurança da Informação foi elaborada pelo Conselho de Ética do SINICON, de acordo com a legislação vigente, realidade e requisitos de negócio da entidade.

2. Objetivos

O propósito desta Política de Segurança da Informação é permitir que o Conselho Diretor, colaboradores e terceiros sigam padrões de comportamento relacionado à segurança da informação e estabelecer as diretrizes aplicáveis ao uso, tratamento, controle e proteção das informações do SINICON, contemplando os seguintes objetivos específicos:

- Definir o escopo da segurança da informação do SINICON;
- Orientar todas as ações de segurança da informação da entidade, para reduzir riscos e garantir a integridade, confidencialidade e disponibilidade da informação para as empresas associadas, colaboradores e terceiros;
- Servir de referência para auditorias, apuração e avaliação de responsabilidades;
- Definir as responsabilidades na gestão da segurança da informação;
- Definir as responsabilidades do Conselho Diretor, Colaboradores e Terceiros na preservação da segurança da informação.

3. Definições

Os termos e definições a seguir são importantes para a compreensão desta Política de Segurança da Informação:

a) Segurança da Informação ou SI:

A informação é um ativo do SINICON, ou seja, é um bem que possui valor e, portanto, deve ser protegida, independentemente de ser escrita ou impressa em papel,

armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. A segurança da informação é alcançada através da preservação da: Confidencialidade, Integridade, Autenticidade e Disponibilidade da informação e diz respeito ao conjunto de tecnologias disponíveis para a defesa dos sistemas de informação e rede de computadores, tendo como objetivo prevenir invasão, roubo ou destruição dos dados.

b) Confidencialidade:

É a garantia de sigilo, ou seja, a informação é acessível somente a pessoas autorizadas, que por sua vez, garantem a guarda dessas informações, não as transmitindo para indivíduos que não necessitem recebê-las. .

c) Integridade:

É a garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida, consiste na fidedignidade da informação, demonstrando a conformidade dos dados.

d) Autenticidade:

É a garantia da veracidade da fonte das informações.

e) Disponibilidade:

É a garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos, sempre que necessário.

f) Informação sensível ou crítica:

Toda e qualquer informação cujo comprometimento possa causar perda de vantagem competitiva, dano ou prejuízo ao negócio ou à imagem da organização.

g) Recursos de Tecnologia da Informação (TI):

Referem-se a qualquer sistema de armazenamento ou processamento da informação, serviço ou infraestrutura, ou às instalações físicas que os abriguem, tais como: pen drives, smartphones, tablets, e-mail, planilhas, documentos, computadores, notebooks, netbooks, equipamentos de rede, dentre outros.

h) Vírus e software malicioso:

Entende-se por vírus qualquer programa de computador que tem a capacidade de se reproduzir automaticamente, sem o conhecimento ou autorização do usuário. Entende-se por software malicioso qualquer software que realiza ações nocivas aos sistemas, como vírus, cavalo de Tróia, verme (worm) e afins.

i) Ameaça:

Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

j) Incidente de segurança da informação:

Evento ou série de eventos indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. Uma ameaça que se concretiza gera um incidente.

k) Vulnerabilidade:

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

4. Escopo

Esta Política de Segurança da Informação aplica-se ao Conselho Diretor do SINICON, Colaboradores e Terceiros.

Objetiva orientar o Conselho Diretor, colaboradores e terceiros do SINICON a exercer suas atividades dentro das melhores práticas de segurança da informação.

5. Papéis e responsabilidades

O Conselho Diretor do SINICON, Colaboradores e Terceiros que possuem relações com o SINICON, têm responsabilidade sobre a informação que acessam e manipulam.

A responsabilidade pelo cumprimento de cada regra desta Política de Segurança da Informação independe da existência de controles que, de forma total ou parcial, obriguem este cumprimento.

5.1. Coordenador de Segurança da Informação

O Coordenador de Segurança da Informação será designado através de decisão do Presidente do Conselho Diretor ou Presidente Executivo do SINICON, sendo o principal responsável pelas iniciativas de segurança. As responsabilidades do Coordenador são:

a) Fornecer o embasamento técnico necessário ao Gestor de *Compliance* do SINICON, para apoiar a tomada de decisão;

b) Coordenar a implantação dos controles e processos de segurança da informação aprovados pelo Conselho Diretor ou Presidente Executivo;

c) Identificar fragilidades e exposição da informação e dos recursos de processamento da informação a ameaças significativas e propor medidas protetivas;

d) Manter registro de incidentes e fragilidades de segurança da informação para apresentação periódica ao Presidente do Conselho Diretor ou Presidente Executivo do SINICON;

e) Coordenar ações emergenciais de segurança com o prestador de serviço de tecnologia da informação;

f) Realizar com o prestador de serviço de tecnologia da informação, periodicamente, análise crítica independente da segurança da informação, podendo considerar inclusive auditorias realizadas, para avaliar a efetividade desta Política de Segurança da Informação e dos controles de segurança da informação adotados.

g) Alertar o Conselho Diretor, Conselho de Ética, Colaboradores e Terceiros sobre ameaças e concretizações de eventos de pishing ou outros tipos de tentativa de violação da segurança das informações, mitigando riscos.

h) Promover a disseminação das diretrizes da Segurança da Informação, através de capacitação e treinamento, presenciais ou virtuais, contendo ensinamentos sobre confidencialidade, integridade e disponibilidade da informação.

5.2. Conselho Diretor, Colaboradores e Terceiros

O Conselho Diretor, Conselho de Ética, Colaboradores e Terceiros com acesso às informações corporativas têm como responsabilidades:

a) Cumprir as determinações desta Política de Segurança da Informação, suas respectivas normas e procedimentos;

b) Proteger a informação contra acesso não autorizado, divulgação, modificação, destruição ou interferência, em todo o seu ciclo de vida;

c) Notificar, com a maior brevidade possível, quaisquer incidentes, fragilidades ou falhas de segurança, e mau funcionamento de hardware ou software ao Coordenador de Segurança da Informação.

6. Pessoal

As pessoas, seu conhecimento, competências e habilidades possuem valor como ativos organizacionais. As medidas a seguir são necessárias para proteger este valor e disseminar a cultura de Segurança da Informação pelo SINICON:

a) Termo de Aceite da Política de Segurança da Informação:

O Termo de Aceite das políticas do SINICON, que inclui a Política de Segurança da Informação deve ser assinado por todos os colaboradores e terceiros do SINICON, devendo passar a constar, inclusive, como documento do processo de admissão.

Além disso, os contratos assinados com terceiros devem conter cláusula que trate da proteção das informações, bem como incluir a presente Política como um dos anexos, de forma que os contratados declarem conhecer o documento. Os contratos em vigor devem ser aditados em até 90 (noventa) dias após a publicação dessa política.

b) Obrigação de Confidencialidade:

Todos os colaboradores e terceiros do SINICON terão incluídos nos contratos clausula de confidencialidade.

O Acordo de Confidencialidade valerá durante todo o período do vínculo dos colaboradores e terceiros com o SINICON e adicionalmente terá duração de 5 (cinco) anos após o término deste vínculo. Em casos específicos, o prazo de validade do Acordo de Confidencialidade obedecerá a regulamentação que orienta a atividade específica, como: saúde, educação, propriedade intelectual, dentre outras.

c) Processos disciplinares:

Violações a esta Política de Segurança da Informação serão analisadas pelo Gestor de Compliance, conforme a natureza, gravidade e impacto causado, sempre com o apoio do Coordenador de Segurança da Informação. Sempre que houver alguma infração a política o Conselho de Ética deverá ser envolvido no processo de análise.

Uma violação pode sujeitar aos colaboradores e terceiros do SINICON às penalidades previstas no Código de Conduta e Ética do SINICON.

Os Terceiros também poderão ser responsabilizados por perdas e danos decorrentes do descumprimento desta Política de Segurança da Informação.

7. Uso aceitável de recursos de Tecnologia da Informação

Os recursos de Tecnologia da Informação são ativos que apoiam cada vez mais os usuários na realização de suas atividades. Estes recursos armazenam ou processam as informações do SINICON e devem ser tratados conforme as diretrizes a seguir:

a) A utilização de recursos de processamento de informação (estações de trabalho, notebooks, netbooks, tablets, smartphones, dentre outros) particulares ou de terceiros na rede do SINICON deve observar os seguintes pontos:

- Para acesso restrito à Internet: é permitido, respeitando-se as regras definidas nesta Política de Segurança da Informação;
- Para acesso a dados: é proibido. Se necessário, exceções devem ser autorizadas pelo gerente da área demandante, desde que sejam adotados os mecanismos de segurança homologados pelo SINICON.

Recursos de processamento de informação fornecidos pelo SINICON só podem ser usados pela sua força de trabalho, respeitando o perfil de acesso de cada atribuição de trabalho.

b) Trabalho remoto:

O acesso remoto de todos os colaboradores e terceiros do SINICON aos recursos e informações corporativas a partir da Internet, deve observar os seguintes pontos:

- Acesso ao correio eletrônico via webmail ou pelo celular é permitido e automaticamente criptografado;
- Acesso a dados é permitido, desde que seja autorizado pelo gerente da área demandante e com criptografia;
- Deve ser feito a partir de computadores fornecidos pelo SINICON. Acesso ao servidor do SINICON a partir de computadores particulares somente pode ser feito quando adotados os mecanismos de segurança homologados pelo SINICON. Acesso a partir de computadores públicos (fornecidos por LAN Houses, Cybercafés, etc.) ou de terceiros não homologados pelo SINICON não são permitidos;
- Se necessário, pode ser realizado a partir de locais públicos (shoppings centers, hotéis, aeroportos, aviões, dentre outros). Os usuários devem atentar para as responsabilidades que assumem quanto à segurança dos computadores utilizados e ter cautela com a exposição de informações sensíveis expostas em tela.

O acesso remoto dos colaboradores e terceiros do SINICON pode ser monitorado ou auditado para apuração de um ato administrativo ou evento de segurança da informação, mediante justificativa e aprovação do Conselho Diretor ou Diretor Executivo.

O acesso remoto deve ser imediatamente revogado ao término do vínculo de trabalho com o SINICON. Neste caso, os equipamentos de propriedade do SINICON deverão ser devolvidos antes da homologação do desligamento.

c) Uso de correio eletrônico (e-mail):

O correio eletrônico corporativo, com endereço @sinicon.org.br, deve ser tratado pelos colaboradores e terceiros como correspondência oficial da organização e ser utilizado exclusivamente para trabalho. Adicionalmente, devem ser observados os seguintes pontos:

- Pode ser monitorado ou auditado para apuração de um ato administrativo, evento de segurança da informação ou por necessidade de cobertura de ausência do proprietário da caixa postal, mediante justificativa e aprovação do Conselho Diretor ou Diretor Executivo.
- Deve incluir obrigatoriamente "*Disclaimer*" (aviso, normalmente colocado no rodapé das mensagens) produzido pela assessoria de comunicação e aprovado pelo Conselho de Ética.
- Recomenda-se o uso de criptografia e assinatura digital em e-mails que contenham informações ou dados sensíveis.
- O acesso a e-mails não corporativos é permitido. Cada colaborador e terceiro é responsável pelo uso e deve, portanto, adotar bom senso, atentar para as questões relacionadas à segurança das informações, minimizando riscos e evitando perda de produtividade.
- E-mails não corporativos não podem ser usados para envio ou recebimento de mensagens relacionadas ao trabalho, exceto em caso de indisponibilidade do e-mail corporativo, formalmente notificada pela Gerência de TI, e para mensagens urgentes.

d) Outros meios de comunicação eletrônica (WhatsApp, Teams, Zoom, Messenger, etc.):

Conforme orientação do responsável de segurança da informação do SINICON. Adicionalmente, devem ser observados os seguintes pontos:

- Cada colaborador e terceiro é responsável pelo uso e deve, portanto, adotar bom senso, atentar para as questões relacionadas à segurança das informações, minimizando riscos e evitando perda de produtividade;
- O uso pode ser monitorado ou auditado para apuração de um ato administrativo ou evento de segurança da informação, mediante justificativa e aprovação do Conselho Diretor ou Diretor Executivo;
- O acesso pode ser bloqueado por solicitação expressa do superior imediato ou por impacto no ambiente operacional, mediante justificativa e aprovação do Conselho Diretor ou Diretor Executivo.

e) Acesso à Internet:

O acesso à Internet deve ser utilizado exclusivamente para trabalho. Adicionalmente, devem ser observados os seguintes pontos:

- Pode ser monitorado ou auditado para apuração de um ato administrativo ou evento de segurança da informação, mediante justificativa e aprovação do Conselho Diretor ou Diretor Executivo;
- Existe controle de acesso baseado nas categorias de sites. Não são permitidos

acessos a categorias de sites consideradas ilegais ou impróprias, que oferecem riscos à segurança da informação ou apresentem alto consumo de banda, conforme exemplos mostrados nas Tabelas 1, 2 e 3, respectivamente;

Tabela 1 – Categorias de sites consideradas ilegais ou impróprias	
Categoria de site	Descrição
Ilegal ou antiético	Sites que apresentam informações, métodos ou instruções sobre ações fraudulentas ou condutas ilegais, tais como fraudes, falsificação, evasão fiscal, furtos, chantagem, etc.
Racismo e ódio	Sites que discriminam grupos ou indivíduos por raça, cor, etnia, orientação sexual, etc.

Tabela 2 – Categorias de sites que oferecem risco à segurança da informação	
Categoria de site	Descrição
Contorno de Proxy	Sites que fornecem informações ou ferramentas sobre como contornar os controles de acesso à Internet e navegar pela Web anonimamente, incluindo os servidores de proxy anônimos.
Hacking	Sites que retratam as atividades ilícitas em torno da modificação não autorizada ou o acesso aos programas, computadores, equipamentos e outros sites.

Tabela 3 – Categorias de sites que apresentam alto consumo de banda	
Categoria de site	Descrição
Internet, TV e Rádio	Sites que difundem comunicações de rádio ou TV através da Internet.
Telefonia via Internet	Sites que permitem Comunicações Telefônicas através da Internet.
Multimídia	Sites que permitem o download de arquivos MP3 ou multimídia.

- O acesso a sites relacionados às categorias mostradas na Tabela 3 pode ser liberado, por solicitação do gerente da área demandante e autorização da Gerência de TI, após avaliação de viabilidade técnica e desde que para fins exclusivamente de interesse da entidade;
- O acesso a sites relacionados a redes sociais (Facebook, Google+, Twitter,

LinkedIn, Wordpress, Blogger ou similares) é permitido. Cada colaborador e terceiro é responsável pelo uso e deve, portanto, adotar cautela, atentar para as questões relacionadas à segurança das informações, minimizando riscos e evitando perda de produtividade. É proibido postar ou expressar informações ou opiniões pessoais em nome do SINICON sem a devida autorização. Informações que já foram publicadas podem ser compartilhadas;

- O uso de softwares de compartilhamentos de arquivos Peer-to-peer (eMule, Kazaa, Ares Galaxy, BitTorrent ou similares) é proibido, sem exceção. É não permitir usuários instalarem qualquer aplicativo. Os programas que sejam necessários deverão ser solicitados ao setor responsável e instalado pela área de TI.

f) Outros recursos de processamento e armazenamento da informação:

Recursos de processamento de informação fornecidos pelo SINICON devem ser usados prioritariamente para trabalho.

Estações de trabalho, notebooks, netbooks, smartphones, impressoras, copiadoras, telefones fixos e celulares devem ser usados para fins de trabalho. Cada colaborador e terceiro é responsável pelo uso e deve, portanto, adotar bom senso, atentar para as questões relacionadas à segurança das informações, minimizando riscos e evitando perda de produtividade.

8. Controles operacionais

Os controles de segurança apresentados a seguir são básicos e essenciais para a proteção das informações do SINICON. Estas diretrizes devem, portanto, ser observadas e respeitadas:

a) Antivírus:

O SINICON deve possuir software antivírus apropriado, para proteção contra vírus e software malicioso. O software antivírus deve estar instalado e mantido devidamente atualizado em todas as estações de trabalho dos usuários, servidores, notebooks e netbooks. Todo e-mail recebido ou enviado deve ser verificado pelo software antivírus, assim como todo o acesso à Internet.

b) Mídias removíveis:

O uso de mídias removíveis (mídias regraváveis, gravadores ópticos, discos rígidos externos, pen drives, cartões de memória ou similares) é permitido. Os usuários devem atentar para as responsabilidades que assumem quanto à segurança das informações armazenadas nestes dispositivos.

c) Backup de dados corporativos e armazenamento de dados pessoais:

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática. Dados e informações corporativas devem ser armazenados em servidores disponibilizados pelo SINICON, incluindo arquivos

de pastas particulares contendo e-mails corporativos. A empresa contratada pelo SINICON para a área de TI é responsável pelo backup exclusivamente dos dados armazenados nos servidores.

O armazenamento de dados particulares nos servidores do SINICON não é permitido.

d) Manutenção e alienação de equipamentos:

Equipamentos de processamento de informação em garantia devem ser enviados para os respectivos fabricantes para manutenção quando necessário. Apenas a equipe de TI pode realizar intervenção de manutenção em equipamentos sem garantia.

e) Uso de senhas:

O acesso a recursos de processamento de informação do SINICON, especificamente estações de trabalho e sistemas, exige autenticação dos usuários através de senha. A senha é pessoal e intransferível. Cada colaborador e terceiro do SINICON é responsável pela confidencialidade de sua senha. O descumprimento desta norma é considerado violação desta Política de Segurança da Informação.

Os colaboradores e terceiros do SINICON devem trocar periodicamente sua senha, por questões de segurança.

f) Retirada e transporte de equipamentos e notebooks ou similares:

Recomenda-se que dispositivos móveis como notebooks, netbooks, tablets ou similares sejam transportados em local seguro, a exemplo do porta-malas do carro, para minimizar o risco de roubos durante o trânsito.

g) Segmentação de rede:

Por questões de segurança e preservação de desempenho, a infraestrutura de rede do SINICON está segmentada. Cabe ao Gestor de *Compliance* avaliar e propor segmentação da rede corporativa, de acordo com o perfil e necessidade dos usuários.

h) Equipamentos de usuários sem monitoração:

Os usuários devem bloquear seus computadores contra acesso não autorizado quando se ausentarem de suas estações de trabalho ou notebooks. O proprietário da senha é responsável por eventuais ações realizadas em decorrência do não bloqueio. Os computadores deverão ser desligados ao final do expediente.

Notebooks, netbooks, tablets, smartphones, celulares ou similares não devem ser deixados desacompanhados em lugares públicos como shoppings centers, hotéis, auditórios, restaurantes, salas de reunião, aeroportos, dentre outros.

9. Propriedade Intelectual

O respeito à propriedade intelectual está intimamente relacionado ao negócio do SINICON.

As seguintes diretrizes devem ser observadas e respeitadas:

- O SINICON adquire e utiliza softwares em conformidade com a legislação vigente.
- A instalação de softwares deve ser realizada exclusivamente pela equipe de TI, conforme a necessidade de uso.

- A Gerência Administrativa Financeira é responsável pelo controle de licenças dos softwares.
- Os colaboradores e terceiros do SINICON são obrigados a respeitar o uso legal de propriedade intelectual de terceiros, incluindo livros, artigos, filmes, áudio, imagens, ou qualquer outro conteúdo sujeito à legislação de propriedade intelectual.
- Qualquer trabalho desenvolvido pelos colaboradores e terceiros pertence ao SINICON, exceto em negociações específicas aprovadas pelo Conselho Diretor ou Diretor Executivo.

10. Disposições finais

A Segurança da Informação é um fator crítico para a continuidade do negócio. O sucesso desta Política de Segurança da Informação está intimamente relacionado ao compromisso de todos no SINICON em realizar suas atividades do cotidiano conforme as diretrizes estabelecidas.

Esta Política de Segurança da Informação estará constantemente disponível no servidor do SINICON, para consultas a qualquer colaborador e terceiros.

O Gestor de *Compliance* e o Coordenador de Segurança da Informação estarão à disposição para o esclarecimento de dúvidas, quando necessário.