POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO PSIC

Emissão: 23/05/2023	Revisor: Gabriela Gomes Elias	Edição: 1.1

SCORE POSITIVO SOLUÇÕES COMERCIAIS LTDA, inscrita no CNPJ sob o nº 40.903.090/0001-45, com sede e na cidade e Comarca de São Paulo/SP, Rua Maestro Cardim, 1.293, Conj. 72, CEP 01323-000, e-mail: *atendimento@scorepositivo.net.br*, *a* seguir denominada de **SCORE POSITIVO** ou empresa, estabelece sua Política de Segurança da Informação e Comunicação (PSIC) em complementariedade ao Código de Ética, Condutas, Procedimentos e Controles Internos.

1. Conceitos:

1.1. Código de Ética, Condutas, Procedimentos e Controles Internos: documento estabelece os princípios, conceitos, valores, regras e normas de procedimento da **SCORE POSITIVO** e de todos aqueles que possuam cargo, função, relação diretiva, empregatícia, comercial, profissional, contratual ou de confiança.

1.2. Compliance de Risco: instituída no código de ética, tem por finalidade assessorar a implementação das ações relacionadas à PSIC definidas neste instrumento.

1.3. Confidencialidade: garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados.

1.4. Credencial de acesso: identificação do colaborador ou terceirizado em ambientes lógicos, sendo composta por seu nome de usuário (*login*) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, *token* e biometria.

1.5. Gestores: diretores e conselheiros.

1.6. Disponibilidade: garantia de que as informações e os recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e autorizados.

1.7. Informação: conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

1.8. Integridade: garantia de que as informações estejam fidedignas em relação à última alteração durante o seu ciclo de vida.

1.9. Legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento jurídico atual.

1.10. Recurso: que tenha valor material ou imaterial, sendo tangível ou intangível, para a **SCORE POSITIVO** e precisa ser adequadamente protegido.

1.11. Recurso Intangível: elemento que possui valor para a **SCORE POSITIVO** e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando a dados, reputação, imagem, marca e conhecimento.

1.12. Recurso Tangível: caracteriza-se por possuir um corpo físico.

1.13. Repositórios Digitais: plataformas de armazenamento em nuvem, a exemplo, mas não se limitando ao Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd.

1.14. Risco: combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

1.15. Sigilo profissional: manutenção de segredo para informação valiosa, cujo domínio de divulgação deva ser fechado, ou seja, restrito a um cliente, a uma organização ou a um grupo, uma vez que a ele é confiada a manipulação da informação.

1.16. Tentativa de Burla: qualquer ato que busque violar as diretrizes estabelecidas nos documentos normativos da **SCORE POSITIVO**.

1.17. Terceiro: prestador de serviço, terceirizado, fornecedor, credenciado, consultor, instrutor, distribuidor, representante comercial ou parceiro.

1.18. Violação: atividade que desrespeite as regras estabelecidas nos documentos normativos da **SCORE POSITIVO**.

2. Objetivo:

2.1. Esta PSIC tem por objetivo complementar o Código de Ética, Condutas, Procedimentos e Controles Internos da empresa, definindo princípios e diretrizes específicas que visam a preservação da segurança da informação da empresa dentro de diretrizes básicas de confidencialidade, disponibilidade, integridade, autenticidade, legalidade dos processos que amparam sua operação, além de estabelecer regras claras de responsabilidades e limites de atuação dos gestores, colaboradores e terceiros em relação à segurança da informação e comunicação.

2.2. Todas as regras aqui estabelecidas devem ser aplicadas aos clientes, estagiários, aprendizes, líderes, executivos, diretores, sócios e conselho administrativo, colaboradores, parceiros, doravante denominados usuários, no que se refere à proteção da informação e uso de recursos tecnológicos da **SCORE POSITIVO**.

2.3. Esta PSIC e seus documentos complementares devem ser interpretados de forma suplementar ao Código de Ética, Condutas, Procedimentos e Controles Internos; havendo divergência, este prevalece.

3. São Princípios Gerais:

a) Preservar e proteger as informações sob a responsabilidade da **SCORE POSITIVO**, inclusive as contidas nos recursos de Tecnologia da Informação e Comunicação (TIC), dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato.

b) Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

c) Assegurar a confidencialidade, para garantir que o acesso à informação seja obtido apenas por pessoas autorizadas

d) Assegurar a integridade, para garantir a exatidão e plenitude da informação e dos métodos de seu processamento, bem como da transparência no tratamento com o público envolvido.

e) Assegurar a disponibilidade, para garantir que as pessoas autorizadas tenham acesso à informação, sempre que necessário.

f) Assegurar a autenticidade, assim como a legalidade no desenvolvimento das atividades do negócio.

g) Cumprir a legislação a que se obriga e demais instrumentos regulamentares relacionados às suas atividades, inclusive dos bancos de dados ("fonte"), utilizadas na prestação de serviços no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

4. Divulgação e Declaração de Responsabilidade

4.1. Esta PSIC deve ser de conhecimento de todos e será divulgada da seguinte forma:

a) Por meio digital, através de envio de e-mail coorporativo;

b) Disponibilizada no site do **SCORE POSITIVO**;

c) Via campanha de Segurança da Informação;

c) Via treinamento pessoal específico da segurança da informação.

4.2. Esta PSIC deve estar disponível em local de acesso dos clientes, funcionário e colaboradores.

4.3. Esta PSIC deverá ser protegida contra alterações.

4.4. Todos os clientes internos, temporários, aprendizes, estagiários, líderes, executivos, diretores, sócios, além de prestadores de serviços, parceiros e fornecedores que realizem qualquer forma de acesso ou manipulação das informações ou utilizem recursos tecnológicos da **SCORE POSITIVO** devem aderir formalmente ao "Termo de Confidencialidade e Ciência da Política de Segurança da Informação" comprometendo-se a agir de acordo com a Política e Normas de segurança da informação, além do Código de Ética e Conduta da **SCORE POSITIVO**.

4.5. Quando houver novos gestores, colaboradores e terceiros da **SCORE POSITIVO**, estes deverão ter conhecimento deste PSIC aderindo aos seus termos.

5. Diretrizes da Segurança da Informação

5.1. Para endereçar todo o esforço e manutenção necessária para a Segurança da Informação, a **SCORE POSITIVO** estabelece as seguintes diretrizes:

a) A Gestão da Segurança da Informação será estabelecida e mantida com apoio da Alta Administração, através de um Sistema de Gestão de Segurança da Informação (SGSI);

b) A informação deverá ser utilizada com senso de responsabilidade e de modo ético e seguro por todos, em benefício exclusivo dos negócios corporativos;

c) Todos os ativos de informação devem ser devidamente identificados, classificados e monitorados;

d) A identificação de cada cliente da **SCORE POSITIVO** é única, pessoal e intransferível;

e) Os riscos identificados deverão ser analisados, classificados e apresentados ao departamento de Gestão da Segurança da Informação, que deliberará sobre o tratamento adequado para tais.

5.2. Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta política o solicitante deverá documentá-las com todas as informações do fato por um documento escrito e comunicá-las imediatamente à área de Segurança da Informação através do endereço de e-mail: *atendimento@scorepositivo.net.br*, para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

6. Gestão de Segurança da Informação

6.1. A fim de manter um nível satisfatório de segurança, o departamento de Gestão da Segurança da Informação adotará as seguintes diretrizes:

a) O controle de acesso dos usuários aos ativos de informação deve ser devidamente controlado e aprovado pelo responsável pela informação (gerência ou, diretoria), a qual o acesso permitirá a manipulação, quer seja para simples consulta ou para alteração;

b) O uso do e-mail sob domínios de propriedade da **SCORE POSITIVO** não será permitido para terceiros, contudo, caso de faça necessário, ocorrerá por tempo determinado pela gerência da área solicitante mediante a assinatura do Termo de responsabilidade. Este tempo poderá ser prorrogado mediante nova solicitação da gerência da área;

c) Cópias de segurança (backup) devem ser realizadas através de mídias específicas para as informações que são consideradas vitais para os sistemas e para a retomada das atividades das áreas, em caso de indisponibilidade;

d) Regras para o desenvolvimento seguro de sistemas e softwares devem ser estabelecidas e aplicadas para os desenvolvimentos realizados dentro da organização;

e) Terceiros somente deverão ter acessos a sistemas legados da empresa quando acompanhados por recurso interno e devidamente autorizados pelo setor competente;

f) As informações devem ser classificadas e manuseadas de acordo com a confidencialidade e as proteções necessárias, da seguinte forma: Pública, Sensível, Privada e Confidencial e devem ser tratadas, armazenadas e descartadas de maneira correta para garantir os aspectos de segurança da informação no negócio da **SCORE POSITIVO** e nas informações dos seus clientes;

g) As responsabilidades de todos quanto à segurança da informação devem ser definidas, seguindo requisitos mínimos de boa conduta e ética;

h) Os ativos tangíveis e intangíveis de informação devem ser identificados de forma individual, inventariados, protegidos e monitorados de acessos indevidos. As mídias devem ser gerenciadas de forma adequada, conforme os requisitos de segurança da informação;

i) Um conjunto de regras para garantir a padronização das técnicas criptográficas deve ser estabelecido, incluindo a aplicação adequada das mesmas e as responsabilidades para manter a segurança no transporte ou armazenamento das informações independente do meio utilizado;

j) Um processo de gestão de mudanças deve estar em vigor para garantir que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, a fim de não ocasionar falhas operacionais ou de segurança no ambiente produtivo da organização;

l) Medidas de segurança devem ser adotadas para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso não autorizado, perda ou dano à informação;
m) Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação (Confidencialidade, Integridade e Disponibilidade);
n) Todos os incidentes que afetem a segurança da informação devem ser reportados à área de Segurança da Informação através do e-mail: *ti@scorepositivo.net.br*. Os técnicos responsáveis analisarão o incidente e tomarão as ações devidas, repassando a tratativa às áreas responsáveis;
o) Todos os incidentes de segurança devem ser reportados para a área de Segurança da Informação, para que sejam analisados, avaliados e tratados pela área responsável;
p) Devem ser definidas regras para garantir que não ocorram violações jurídicas, regulamentares ou contratuais nos requisitos de segurança da informação na organização;
q) Devem ser estipuladas diretrizes para garantir que o acesso físico às instalações onde os ativos de TI e as informações críticas a continuidade do negócio estejam armazenados seja controlado de forma a garantir a sua disponibilidade, integridade e confidencialidade.

7. Monitoramento e Auditoria

7.1. A **SCORE POSITIVO** monitora e registra todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto a empresa mantem controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgou necessário para reduzir os riscos, e reservar-se o direito de:
a) Implantar outros sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônicos, navegação, Internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;
b) Inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta PSI;
c) Instalar outros sistemas de proteção e detecção de invasão para prevenir a segurança das informações e dos perímetros de acesso, levando em consideração normas específicas e contratual de nossos clientes contratantes, e;
d)Instalar câmeras nas instalações físicas, levando em consideração normas específicas e contratual de nossos clientes contratantes.

8. Penalidades

8.1. Para toda e qualquer infração à Política de Segurança da Informação (PSI), às Normas de Segurança da Informação e ao Código de Ética e Conduta, deverá ser aberto um incidente de segurança da informação, tratado de acordo com o Plano de Tratamento de Incidentes de Segurança da Informação e informado ao departamento de Gestão de Segurança da Informação e, por conseguinte, apurada através de procedimentos internos conduzidos pelo departamento de Gestão da Segurança da informação em conjunto com o departamento jurídico da **SCORE POSITIVO**.
8.2. Caso o Comitê de departamento de Gestão de Segurança da Informação julgue cabível, o envolvido poderá, enquanto durar o processo de apuração interna, ser afastado da função ou suspenso.
8.3. Ao cliente interno suspeito de cometer violações à Política e Normas de Segurança da Informação, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração deverá ser aplicada com proporcionalidade à ocorrência com base no Código de Ética e Conduta, Termo de Confidencialidade e Aceite da Política de Segurança da Informação (PSI) e legislações vigentes.
8.4. A **SCORE POSITIVO** se exonera de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus clientes, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis.

9. Revisão e Manutenção

9.1. Esta PSIC deverá ser revisada anualmente ou quando uma mudança significativa ocorrer na organização.
9.2. Informações do Documento:
a) Local de armazenamento do documento: https://scorepositivo.net.br/psic_sa.pdf
b) Responsável pelo Documento: Departamento Jurídico
c) Classificação da Informação: Sensível
9.3. Versões do Documento:

Versão	Data	Editor/Revisor	Comentário
1.0	20/10/2022	Gabriela Gomes Elias	Versão Inicial do Documento
1.1	23/05/2023	Gabriela Gomes Elias	Atualização do Termo de Confidencialidade e Ciência da PSI.

10. Documentos de referência:
a) Código de Ética, Condutas, Procedimentos e Controles Internos da **SCORE POSITIVO**;
b)Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Federal nº. 13.709/2018.

ANEXO I
APROVAÇÃO DO DOCUMENTO PSIC

Nome	Cargo	Assinatura Digital
Anderson Cavalheiro Vecchia	CEO	
Mônia Souza	Diretora Comercial	
Leonardo Lima	CTO	
Rosane	Financeiro	
Gabriela Gomes Elias	DPO	

ANEXO II

TERMO DE CONFIDENCIALIDADE E CONHECIMENTO DA PSIC

Dados do Usuário	
Nome:	
Área/departamento:	Localidade:
Empresa (caso não funcionário):	
CNPJ (caso não funcionário):	

1. Para os devidos fins, declaro que i e entendi o documento chamado "Política de Segurança da Informação e Comunicação PSIC" e comprometo-me em sempre estar atento às atualizações desta Política e das normas que a suportam;
2. Estou ciente que todos os ambientes da **SCORE POSITIVO**, físicos e eletrônicos, como contas de e-mail fornecidas pela empresa, acesso à internet, dispositivos móveis, estão sujeitos a monitoramento para devida proteção e guarda dos ativos da empresa, seja com uso de câmeras com captação de imagem e voz, seja com uso de dispositivos de autenticação de identidade ou *softwares* de segurança da informação, para auditorias físicas e/ou eletrônicas;
3. Assumo o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de minhas funções na **SCORE POSITIVO**, mesmo depois de terminado meu vínculo contratual mantido com a organização;
4. Estou ciente e de acordo que o não cumprimento das condições estabelecidas neste termo poderá culminar no exame da conduta sob o aspecto disciplinar, nos termos previstos no Código de Ética e Conduta da **SCORE POSITIVO**, para reparações de natureza civil e criminal, sem prejuízo da rescisão do contrato de trabalho por justa causa ou rescisão unilateral de contrato, se apurada minha responsabilidade;
5. Declaro neste ato que comunicarei ao Departamento de Segurança da Informação todas as irregularidades porventura ocorridas no uso dos recursos tecnológico e no manuseio de informações, bem como, qualquer suspeita ou ameaça ao sigilo, integridade ou segurança das informações que eu detectar, para que seja providenciada a imediata regularização e averiguação.
6.Por fim, manifesto neste ato minha concordância expressa com todas as cláusulas acima, assinando o presente Termo de Confidencialidade e Ciência da PSI como prova de meu livre e espontâneo aceite.

(Assinatura Digital)