POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Código: POL-088-SI-01

Classificação: Pública

Tipo de documento: Política

Departamento Responsável: Segurança da Informação

Scala Data Centers

Documento para uso na Scala Data Centers. Impressão e/ou reprodução são proibidas sem autorização. Se houver necessidade da cópia, solicitar à área de SGI.

ÍNDICE

1. OBJETIVO 3
2. ABRANGÊNCIA 3
3. DEFINIÇÕES 3
4. DOCUMENTOS DE REFERÊNCIA 3
5. PAPÉIS E RESPONSABILIDADES 4
6. DIRETRIZES 6
6.1 PROPRIEDADE, MONITORAMENTO E CLASSIFICAÇÃO DA INFORMAÇÃO 6
6.2 USO DE RECURSOS 8
6.3 DESCARTE DE INFORMAÇÕES 8
6.4 SEGURANÇA COM FORNECEDORES 8
6.5 CONFORMIDADE COM A LEY MARCO DE CIBERSEGURIDAD (CHILE) 9
6.6 CONFORMIDADE COM O MARCO CIVIL DA INTERNET (BRASIL) 9
6.7 REPORTE DE DESVIOS 10
7. ANEXOS 11
8. REGISTROS 11
9. CONTROLE DE VERSÕES 11
10. LISTA DE DISTRIBUIÇÃO 12

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

1. OBJETIVO

Estabelecer o direcionamento estratégico da Scala para a segurança da informação na empresa, visando mitigar eventuais riscos e danos relacionados às ameaças externas ou internas, deliberadas ou acidentais, que possam impactar a confidencialidade, integridade e disponibilidade das informações de qualquer natureza, para sua preservação.

2. ABRANGÊNCIA

Aplica-se a todos os integrantes, estagiários, conselheiros, diretores (“Colaboradores”) da Scala Data Centers (“Scala Data Centers”, “Scala”, “Companhia”) e aqueles externos que representam ou atuam em nome da Companhia, incluindo prestadores de serviços, fornecedores de materiais ou insumos, consultores e demais terceiros (“Fornecedores”).

3. DEFINIÇÕES

- DPO (Data Protection Officer): também conhecido como Encarregado pelo Tratamento de Dados Pessoais, é o principal responsável por manter a conformidade das organizações com a LGPD, sendo considerado o guardião do Programa de Governança em Privacidade.
Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), o DPO deve ser uma pessoa, natural ou jurídica, indicada pelo controlador, para atuar, principalmente, como um canal de comunicação entre o agente de tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

- Pilares de Segurança da Informação:

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

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

4. DOCUMENTOS DE REFERÊNCIA

I. Código de Ética e Conduta da Scala Data Centers;
II. Política de Privacidade de Dados da Scala Data Centers;

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

III. ISO'S 27001:2022 e 27701:2019;
IV. Lei Geral de Proteção de Dados;
V. Ley N° 21.663 – Ley Marco de Ciberseguridad (Chile), Decreto 295/2024, Decreto 285/2024 e Instrucciones Generales da Agencia Nacional de Ciberseguridad (ANCI).
VI. Lei nº 12.965/2014 – Marco Civil da Internet e Decreto nº 8.771/2016 (Brasil).

5. PAPÉIS E RESPONSABILIDADES

- **RESPONSÁVEL PELA ÁREA DE SEGURANÇA DA INFORMAÇÃO**

I. Prover ampla divulgação da Política e das Normas de Segurança da Informação;

II. Promover ações periódicas de conscientização sobre segurança de informação para os Colaboradores e Fornecedores;

III. Propor ações de aperfeiçoamento da segurança da informação;

IV. Estabelecer normas e procedimentos relacionados à instrumentação da segurança da informação, dispondo sobre a propriedade e o uso da informação, a gestão de acessos e identidades e os incidentes de segurança da informação; e

V. Garantir o cumprimento das normas e critérios desta Política e das Normas de Segurança da Informação quanto à disponibilidade, integridade e qualidade dos sistemas, serviços, segurança, assegurando a confidencialidade das informações;

VI. Disponibilizar e gerir o controle de acessos aos sistemas e à rede para minimizar riscos de acesso não autorizado às informações.

- **DATA PROTECTION OFFICER (DPO) DA SCALA**

I. Cabe ao DPO o desenvolvimento e manutenção da atualização das diretrizes e desdobramento desta Política, visando a orientação da ação dos Responsáveis por Segurança da Informação, Gestores e demais Colaboradores.

- **DELEGADO DE CIBERSEGURIDAD E ENCARGADO DE REPORTES (CHILE)**

I. O Delegado de Ciberseguridad atua como contraparte da Scala perante a Agencia Nacional de Ciberseguridad (ANCI), conforme a Ley N° 21.663 e a Instrucción General 03, e reporta diretamente à alta direção da Companhia;

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

II. O Delegado de Ciberseguridad exerce a função com independência funcional em relação à área de Tecnologia da Informação e deve possuir formação, certificação ou experiência especializada em cibersegurança. Podem ser designados delegados subrogantes;

III. A designação do Delegado e de seus subrogantes é formalizada em documento assinado pelo representante legal e remetido à ANCI pela plataforma oficial. Cessação de funções, renúncia, mudança de área ou qualquer circunstância que afete suas atribuições é comunicada à ANCI, com a acreditação do substituto, em até 5 (cinco) dias úteis;

IV. O Encargado de Reportes de Ciberseguridad, com formação ou experiência técnica em cibersegurança, é responsável pelo cadastro da Companhia na plataforma da ANCI, pela manutenção do e-mail institucional oficial de comunicação com a autoridade e pelo envio dos reportes de incidentes ao CSIRT Nacional, conforme DI-088-SI-08 Report de Incidentes de Segurança da Informação. Sua substituição é comunicada imediatamente à ANCI.

- **LÍDERES DA SCALA**

I. Todos os Colaboradores que ocupam cargos de Gestão devem assegurar que seus liderados conheçam e compreendam esta Política;

II. Reforçar a importância da Segurança da Informação, comunicar, influenciar, bem como fomentar os termos, as obrigações e as responsabilidades desta Política aos seus liderados;

III. Definir quais Colaboradores e Fornecedores, sob sua liderança, podem acessar informações da Scala seguindo as orientações de classificação de informações, conforme descrição contida no documento DI-088-SI-01 Classificação e Descarte de Informação.

- **COLABORADORES**

I. Zelar e garantir o cumprimento da presente Política de Segurança de Informação;

II. Caso um Colaborador equivocadamente acesse informações restritas, internas ou confidenciais, deve, de imediato, comunicar a sua liderança sobre o ocorrido e providenciar o descarte da informação acompanhado de um representante da Área de Tecnologia da Informação da Scala;

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

III. Participar dos treinamentos para os quais forem convocados e comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou normas e procedimentos.

- **PESSOAS ATUANDO EM NOME E BENEFÍCIO DA SCALA**

I. Qualquer pessoa (seja física ou jurídica) que esteja atuando em nome e benefício da Scala não está autorizada a praticar quaisquer atos vedados nesta Política;

II. Preservar a integridade, confidencialidade e proteção das informações, incluindo dados pessoais, aos que têm acesso e fazem uso, bem como zelar e proteger os respectivos de processamento de informações.

6. DIRETRIZES

Segurança da informação consiste na adoção de medidas para proteger a propriedade, confidencialidade, disponibilidade e integridade das informações, da Scala Data Centers e seus clientes, em qualquer forma e suporte que se apresente – física ou digital – das diversas ameaças existentes, a fim de evitar seu uso indevido, inadequado, ilegal ou em desconformidade com a Diretriz de Segurança da Informação da empresa e outras políticas internas.

A segurança de informação é aqui caracterizada pela preservação dos seguintes conceitos:

- A informação constitui um ativo valioso de extrema importância para a Companhia e fundamental para o sucesso dos seus negócios, merecendo, portanto, proteção adequada.

- As diretrizes dispostas nesta Política devem ser parte integrante de todo o ciclo de vida dos sistemas de informação, desde a aquisição, desenvolvimento de novos sistemas e/ou melhoramento dos sistemas já existentes.

- Todas as orientações referentes ao armazenamento e compartilhamento de informação, acesso a sistemas e informação, violação à segurança, fraude, ou vulnerabilidades técnicas, dentre outras, estão relacionadas no documento PR-088-SI-10 Práticas de Segurança da Informação.

6.1 PROPRIEDADE, MONITORAMENTO E CLASSIFICAÇÃO DA INFORMAÇÃO

As informações produzidas e disponibilizadas pelos Colaboradores e Fornecedores em decorrência de suas atividades para a Companhia, em formato físico ou digital, são de propriedade exclusiva da

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

Scala e devem ser utilizadas única e exclusivamente para o atendimento dos interesses do negócio da Scala.

Os equipamentos, meios de comunicação e sistemas da Scala estão sujeitos a monitoramento, sendo certo que eventuais informações de cunho pessoal tratadas por esses meios ou fornecidas à Companhia serão abrangidas por referido controle.

O Colaborador deve estar ciente de que os recursos computacionais e tecnológicos são devidamente monitorados, podendo ser auditados a qualquer momento pela Scala, sem necessidade de aviso prévio.

A classificação das informações é de responsabilidade de todos os Colaboradores e Fornecedores da Scala que criarem arquivos e documentos que se enquadrem nos conceitos de informação Pública, Interna, Restrita ou Confidencial. A classificação deverá ser incluída de forma expressa, conforme diretriz interna da empresa para a Classificação e Descarte de Informações.

Os Responsáveis de cada área devem atentar-se: (i) à classificação expressa das informações que geram durante a realização das atividades, em relação ao seu nível de sigilo, para descrever o devido tratamento e proteção a essas informações, e: (ii) ao respectivo recurso de informação que a armazena.

As informações devem estar adequadamente protegidas e rotuladas em observância às diretrizes desta Política em todo o seu ciclo de vida, que compreende: geração, acesso, manuseio, armazenamento, reprodução, transporte e descarte. Todos os Colaboradores devem estar capacitados para identificação e execução da classificação de informações.
As informações são protegidas por sistemas digitais especializados para evitar a perda de dados da companhia.

Não acessar, manipular, processar ou transmitir informações confidenciais ou restritas da Scala Data Centers ou de seus clientes, sem a autorização do responsável.

A concessão de acessos às Informações Confidenciais deve obedecer ao critério de menor privilégio, no qual os Colaboradores têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

O dever de confidencialidade dos Colaboradores com relação às informações confidenciais que tiverem acesso durante o desempenho de suas funções subsistirá, ainda, nos casos de desligamentos e/ou término da relação contratual.

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

É dever dos Colaboradores detentores de Informações Confidenciais, em função de seus cargos ou atribuições, estabelecer controles rigorosos para que apenas pessoas necessárias e autorizadas tenham acesso a tais informações.

O acesso às informações confidenciais deve ser controlado e restrito aos profissionais com responsabilidades atinentes a tais tópicos, com o devido controle tecnológicos e físico de acesso restrito.

6.2 USO DE RECURSOS

Os recursos tecnológicos e computacionais, bem como o acesso à internet, colocados à disposição dos Colaboradores e Fornecedores autorizados, somente podem ser utilizados para o atendimento dos interesses de negócio da Scala.

Os equipamentos corporativos sob guarda dos Colaboradores e Prestadores de Serviços devem ter instalados os requisitos mínimos de segurança definidos pelo Responsável de Tecnologia e Informação da Scala para acesso interno e remoto à rede corporativa.

Somente *softwares* homologados/validados pela Área de Tecnologia de Informação podem ser instalados nos recursos da Companhia, sendo a instalação de responsabilidade exclusiva da equipe de TI.

Os recursos de tecnologia não podem ser utilizados para expressar opinião pessoal de qualquer natureza, distribuir ou acessar material protegido por direito autoral, anúncios, conteúdos pornográficos, correntes de solidariedade, jogos eletrônicos ou conteúdo que viole direitos da Companhia ou de Fornecedores e Prestadores de bens e serviços.

6.3 DESCARTE DE INFORMAÇÕES

O descarte da informação deve ser realizado com emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital. A informação deve ser descartada considerando os prazos mínimos legais e regulatórios, bem como sua necessidade para o negócio ou área, o que for maior.

6.4 SEGURANÇA COM FORNECEDORES

Para garantir a mitigação dos riscos associados com o acesso de Fornecedores aos ativos da Scala, os requisitos de segurança da informação devem ser formalmente acordados. Por exemplo, os contratos com Fornecedores que possuem acesso às informações devem conter cláusulas que

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

assegurem o cumprimento das regras de segurança da informação, bem como penalidades no caso de descumprimento.

6.5 CONFORMIDADE COM A LEY MARCO DE CIBERSEGURIDAD (CHILE)

Na condição de prestadora de serviços essenciais no Chile, a Scala cumpre as obrigações do artigo 8º da Ley N° 21.663 e da regulamentação da ANCI, por meio dos seguintes compromissos:

I. Manter um sistema contínuo de gestão de segurança da informação, baseado na ISO/IEC 27001, para identificar os riscos às redes, sistemas, dados e à continuidade operacional, com registro das ações executadas;
II. Elaborar, implementar e testar planos de continuidade operacional e de cibersegurança, revisados no mínimo a cada 2 (dois) anos;
III. Realizar continuamente operações de monitoramento, revisão, exercícios, simulados e análise das redes e sistemas, comunicando à ANCI as ações ou programas maliciosos detectados que comprometam a cibersegurança;
IV. Adotar de forma oportuna as medidas de contenção necessárias para reduzir o impacto e a propagação de incidentes, e reportar os incidentes de efeito significativo à ANCI nos prazos legais, conforme DI-088-SI-08;
V. Manter firewalls com política de bloqueio de conexões de entrada por padrão, segmentação de redes, restrição de acessos remotos e ferramentas de detecção e contenção, conforme a Instrucción General 04 e os procedimentos técnicos de TI e Segurança da Informação;
VI. Manter programa contínuo de capacitação e campanhas de ciber-higiene para Colaboradores e Fornecedores;
VII. Obter e manter vigentes as certificações de cibersegurança exigidas pela legislação ou pela ANCI, emitidas por entidades do registro de certificadoras autorizadas;
VIII. Designar o Delegado de Ciberseguridad e o Encargado de Reportes, conforme item 5 desta Política.

6.6 CONFORMIDADE COM O MARCO CIVIL DA INTERNET (BRASIL)

Na condição de administradora de sistema autônomo e de provedora de conexão e de aplicações de internet no Brasil, a Scala cumpre a Lei nº 12.965/2014 (Marco Civil da Internet) e o Decreto nº 8.771/2016, por meio dos seguintes compromissos:

I. Manter o histórico de atribuição de endereços IP a clientes (bloco ou endereço IP, cliente e data e hora de início e término de cada atribuição), que constitui o registro de conexão previsto no

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

Marco Civil, pelo prazo mínimo de 1 (um) ano após o término de cada atribuição, sob sigilo, em ambiente controlado e de segurança;

II. Não armazenar, na provisão de conexão, o histórico de aplicações, sites ou serviços acessados pelos clientes;
III. Manter os registros de acesso ao portal de clientes e às demais aplicações de internet por ela disponibilizadas (usuário, endereço IP e porta de origem, data e hora do acesso), pelo prazo mínimo de 6 (seis) meses;
IV. Proteger os registros com controle estrito de acesso, autenticação multifator, inventário dos acessos realizados e criptografia ou medida de proteção equivalente;
V. Reter a menor quantidade possível de dados pessoais e registros, excluindo-os tão logo atingida a finalidade ou encerrado o prazo legal;
VI. Disponibilizar registros de conexão e de acesso somente mediante ordem judicial, e dados cadastrais apenas às autoridades administrativas com competência legal para requisitá-los;
VII. Tratar de forma isonômica os pacotes de dados, sem monitorar, filtrar ou analisar seu conteúdo, limitando o gerenciamento de tráfego a requisitos técnicos e de segurança da rede, como a mitigação de ataques de negação de serviço.

6.7 REPORTE DE DESVIOS

É dever dos Colaboradores da Scala proteger a propriedade, confidencialidade, disponibilidade e integridade da informação, devendo utilizá-la no melhor interesse da Empresa.

O descumprimento desta Política ou de qualquer Legislação Aplicável está sujeito às medidas disciplinares e outras consequências que podem ser aplicadas pela Scala, sem prejuízo de eventuais medidas legais aplicáveis.

Qualquer pessoa que tenha conhecimento de práticas que possam representar violação ou potencial violação a essa Política ou esteja em desacordo com as legislações nacionais e estrangeiras aplicáveis deverá reportar a situação imediatamente para a área de Segurança da Informação, pelo canal oficial de abertura de chamados, comunicar ao seu gestor direto e à Diretoria de Compliance, por meio dos seguintes canais:

E-mail: scaladatacenters@contatoseguro.com.br
Telefones:

BRASIL: 0800 9009 292
MEXICO: 800 099 1526
COLÔMBIA: 01-800-5189185

CHILE: 800 719 909

Ao fazer um relato, o denunciante deve fornecer o maior detalhamento possível sobre a situação para que as informações apoiem e direcionem os procedimentos de investigação. É importante que o denunciante mantenha o número de registro do relato e o consulte periodicamente para verificar interações que podem ser registradas pela equipe da Scala na plataforma do Canal de Ética a fim de esclarecer e/ou solicitar informações adicionais sobre o relato.

A Scala Data Centers se compromete a investigar todas as denúncias recebidas com independência, cautela e responsabilidade, de maneira justa e imparcial, e aplicar as medidas disciplinares e/ou legais cabíveis, quando necessário.

Toda e qualquer forma de retaliação ao denunciante é reprovada e proibida pela Scala Data Centers.

7. ANEXOS

N/A.

8. REGISTROS

Identificação	Classificação	Proteção	Local de Armazenamento	Recuperação	Tempo mínimo de retenção	Disposição (Forma descarte)
N/A	N/A	N/A	N/A	N/A	N/A	N/A

9. CONTROLE DE VERSÕES

Versão	Elaboração			Análise Crítica			Aprovação		
	Data	Responsável	Departamento	Data	Responsável	Departamento	Data	Responsável	Departamento
1.0	30/10/2024	Isabella Neves Elias Sarmento	Compliance	26/11/2024	Márcio Félix	Segurança da Informação	26/11/2024	Agostinho de Arruda Villela	Technology VP
2.0	08/12/2025	Thiago Miziara	Segurança da Informação	08/12/2025	Márcio Félix	Segurança da Informação	08/12/2025	Leandro Sulinsk	HR VP
3.0	18/09/2026	Thiago Miziara	Segurança da Informação	18/09/2026	Fernando Padia	Segurança da Informação	18/09/2026	Leandro Sulinsk	HR VP

Versão	Alteração Realizada
1.0	Emissão Inicial
2.0	Inclusão de monitoramento contra perda de dados.

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com

3.0	Inclusão da Ley N° 21.663 (Chile) e regulamentação da ANCI nos Documentos de Referência; inclusão dos papéis de Delegado de Ciberseguridad e Encargado de Reportes no item 5; inclusão do item 6.5 – Conformidade com a Ley Marco de Ciberseguridad; inclusão da Lei nº 12.965/2014 e do Decreto nº 8.771/2016 nos Documentos de Referência e do item 6.6 – Conformidade com o Marco Civil da Internet (Brasil).

10. LISTA DE DISTRIBUIÇÃO

Scala Data Centers

Alameda Tocantins, 350, 16º andar • Barueri • SP • 06455-020.
scaladatacenters.com