Política do Sistema de Gestão de Segurança da Informação e Privacidade



LISTA DE DISTRIBUIÇÃO	
Público interno e externo	**X**

HISTÓRICO DE REVISÃO		
AUTOR: **Mariel Prado** Segurança e Processos	**REVISOR:** **Marco Tangari** Segurança e Processos	**APROVADOR:** **Carlos Eduardo Felicio** Operações e Engenharia

VERSÃO	DATA	DESCRIÇÃO
V1.0	29/09/2025	Elaboração do documento

SUMÁRIO

1. OBJETIVO 3
2. ABRANGÊNCIA 3
3. DOCUMENTOS DE REFERÊNCIA 3
4. DEFINIÇÕES 3
5. RESPONSABILIDADES 4
6. AÇÕES DE CONSCIENTIZAÇÃO 4
7. LINHAS GERAIS DOS PROCEDIMENTOS E CONTROLES DE SEGURANÇA 4
7.1 LIMITE DE RISCOS ALTOS EM SEGURANÇA DA INFORMAÇÃO 5
7.2 CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE 5
7.3 LIMITE DE VULNERABILIDADES ALTAS 5
7.4 CONTROLE DE INCIDENTES DE PRIVACIDADE REPORTADOS 6
7.5 ANUTENÇÃO DA PONTUAÇÃO NA FERRAMENTA DE RISCO CIBERNÉTICO 6

1. OBJETIVO

Garantir o compromisso contínuo da **SBA Edge** com a segurança da informação e a privacidade.

2. ABRANGÊNCIA

Esta Política aplica-se a todos os colaboradores e prestadores de serviços no desempenho de suas atividades para a **SBA Edge**.

3. DOCUMENTOS DE REFERÊNCIA

- ABNT NBR ISO/IEC 27001;

4. DEFINIÇÕES

• **Privacidade**: direito relacionado à proteção dos dados pessoais, garantindo que sejam coletados, utilizados, armazenados e descartados com ética, transparência e em conformidade com a legislação vigente (como a LGPD).

• **Ativo de Informação**: qualquer informação ou recurso (digital ou físico) que tenha valor para a organização, incluindo sistemas, dados, pessoas, infraestrutura e processos.

• **Vulnerabilidade**: fraqueza ou falha em sistemas, processos ou controles que pode ser explorada por uma ameaça para causar impacto à segurança da informação ou à privacidade.

• ***Compliance***: conjunto de práticas e ações adotadas para garantir que a organização esteja em conformidade com leis, regulamentos, políticas internas e padrões éticos, incluindo a Política Internacional de Compliance Anticorrupção.

• ***Pentest* (Teste de Intrusão):** simulação controlada de ataques a sistemas e redes, com o objetivo de identificar e explorar vulnerabilidades antes que possam ser utilizadas por agentes mal-intencionados.

• ***Vulnerability Scanning* (Varredura de Vulnerabilidades):** processo automatizado que busca detectar falhas de segurança em sistemas, redes e aplicações.

- ***Risk Scoring (Pontuação de Risco Cibernético):*** metodologia utilizada para medir e acompanhar o nível de risco cibernético da organização, com base em uma combinação de indicadores técnicos e comportamentais.

5. RESPONSABILIDADES

Todos os colaboradores e prestadores de serviços da **SBA Edge**, têm a obrigação de zelar pela segurança das informações que estão em seu poder, portanto é indispensável que todos tenham o conhecimento dessa política, de toda a estrutura do Sistema de Gestão de Segurança da Informação e Privacidade em especial ao documento POL 001 - Política de Segurança da Informação e a POL 002 – Política de Privacidade que estabelece todas as diretrizes para o tema.

Garantindo o cumprimento rígido de nossas diretrizes a SBA *Communications Corporations* estabelece a Política de Código de Conduta e Política Internacional De Compliance Anticorrupção.

6. AÇÕES DE CONSCIENTIZAÇÃO

A **SBA Edge** em conjunto com a SBA *Communications Corporations*, por meio de suas políticas e procedimentos organizacionais, estabelece o compromisso de promover a conscientização e o engajamento de todos os colaboradores na manutenção de uma estrutura sólida de segurança da informação. Para isso, realiza treinamentos internos obrigatórios que visam disseminar boas práticas e fortalecer a cultura de proteção dos ativos de informação.

7. LINHAS GERAIS DOS PROCEDIMENTOS E CONTROLES DE SEGURANÇA

A **SBA Edge** através da Alta Direção estabelece, mantém e divulga as Políticas do Sistema de Gestão de Segurança da Informação e Privacidade com o propósito de garantir a confidencialidade, integridade, disponibilidade e privacidade das informações necessárias para o fornecimento dos serviços de *Colocation* e *Cloud Computing* em conformidade com seus objetivos estabelecidos e seguintes compromissos:

7.1 LIMITE DE RISCOS ALTOS EM SEGURANÇA DA INFORMAÇÃO

São disponibilizadas ao cliente opções de atendimento em canais pré-determinados de telefone e Sistema de Atendimento da **SBA Edge.**

A **SBA Edge** adota uma abordagem proativa e sistematizada para a gestão de riscos, com o objetivo de manter, de forma contínua estabelecendo um limite de riscos altos. Com isso adotamos as seguintes práticas:

- Ciclos regulares de avaliação de riscos, considerando mudanças no ambiente tecnológico, ameaças emergentes e inclusão de novos ativos;
- Planos de tratamento formalmente definidos, com responsáveis, prazos e controles específicos para mitigação, em conformidade com os princípios da ISO/IEC 27001 e a ISO/IEC 27005;
- Integração entre as áreas, promovendo uma governança eficiente sobre os ativos críticos do negócio.

Essa prática fortalece a resiliência organizacional e assegura a continuidade dos serviços prestados.

7.2 CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Reconhecendo que a conscientização é um dos pilares mais eficazes da segurança, a **SBA Edge** investe continuamente em ações de capacitação e sensibilização de seus colaboradores. Com base em sua agenda anual de treinamentos e campanhas internas, a organização define metas tangíveis que atendam a política, conforme as certificações vigentes.

7.3 LIMITE DE VULNERABILIDADES ALTAS

Para preservar a integridade de seu ambiente tecnológico, a **SBA Edge** estabelece práticas de higiene cibernética avançadas, com foco na identificação e correção tempestiva de vulnerabilidades críticas. Para atender a esse critério, a organização realiza:

- Varreduras automatizadas de vulnerabilidades (vulnerability scanning);
- Testes de intrusão (pentests) conduzidos por empresas especializadas;

Tais medidas estão alinhadas com os controles da ISO/IEC 27002 e práticas recomendadas de segurança cibernética internacional.

7.4 CONTROLE DE INCIDENTES DE PRIVACIDADE REPORTADOS

Como forma de garantir o pleno atendimento aos princípios da privacidade e da proteção de dados pessoais, a **SBA Edge** adota medidas robustas e integradas de prevenção e monitoramento, conforme as certificações vigentes.

A abordagem preventiva, aliada à cultura organizacional de responsabilidade com dados, sustenta esse compromisso.

A autorização de entrada de equipamentos será dada desde que seja respeitado o espaço e energia contratados;

7.5 MANUTENÇÃO DA PONTUAÇÃO NA FERRAMENTA DE RISCO CIBERNÉTICO

A **SBA Edge** adota uma ferramenta especializada de avaliação contínua de risco cibernético, reconhecida internacionalmente, com o objetivo de monitorar de forma proativa a postura de segurança da organização no ambiente digital.

Para alcançar e sustentar esse desempenho, a organização implementa as seguintes práticas:

- Monitoramento contínuo dos indicadores de segurança avaliados pela plataforma, com revisões periódicas e análise de tendências;
- Planos de ação específicos para remediação de vulnerabilidades e não conformidades, acompanhados por comitês técnicos e instâncias de governança;
- Melhoria contínua da infraestrutura tecnológica e dos processos de segurança, garantindo aderência às exigências do mercado, das boas práticas internacionais e dos controles descritos na ISO/IEC 27001.

A medição dos objetivos de segurança e privacidade é documentada e acompanhada sistematicamente assegurando a rastreabilidade, a prestação de contas e a melhoria contínua do SGI.