POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

PK

SCP

CONTROLE DO DOCUMENTO

HISTÓRICO DE MUDANÇAS

Versão	Data da Alteração	Natureza da Alteração
1.1	30/03/2022	Versão inicial do documento
1.2	13/03/2023	Revisão da estrutura documental e ajuste de indentação.
1.3	21/03/2024	Revisão na estrutura documental e ajuste de indentação. Substituição de todos os termos “Take Blip” para “Grupo Blip” assim como alterações no layout e capa do documento atendendo a nova marca.

CRIAÇÃO E REVISÃO DO DOCUMENTO

Versão	Nome	E-mail	Data
1.1	Fabiana Ferreira	fabiana.ferreira@take.net	30/03/2022
1.2	Júlio César Silva	julio.cesar@take.net	13/03/2023
1.3	Ingrid Ramos Thainá Moreira	ingrid.ramos@blip.ai thaina.moreira@blip.ai	21/03/2024

APROVADORES DO DOCUMENTO

Versão	Nome	Função	Data
1.1	Comitê de Segurança da Informação	Membros deliberativos	06/04/2022
1.2	Comitê de Segurança da Informação	Membros deliberativos	13/03/2023
1.3	Comitê Gestor de Segurança da Informação, Privacidade e Proteção de Dados	Membros deliberativos	03/04/2024

Pk

SCP

SUMÁRIO

PK

SCP

1. OBJETIVO

Este documento contempla as principais diretrizes de segurança da informação e cibernética que devem ser observadas por todos os fornecedores que possuem relação com os ativos de informação do Grupo Blip, bem como para conscientizar os fornecedores sobre o uso aceitável dos recursos da organização.

Ainda, este documento estabelece a definição de responsabilidade sobre as ações de fornecedores e ações disciplinares correlatas.

2. ESCOPO

Esta política de segurança da informação para fornecedores deve ser parte integrante do contrato de prestação de serviço de todos os fornecedores do Grupo Blip.

No ato da assinatura do contrato de prestação de serviço o fornecedor assume total conhecimento e concordância com as diretrizes estabelecidas neste documento.

3. DIRETRIZES

As seções abaixo descrevem as diretrizes de segurança da informação relacionadas com os fornecedores.

3.1. PROPRIEDADE INTELECTUAL

3.1.1. O fornecedor é responsável por garantir a conformidade legal de todo e qualquer sistema ou conteúdo utilizado durante a realização de seu serviço;

3.1.2. O fornecedor é responsável pela propriedade intelectual do conteúdo dos ativos de sua propriedade nas dependências do Grupo Blip;

3.1.3. O fornecedor é responsável por garantir que os softwares por ele instalados, não ferem qualquer lei de Propriedade Intelectual, incluindo direitos autorais.

3.2. ACESSO À INTERNET

3.2.1. O fornecedor só poderá acessar a Internet por meio das redes disponibilizadas pelo Grupo Blip com autorização formal e acompanhamento de um colaborador responsável.

3.2.2. O Grupo Blip se reserva o direito de monitorar o acesso à Internet do fornecedor a fim de garantir o uso adequado;

3.2.3. O Grupo Blip se reserva o direito de bloquear o acesso aos sites que considerar inadequados, sem prévio aviso;

3.2.4. O acesso à Internet realizado pelo fornecedor deverá ter como único objetivo o cumprimento de seu serviço, seja este acesso fornecido pelo Grupo Blip ou por terceiros.

3.3. COMPUTAÇÃO MÓVEL

Pk

SCP

3.3.1. O Grupo Blip reserva-se o direito de realizar auditoria nos equipamentos do fornecedor, antes de autorizar sua utilização;

3.3.2. O fornecedor se compromete inteiramente pela segurança dos dados de seus equipamentos nas dependências do Grupo Blip;

3.3.3. O fornecedor é responsável por garantir que os equipamentos ou mídias que utiliza estão com todos os softwares atualizados, legalizados, com antivírus e livres de qualquer tipo de software que possa prejudicar a rede interna do Grupo Blip.

3.4. MENSAGERIA ELETRÔNICA

3.4.1. O Grupo Blip reserva-se o direito de monitorar os e-mails enviados e recebidos pelo fornecedor, quando este utilizar a plataforma de gerenciamento de e-mails fornecida pelo Grupo Blip. ;

3.4.2. O Grupo Blip deverá garantir que o fornecedor assume que todos os e-mails enviados durante a execução de serviço, utilizando conta fornecida pelo Grupo Blip são e-mails corporativos e podem ser monitorados;

3.4.3. Nas dependências do Grupo Blip o fornecedor deve ler e enviar e-mails apenas relacionados com seu trabalho;

3.4.4. Em qualquer momento e de qualquer local, o fornecedor não deve encaminhar e-mails para colaboradores do Grupo Blip cujo conteúdo não tenha relação com o trabalho.

3.5. MANUSEIO E CLASSIFICAÇÃO DAS INFORMAÇÕES

3.5.1. O fornecedor se compromete a apenas receber informações do Grupo Blip que tenham relação direta com seu serviço e após consentimento e autorização formal do Grupo Blip;

3.5.2. O fornecedor deverá se comprometer com a total confidencialidade, integridade e disponibilidade das informações do Grupo Blip que lhe forem concedidas;

3.5.3. A divulgação interna das informações do Grupo Blip dentro da empresa do fornecedor deve ser prévia e expressamente aprovada pelo Grupo Blip;

3.5.4. O fornecedor se compromete a não transmitir informações do Grupo Blip por canais de comunicação não seguros, que possam ocasionar vazamento destas informações;

3.5.5. O fornecedor se compromete a providenciar o descarte adequado e seguro das informações do Grupo Blip ao final do serviço ou quando elas não forem mais utilizadas (o que ocorrer primeiro);

3.5.6. O Grupo Blip se reserva no direito de realizar auditorias de segurança da informação em seus fornecedores, quando as informações fornecidas forem de classificação RESTRITA ou CONFIDENCIAL.

3.6. TRATAMENTO DAS INFORMAÇÕES

3.6.1. O armazenamento de informações do Grupo Blip pelo fornecedor deve ser realizado de modo seguro, ou seja, com controle de acesso restrito aos envolvidos com o serviço dentro da empresa e com criptografia quando a informação for classificada como confidencial;

Pk

SCP

3.6.2. Caso o fornecedor esteja com uma mídia em trânsito contendo informações do Grupo Blip, este é responsável por garantir que a perda ou roubo desta mídia não implique no acesso a estas informações;

3.6.3. Se necessário, o fornecedor deve realizar uma avaliação e tratamento de riscos quanto ao tratamento de informações sensíveis do Grupo Blip;

3.6.4. O fornecedor também se compromete com a garantia de que as informações do Grupo Blip não serão alteradas durante o armazenamento em qualquer tipo de mídia sob sua responsabilidade.

3.7. ACESSO À REDE

3.7.1. O fornecedor somente poderá acessar a rede interna do Grupo Blip após autorização formal desta e mediante autenticação individual;

3.7.2. O acesso do fornecedor à rede interna poderá ser monitorado pela área de Segurança da Informação do Grupo Blip, quando esta julgar necessário;

3.7.3. O Grupo Blip se reserva no direito de liberar o acesso local ou remoto à sua rede interna somente após a autorização formal e com o devido acompanhamento por um colaborador;

3.7.4. Os acessos remotos de todos os fornecedores devem ser criados e autorizados pela área de Segurança da Informação do Grupo Blip.

3.8. CREDENCIAIS DE ACESSO

3.8.1. O fornecedor não deve solicitar, aceitar ou utilizar senha de acesso dos colaboradores do Grupo Blip em nenhum caso;

3.8.2. Toda senha utilizada pelo fornecedor deve ter sido criada especificamente para este fim e identificá-lo de modo inequívoco;

3.8.3. O Grupo Blip é responsável por realizar a inativação da senha do fornecedor. Caso o fornecedor identifique que a credencial ainda está ativa, após finalização de contrato, este deve solicitar obrigatoriamente a sua desativação;

3.8.4. O fornecedor não deve compartilhar senhas utilizadas para acesso a sistemas do Grupo Blip entre seus colaboradores, ou seja, cada credencial e senha deve identificar um único colaborador do fornecedor;

3.8.5. O fornecedor é responsável pela segurança das senhas que lhe são entregues e deve comunicar imediatamente ao Grupo Blip a sua perda ou vazamento.

3.9. COLABORADORES

3.9.1. O fornecedor deve garantir que seus colaboradores alocados para a realização de determinado serviço possuem a formação e qualificação necessária para tal;

3.9.2. O fornecedor deve informar ao Grupo Blip o nome, formação e tempo de serviço de seus colaboradores quando for solicitado;

3.9.3. O Grupo Blip reserva-se o direito de estabelecer requisitos de qualificação, formação e tempo de serviço, para autorizar o acesso de colaboradores do fornecedor a suas informações, sistemas ou dependências físicas;

Pk

SCP

3.9.4. O fornecedor é responsável por comunicar imediatamente ao Grupo Blip o desligamento de seus colaboradores, quando estes estejam prestando algum serviço interno ou possuam credenciais de acesso aos sistemas e informações do Grupo Blip;

3.9.5. O fornecedor deve comunicar imediatamente qualquer mudança na lista de seus colaboradores autorizados a prestar o serviço interno do Grupo Blip;

3.9.6. Todos os colaboradores do fornecedor que prestam serviço ao Grupo Blip assumem total conhecimento e concordância com o conteúdo deste documento.

3.10. SEGURANÇA FÍSICA

3.10.1. O fornecedor é responsável pela informação física concedida a ele pelo Grupo Blip, devendo assegurar a confidencialidade, integridade e disponibilidade destas quando estiverem em seu poder;

3.10.2. O fornecedor é responsável pela devolução para o Grupo Blip ou pelo descarte adequado das informações físicas quando estas não forem mais necessárias ou ao final de seu serviço;

3.10.3. O fornecedor se compromete a acessar as dependências físicas do Grupo Blip somente quando devidamente autorizado e acompanhado por um colaborador;

3.10.4. O fornecedor não aceitará receber para si qualquer tipo de meio de acesso físico às dependências do Grupo Blip (ex. senhas de alarmes, senhas de controle de acesso, chaves das portas, entre outros);

3.10.5. Para a retirada de equipamentos do Grupo Blip, por qualquer motivo, o fornecedor deverá receber autorização formalizada por um dos colaboradores da organização, podendo esta ser por e-mail ou registro de chamado interno.

4. INCIDENTES DE SI E SANÇÕES DISCIPLINARES

4.1. Eventual violação das diretrizes constituintes dessa política implica incidente de segurança da informação será devidamente registrado e analisado pelo Comitê Gestor de Segurança da Informação, Privacidade e Proteção de Dados (CGSIPD).

4.2. Após análise do Comitê Gestor de Segurança da Informação, Privacidade e Proteção de Dados (CGSIPD), serão deliberadas medidas disciplinares ao fornecedor, que podem incluir:

4.2.1. Advertência formal ou informal;
4.2.2. Suspensão do contrato (interrupção temporária);
4.2.3. Rescisão do contrato (cancelamento definitivo);
4.2.4. Multas previstas em contrato;
4.2.5. Ações judiciais ou abertura de boletim de ocorrência.

Pk

SCP

5. REFERÊNCIAS

PO.SEG.001 - Política de Segurança da Informação.

NO.SEG.008 - Norma Gestão de Fornecedores.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos.

ABNT NBR ISO/IEC 27001:2022 – Segurança da Informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da Segurança da Informação.

ABNT NBR ISO/IEC 27002:2022 – Segurança da Informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.

Pk

SCP

6. ANEXOS

Não há.

Sergio Cruz Passos

Paulo Kimura