Política de Segurança da Informação para Fornecedores

Versão 1.0
Última atualização: 06/04/2022

Sumário

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 de Take 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 da Take 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 da Take 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 acesso à Internet realizado pelo fornecedor em qualquer uma das redes disponibilizadas por Take Blip, somente poderá ocorrer após autorização formal e com acompanhamento de um colaborador de Take Blip responsável;

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

3.2.3. Take 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 pela Take Blip ou por terceiros.

3.3. COMPUTAÇÃO MÓVEL

3.3.1. Take Blip reserva-se no 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 da Take 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 de Take Blip.

3.4. MENSAGERIA ELETRÔNICA

3.4.1. Take 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 por Take Blip;

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

3.4.3. Nas dependências de Take 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 de Take 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 da Take Blip que tenham relação direta com seu serviço e após consentimento e autorização formal da Take Blip;

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

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

3.5.4. O fornecedor se compromete a não transmitir informações de Take 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 de Take Blip ao final do serviço ou quando elas não forem mais utilizadas (o que ocorrer primeiro);

3.5.6. Take 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 de Take 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;

3.6.2. Caso o fornecedor esteja com uma mídia em trânsito contendo informações de Take 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 de Take Blip;

3.6.4. O fornecedor também se compromete com a garantia de que as informações de Take 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 de Take 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 de Take Blip, quando esta julgar necessário;

3.7.3. Take 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 da Take Blip.

3.8. CREDENCIAIS DE ACESSO

3.8.1. O fornecedor não deve solicitar, aceitar ou utilizar senha de acesso dos colaboradores de Take 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. Take 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 de Take 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 a Take 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 a Take Blip o nome, formação e tempo de serviço de seus colaboradores quando for solicitado;

3.9.3. A Take 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;

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

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

3.9.6. Todos os colaboradores do fornecedor que prestam serviço a Take 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 por Take Blip, devendo assegurar a confidencialidade, integridade e disponibilidade destas quando estiverem em seu poder;

3.10.2. O fornecedor é responsável pela devolução para Take 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 de Take 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 de Take Blip (ex. senhas de alarmes, senhas de controle de acesso, chaves das portas, entre outros);

3.10.5. Para a retirada de equipamentos de Take 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 (CGSI).

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

4.2.1. Advertência formal ou informal;

4.2.2. Cancelamento do contrato de prestação de serviço;

4.2.3. Multas previstas em contrato;

4.2.4. Ações judiciais ou abertura de boletim de ocorrência.

5. REFERÊNCIAS

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

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – 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.

6. ANEXOS

Não há.