BLUE TECHNOLOGY
CNPJ/MF 18.191.583/0001-40
Rua Arnóbio Marques, 253 SALAS 2403 e 2404 – Empresarial Camilo Brito
Santo Amaro - Recife/PE - CEP: 50.100-130

Política de Segurança da Informação - PSI

BLUE TECHNOLOGY
CNPJ/MF 18.191.583/0001-40
Rua Arnóbio Marques, 253 SALAS 2403 e 2404 – Empresarial Camilo Brito
Santo Amaro - Recife/PE - CEP: 50.100-130

Política de Segurança da Informação - PSI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de Informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas. Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos a **BLUE TECHNOLOGY** e prejudicar o crescimento e vantagens competitivas.

Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação da BLUE TECHNOLOGY, no que tange aos dados nele armazenados.

Segurança da Informação são esforços contínuos para a proteção dos ativos de informação, auxiliando a BLUE TECHNOLOGY a cumprir sua missão. Para tanto, visa atingir os seguintes objetivos:

- **Confidencialidade**: garantir que as informações tratadas sejam deconhecimento exclusivo de pessoas especificamente autorizadas;
- **Integridade**: garantir que as informações sejam mantidas íntegras, sem modificações indevidas - acidentais ou propositais;
- **Disponibilidade**: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.
- **Autenticidade**: Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação.

PROTEÇÃO DA INFORMAÇÃO

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos físicos da BLUE TECHNOLOGY, a informação deve ser adequadamente manuseada e protegida. A informação pode estar presente em diversas formas, tais como:

- Sistemas de informação;
- Diretórios de rede;
- Bancos de dados;
- Mídia impressa, magnética ou ótica;
- Dispositivos eletrônicos;
- Equipamentos portáteis;

Toda informação relacionada às operações da BLUE TECHNOLOGY, gerada ou desenvolvida nas dependências do mesmo ou de algum prestador de serviço, constitui ativo desta instituição, essencial à condução de negócios, e em última análise, à sua existência

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da BLUE TECHNOLOGY.

É diretriz que toda informação de propriedade da BLUE TECHNOLOGY seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

RESPONSABILIDADES

É missão e responsabilidade de cada prestador de serviço, seja por meio de seu prestador, estagiário, parceiro ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente ***Política de Segurança da Informação***. É imprescindívelque cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas pela empresa, por meio de seus prestadores de serviços e estagiários, devem observar a legislação vigente e a normatizaçãode órgãos e entidades reguladoras, com relação à segurança da informação.

Para auxiliar a todos os usuários nessa missão, a BLUE TECHNOLOGY criou a área de compliance, que administra as disciplinas de conhecimento que dão suporte a essa ciência. A área de Compliance e o Encarregado de Dados Pessoais da BLUE TECHNOLOGY é responsável por editar as políticas e padrões que apoiam a todos na proteção dos ativos

de informação e estão preparados para auxiliar na resolução de problemas relacionados ao tema.

INFORMAÇÕES CONFIDENCIAIS

São consideradas informações confidenciais, para os fins desta política, quaisquer informações das partes consideradas não disponíveis ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais de apoio, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em quaisquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela BLUE TECHNOLOGY e/ou obtidas pelos prestadores de serviço em decorrência da execução do contrato de prestação de serviço. São responsáveis pela observância desta Política os:

- Prestadores de serviços em geral da BLUE TECHNOLOGY;
- Terceiros que indiretamente possuem relação com a BLUE TECHNOLOGY (incluindo advogados, fornecedores, auditores e consultores).

Os prestadores de serviços e consultores que receberem as informações confidenciais deverão mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções. Nenhuma das informações confidenciais poderá ser repassada para terceiros sem consentimento por escrito da BLUE TECHNOLOGY. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pela BLUE TECHNOLOGY.

As informações confidenciais somente poderão ser utilizadas para fins deexecução de atividades, conforme acordadas com a BLUE TECHNOLOGY.

O prestador de serviço e/ou terceiro deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las, a não ser para o proprietário dos dados ou seu representante legal.

O prestador de serviço e/ou terceiro deverá informar prontamente a BLUE TECHNOLOGY sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta Política.

Excetuam-se da obrigação de confidencialidade disposta nesta política:

- O atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, Tribunais e de Órgãos Públicos Administrativos;
- A divulgação das informações confidenciais aos agentes públicos e representantes (incluindo, mas não se limitando, a advogados, procuradores, auditores e consultores);
- Informações confidenciais que forem divulgadas somente após o consentimento, por escrito, da BLUE TECHNOLOGY.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam alertar e responsabilizar o prestador de serviço no exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito.

CLASSIFICAÇÃO DA INFORMAÇÃO

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.

As informações, no período de geração, guarda, uso, transferência e destruição, devem ser tratadas em conformidade com cada etapa do ciclo.

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las.

Cabem aos prestadores de serviço todos os esforços necessários de segurança para protegê-las.

Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem da BLUE TECHNOLOGY podendo levar à extinção das operações ou prejuízos graves ao crescimento.

PROTEÇÃO DOS DADOS PESSOAIS

Para garantir a privacidade e a proteção dos seus Dados Pessoais, adotamos recursos tecnológicos avançados para garantir a segurança de todos os dados tratados pela Empresa. Entre as medidas de segurança implementadas, estão a implementação de controles de acesso a sistemas e ambientes de tratamento de dados, técnicas de criptografia e a instalação de barreiras contra o acesso indevido às bases de dados.

Por isso, a atuação dos prestadores de serviço é fundamental para a manutenção de um ambiente seguro para todos. Caso seja identificado ou tome conhecimento de qualquer fator que comprometa a segurança dos seus dados na sua relação com a BLUE TECHNOLOGY, por favor entre em contato com a Equipe de Compliance e o Encarregado de Dados Pessoais.

SENHAS

Boas práticas para criação de senhas

Evitar a utilização de:

- Nomes, sobrenomes, nomes de contas de utilizadores de dados de membros da família;
- Números de documentos ou de telefone
- Placa de carros
- Datas de aniversários, festivas, etc.;
- Sequência do teclado

Utilizar:

- Números aleatórios;
- Vários e diferentes tipos de caracteres;
- Caracteres especiais;
- Substituir uma letra por número com semelhança visual;
- Frase longa com letras e números;
- A primeira, segunda ou última letra de uma frase incluindo números

CORREIO ELETRÔNICO (E-MAIL)

O uso do correio eletrônico da BLUE TECHNOLOGY é para fins corporativos e relacionados as atividades do prestador de serviço usuário dentro da empresa. A utilização desse serviço para fins pessoais não é permitida para que não prejudique a BLUE TECHNOLOGY e não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos prestadores de serviço o uso do correio eletrônico da BLUE TECHNOLOGY:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legitimo da BLUE TECHNOLOGY (**caso necessário enviar a múltiplos destinatários distintos, recomendamos utilizar a ferramenta de cópia oculta dentro do e-mail**);
- Enviar mensagens por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico

que não esteja autorizado a utilizar;

- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a BLUE TECHNOLOGY vulnerável a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer sócio ou prestador da BLUE TECHNOLOGY estiver sujeito a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:

    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da BLUE TECHNOLOGY;
    - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
    - contenha arquivos com código executável (.EXE, .COM, .BAT, .PIF, .JS, .VBS, .HTA, .SRC, .CPL, .REG, .DLL, .INF, PPS, DBX, DDL, Inbox, EML, MBX, MMS, NCH, ODS, SYS, BIN e TBB) ou qualquer outra extensão que represente um risco à segurança;
    - vise obter acesso não autorizado a outro computador, servidor ou rede;
    - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    - vise burlar qualquer sistema de segurança;
    - vise vigiar secretamente ou assediar outro usuário;
    - vise acessar informações confidenciais sem explícita autorização do proprietário;
    - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
    - tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
    - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
    - tenha fins políticos locais ou do país (propaganda política);
    - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do prestador de serviço
- Gerência/função ou departamento
- Nome da empresa
- Texto informativo da LGPD.

CONTROLES DE ACESSO

Os controles de acesso utilizados pela organização para proteger informações confidenciais de acessos não autorizados são:

- Login e senha próprio de cada usuário, seja ele um prestador de serviços, estagiário, fornecedor ou outro tipo de contrato;
- Criptografia;

MEDIDAS DE SEGURANÇA APLICADAS

Na BLUE TECHNOLOGY são utilizadas algumas medidas de proteção das informações por intermédio de diversas ações. Aqui na BLUE TECHNOLOGY nós utilizamos, além das medidas de controle de acesso acima, medidas de segurança, como *firewall* e antivírus.

VIOLAÇÃO DA POLÍTICA, NORMAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

As violações de segurança devem ser informadas à área de compliance e ao Encarregado de Dados Pessoais de forma imediata. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas;

Os princípios de segurança estabelecidos na presente política embasam a administração da BLUE TECHNOLOGY e devem ser observados por **todos** na execução de suas funções.

A desconformidade com as diretrizes desta política e a respectiva violação de normas sujeitam os prestadores de serviço e/ou consultores a penalidades civis e/ou criminais na máxima extensão que a lei permitir e ensejam rescisão de contrato.

Caso haja dúvida quanto aos princípios e responsabilidades descritas nesta norma, deve-se entrar em contato com o Compliance ou Encarregado de Dados Pessoais.

DIREITOS DE PROPRIEDADE

Todo produto resultante do trabalho dos prestadores de serviço e/ou consultores (coleta de dados, documentos, sistema, metodologia, dentre outros) é de propriedade da BLUE TECHNOLOGY.

Em caso de extinção ou rescisão de contrato de prestação de serviços, o prestador de serviço e/ou consultor que detiver informações confidenciais geradas em decorrência dessa prestação deverá repassá-las de imediato à Diretoria da BLUE TECHNOLOGY.

ORGANIZAÇÃO DO AMBIENTE DE TRABALHO

Em relação a como se comportar no ambiente de trabalho no que diz respeito a telas e mesas de trabalho, é imprescindível o prestador de serviço agir de acordo com a política de mesa e tela limpa da BLUE TECHNOLOGY, que em caso de descumprimento, poderá gerar penalidades disciplinares.

CONVERSAS EM LOCAIS PÚBLICOS E REGISTRO DE INFORMAÇÕES

Não discutir ou comentar assuntos confidenciais em:

- Locais públicos;
- Redes sociais; e/ou
- Mensagens de texto, exceto quando autorizada pelo cliente e respeitando a política de privacidade da BLUE TECHNOLOGY.

LEIS E REGULAMENTOS

É de obrigatoriedade dos prestadores de serviços e consultores conhecer a legislação e cumprir os requisitos legais, normas e padrões locais vigentes.

Esta Política orienta a conduta de todos no desempenho das atividades relacionadas ao trabalho pelo qual foram contratados para prestação de serviço.

O descumprimento dos preceitos contidos nesta Política acarretará a apuração de responsabilidades e aplicação de medidas disciplinares conforme disposto abaixo.

SANÇÕES:

a) Caso o utilizador não cumpra as regras desta Política, ele estará sujeito à aplicação de sanções que serão determinadas pela direção do **BLUE TECHNOLOGY** de acordo com o grau de gravidade da conduta praticada pelo utilizador:

(i) **notificação**: no caso de infrações consideradas leves;
(ii) **suspensão do contrato**: no caso de infrações consideradas graves ou quando for constatada a reincidência de uma conduta classificada leve; e,
(iii) **encerramento do contrato**: no caso de infrações consideradas gravíssimas ou quando for constatada reincidência de uma conduta considerada grave. Tratando-se de prestador de serviços, isso significa a rescisão do contrato.

b) Os utilizadores que cometerem infração às regras desta Política serão
c) comunicados por escrito. Tal comunicação conterá a regra violada, a conduta praticada pelo utilizador e a sanção aplicada pela empresa **BLUE TECHNOLOGY**.

Recife, 04/03/2025

